II

(Akty o charakterze nieustawodawczym)

ROZPORZĄDZENIA

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2016/799

z dnia 18 marca 2016 r.

w sprawie wykonania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 165/2014 ustanawiającego wymogi dotyczące budowy, sprawdzania, instalacji, użytkowania i naprawy tachografów oraz ich elementów składowych

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 165/2014 z dnia 4 lutego 2014 r. w sprawie tachografów stosowanych w transporcie drogowym ([1]), w szczególności jego art. 11 i art. 12 ust. 7,

a także mając na uwadze, co następuje:

(1) Rozporządzeniem (UE) nr 165/2014 wprowadzono tzw. drugą generację tachografów cyfrowych (tzw. tachografów inteligentnych), które obejmują połączenie z urządzeniem GNSS (globalny system nawigacji satelitarnej), urządzenie wczesnego wykrywania na odległość oraz interfejs do inteligentnych systemów transportowych. Należy ustanowić specyfikacje dotyczące wymogów technicznych w zakresie budowy tachografów inteligentnych.

(2) Urządzenie wczesnego wykrywania na odległość, przewidziane na mocy art. 9 ust. 4 rozporządzenia (UE) nr 165/2014, powinno przekazywać funkcjonariuszowi kontroli drogowej dane z tachografu cyfrowego oraz informacje dotyczące mas oraz masy przypadającej na osie całego zespołu pojazdów (ciągnika i przyczep lub naczep), zgodnie z dyrektywą 96/53/WE Parlamentu Europejskiego i Rady ([2]). Powinno to umożliwić skuteczną i szybką kontrolę pojazdów przez organy kontrolne, przy zmniejszeniu liczby urządzeń elektronicznych w kabinie pojazdu.

(3) Zgodnie z dyrektywą 96/53/WE, w przypadku urządzenia wczesnego wykrywania na odległość należy stosować normy CEN DSRC ([3]), o których mowa we wspomnianej dyrektywie, w zakresie częstotliwości 5795–5805 MHz. Ponieważ ten zakres częstotliwości jest wykorzystywany również na potrzeby elektronicznych systemów pobierania opłat, a także w celu uniknięcia zakłóceń między aplikacjami służącymi do pobierania i kontroli opłat drogowych, funkcjonariusze służb kontrolnych nie powinni używać urządzenia wczesnego wykrywania na odległość na placu poboru opłat.

(4) Należy wprowadzić w tachografie inteligentnym nowe mechanizmy zabezpieczeń na potrzeby utrzymania poziomu bezpieczeństwa tachografu cyfrowego, aby wyeliminować obecne luki w zakresie bezpieczeństwa. Jednym z takich zagrożeń jest brak daty ważności certyfikatów cyfrowych. W celu uwzględnienia najlepszych praktyk w dziedzinie bezpieczeństwa zaleca się unikanie stosowania certyfikatów cyfrowych bez dat ważności. Okres ważności normalnie użytkowanych przyrządów rejestrujących powinien wynosić 15 lat, licząc od dnia wystawienia certyfikatu cyfrowego przyrządu rejestrującego. Przyrządy rejestrujące powinny być wymieniane po upływie tego okresu ważności.

([1]) Dz.U. L 60 z 28.2.2014, s. 1.

([2]) Dyrektywa Rady 96/53/WE z dnia 25 lipca 1996 r. ustanawiająca dla niektórych pojazdów drogowych poruszających się na terytorium Wspólnoty maksymalne dopuszczalne wymiary w ruchu krajowym i międzynarodowym oraz maksymalne dopuszczalne obciążenia w ruchu międzynarodowym (Dz.U. L 235 z 17.9.1996, s. 59).

([3]) Normy Europejskiego Komitetu Normalizacyjnego (CEN) EN 12253, EN 12795, EN 12834 i EN 13372 oraz norma ISO 14906 w zakresie wydzielonej łączności krótkiego zasięgu.

(5) Zapewnienie bezpiecznych i wiarygodnych informacji o położeniu jest niezbędnym elementem skutecznego działania tachografów inteligentnych. Dlatego też należy zapewnić ich kompatybilność z usługami dodanymi oferowanymi przez program Galileo, określonymi w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 1285/2013 ([1]), aby poprawić bezpieczeństwo tachografów inteligentnych.

(6) Zgodnie z art. 8 ust. 1, art. 9 ust. 1 oraz art. 10 ust. 1 i 2 rozporządzenia (UE) nr 165/2014, stosowanie mechanizmów zabezpieczających wprowadzonych przez to rozporządzenie powinno rozpocząć się po 36 miesiącach od wejścia w życie niezbędnych aktów wykonawczych, aby umożliwić producentom opracowanie nowej generacji tachografów inteligentnych oraz uzyskanie świadectw homologacji typu od właściwych organów.

(7) Zgodnie z rozporządzeniem (UE) nr 165/2014, pojazdy zarejestrowane po raz pierwszy w państwie członkowskim po upływie 36 miesięcy od wejścia w życie niniejszego rozporządzenia Komisji, powinny być wyposażone w tachograf inteligentny spełniający jego wymogi. W każdym przypadku wszystkie pojazdy użytkowane w państwie członkowskim innym niż ich państwo członkowskie rejestracji powinny zostać wyposażone w tachograf inteligentny spełniający wymogi w ciągu 15 lat od daty rozpoczęcia stosowania tych wymogów.

(8) Rozporządzeniem Komisji (WE) nr 68/2009 ([2]) zezwolono na stosowanie – w okresie przejściowym upływającym dnia 31 grudnia 2013 r. – adaptera, aby umożliwić instalowanie tachografów w pojazdach kategorii M1 i N1. Biorąc pod uwagę trudności techniczne związane z poszukiwaniem rozwiązania alternatywnego dla stosowania adaptera, eksperci z sektora motoryzacji i tachografów wraz z Komisją stwierdzili, że żadne alternatywne rozwiązanie dla adaptera nie jest wykonalne bez poniesienia przez branżę wysokich kosztów, które byłyby nieproporcjonalne do rozmiaru rynku. W związku z tym należy bezterminowo dopuścić stosowanie adapterów w pojazdach kategorii M1 i N1.

(9) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią komitetu, o którym mowa w art. 42 ust. 3 rozporządzenia (UE) nr 165/2014,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Przedmiot i zakres stosowania

1. Niniejsze rozporządzenie ustanawia przepisy niezbędne do jednolitego stosowania następujących aspektów dotyczących tachografów:

a) zapisywanie położenia pojazdu w pewnych punktach podczas dziennego okresu pracy kierowcy;

b) wczesne wykrywanie na odległość możliwych przypadków manipulowania tachografami inteligentnymi lub ich niewłaściwego użytkowania;

c) interfejs do inteligentnych systemów transportowych;

d) wymogi administracyjne i techniczne dotyczące procedur homologacji typu dla tachografów, w tym mechanizmy zabezpieczające.

2. Budowa, sprawdzanie, instalacja, kontrola, użytkowanie i naprawa tachografów inteligentnych i ich elementów składowych muszą być zgodne z wymogami technicznymi określonymi w załączniku 1C do niniejszego rozporządzenia.

3. Tachografy inne niż tachografy inteligentne muszą nadal spełniać, jeśli chodzi o ich budowę, sprawdzanie, instalację, kontrolę, użytkowanie i naprawę, wymogi zawarte w załączniku 1 albo w załączniku 1B do rozporządzenia Rady (EWG) nr 3821/85 ([3]), stosownie do przypadku.

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1285/2013 z dnia 11 grudnia 2013 r. w sprawie realizacji i eksploatacji europejskich systemów nawigacji satelitarnej oraz uchylające rozporządzenie Rady (WE) nr 876/2002 i rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 683/2008 (Dz.U. L 347 z 20.12.2013, s. 1).

([2]) Rozporządzenie Komisji (WE) nr 68/2009 z dnia 23 stycznia 2009 r. dostosowujące do postępu technicznego po raz dziewiąty rozporządzenie Rady (EWG) nr 3821/85 w sprawie urządzeń rejestrujących stosowanych w transporcie drogowym (Dz.U. L 21 z 24.1.2009, s. 3).

([3]) Rozporządzenie Rady (EWG) nr 3821/85 z dnia 20 grudnia 1985 r. w sprawie urządzeń rejestrujących stosowanych w transporcie drogowym (Dz.U. L 370 z 31.12.1985, s. 8).

4. Zgodnie z art. 10d dyrektywy 96/53/WE, urządzenie wczesnego wykrywania na odległość musi również przekazywać dane dotyczące mas dostarczone przez wewnętrzny pokładowy system ważenia na potrzeby wczesnego wykrywania nadużyć.

Artykuł 2

Definicje

Do celów niniejszego rozporządzenia zastosowanie mają definicje zawarte w art. 2 rozporządzenia (UE) nr 165/2014.

Zastosowanie mają ponadto następujące definicje:

1) „tachograf cyfrowy" lub „tachograf pierwszej generacji" oznacza tachograf cyfrowy inny niż tachograf inteligentny;

2) „urządzenie zewnętrzne GNSS" oznacza urządzenie, które zawiera odbiornik GNSS, jeżeli przyrząd rejestrujący nie jest pojedynczym urządzeniem, a także inne elementy składowe niezbędne do ochrony przekazywania danych o położeniu reszcie przyrządu rejestrującego;

3) „folder informacyjny" oznacza pełny folder, w formie elektronicznej lub papierowej, zawierający wszystkie informacje dostarczone przez producenta lub jego przedstawiciela organowi udzielającemu homologacji typu na potrzeby homologacji typu tachografu lub jego elementu składowego, w tym certyfikaty, o których mowa w art. 12 ust. 3 rozporządzenia (UE) nr 165/2014, wyniki testów przewidzianych w załączniku 1C do niniejszego rozporządzenia, a także rysunki, fotografie i inne istotne dokumenty;

4) „pakiet informacyjny" oznacza folder informacyjny, w formie elektronicznej lub papierowej, któremu towarzyszą wszelkie inne dokumenty dodane przez organ udzielający homologacji typu do folderu informacyjnego w ramach wykonywania jego funkcji, w tym – na zakończenie procesu homologacji typu – świadectwo homologacji typu WE tachografu lub jego elementu składowego;

5) „indeks do pakietu informacyjnego" oznacza dokument zawierający numerowany spis treści pakietu informacyjnego, wskazujący wszystkie istotne części tego pakietu. Format tego dokumentu umożliwia rozróżnienie kolejnych etapów w procesie homologacji typu WE, w tym dat wszelkich rewizji i aktualizacji tego pakietu;

6) „urządzenie wczesnego wykrywania na odległość" oznacza urządzenie przyrządu rejestrującego, które jest używane do przeprowadzania ukierunkowanych kontroli drogowych;

7) „tachograf inteligentny" lub „tachograf drugiej generacji" oznacza tachograf cyfrowy spełniający wymogi art. 8, 9 i 10 rozporządzenia (UE) nr 165/2014 oraz załącznika 1C do niniejszego rozporządzenia;

8) „element składowy tachografu" lub „element składowy" oznacza dowolny z następujących elementów: przyrząd rejestrujący, czujnik ruchu, karta do tachografu, wykresówka, urządzenie zewnętrzne GNSS oraz urządzenie wczesnego wykrywania na odległość;

9) „organ udzielający homologacji typu" oznacza organ państwa członkowskiego właściwy w sprawach przeprowadzania homologacji typu tachografu lub jego elementów składowych, procesu zatwierdzania, wydawania oraz – w stosownych przypadkach – cofania świadectw homologacji typu, który działa jako punkt kontaktowy dla organów udzielających homologacji typu innych państw członkowskich oraz dopilnowuje, aby producenci wypełniali swoje obowiązki dotyczące zapewnienia zgodności z wymogami niniejszego rozporządzenia.

Artykuł 3

Usługi w zakresie lokalizacji

1. Producenci muszą zapewnić kompatybilność tachografów inteligentnych z usługami określania pozycji świadczonymi przez system Galileo i europejski system wspomagania satelitarnego („EGNOS").

2. Oprócz systemów, o których mowa w ust. 1, producenci mogą również postanowić o zapewnieniu kompatybilności z innymi systemami nawigacji satelitarnej.

Artykuł 4

Procedura homologacji typu tachografu i elementów składowych tachografu

1. Producent lub jego przedstawiciel składa wniosek o udzielenie homologacji typu dla tachografu lub jego dowolnego elementu składowego, bądź grupy elementów składowych, do organu udzielającego homologacji typu wyznaczonego przez dane państwo członkowskie. Obejmuje on folder informacyjny zawierający informacje na temat każdego z odpowiednich elementów składowych, w tym – w stosownych przypadkach – świadectwa homologacji typu innych elementów składowych niezbędnych dla kompletności tachografu, jak również wszelkie inne istotne dokumenty.

2. Państwo członkowskie udziela homologacji typu dla każdego tachografu, elementu składowego lub grupy elementów składowych, który(-a) spełnia wymogi administracyjne i techniczne określone w art. 1 ust. 2 lub 3, stosownie do przypadku. W takim przypadku organ udzielający homologacji typu wydaje wnioskodawcy świadectwo homologacji typu zgodne ze wzorem określonym w załączniku II do niniejszego rozporządzenia.

3. Organ udzielający homologacji typu może zażądać od producenta lub jego przedstawiciela dostarczenia wszelkich dodatkowych informacji.

4. Producent lub jego przedstawiciel udostępnia organom udzielającym homologacji typu, jak również podmiotom odpowiedzialnym za wydawanie certyfikatów, o których mowa w art. 12 ust. 3 rozporządzenia (UE) nr 165/2014, taką liczbę tachografów lub elementów składowych tachografu, jaka jest niezbędna, aby umożliwić przeprowadzenie procedury homologacji typu w satysfakcjonujący sposób.

5. Jeżeli producent lub jego przedstawiciel ubiega się o homologację typu niektórych elementów składowych lub grup elementów składowych tachografu, musi dostarczyć organom udzielającym homologacji typu inne elementy składowe, które uzyskały już homologację typu, a także inne części niezbędne do zbudowania kompletnego tachografu, aby umożliwić tym organom przeprowadzenie niezbędnych badań.

Artykuł 5

Modyfikacje homologacji typu

1. Producent lub jego przedstawiciel informuje niezwłocznie organy udzielające homologacji typu, które udzieliły pierwotnej homologacji typu, o wszelkich modyfikacjach oprogramowania lub sprzętu tachografu bądź charakteru materiałów użytych do jego produkcji, które zostały odnotowane w pakiecie informacyjnym, i składa wniosek o modyfikację homologacji typu.

2. Organy udzielające homologacji typu mogą dokonać rewizji lub rozszerzenia dotychczasowej homologacji typu albo wydać nową homologację typu w zależności od rodzaju i właściwości tych modyfikacji.

„Rewizja" ma miejsce, jeżeli organ udzielający homologacji typu uzna, że modyfikacje oprogramowania lub sprzętu tachografu, bądź rodzaju materiałów użytych do jego produkcji, są niewielkie. W takich przypadkach organ udzielający homologacji typu wydaje zrewidowane dokumenty pakietu informacyjnego, wskazując rodzaj dokonanych modyfikacji i datę ich zatwierdzenia. Zaktualizowana wersja pakietu informacyjnego w formie skonsolidowanej, której towarzyszy szczegółowy opis dokonanych modyfikacji, jest wystarczająca do spełnienia tego wymogu.

„Rozszerzenie" ma miejsce, jeżeli organ udzielający homologacji typu uzna, że modyfikacje oprogramowania lub sprzętu tachografu, bądź rodzaju materiałów użytych do jego produkcji, są istotne. W takich przypadkach Komisja może zwrócić się o przeprowadzenie nowych badań i poinformować o tym odpowiednio producenta lub jego upoważnionego przedstawiciela. Jeśli wyniki tych badań okażą się zadowalające, organ udzielający homologacji typu wydaje zrewidowane świadectwo homologacji typu, które zawiera numer odnoszący się do udzielonego rozszerzenia. Świadectwo homologacji typu wskazuje powód rozszerzenia oraz datę jego wydania.

3. Indeks do pakietu informacyjnego wskazuje datę ostatniego rozszerzenia lub rewizji homologacji typu, bądź datę ostatniej konsolidacji zaktualizowanej wersji homologacji typu.

4. Nowa homologacja typu jest konieczna, jeżeli wnioskowane modyfikacje tachografu lub jego elementów składowych posiadających homologację typu prowadziłyby do wydania nowego świadectwa bezpieczeństwa lub interoperacyjności.

Artykuł 6

Wejście w życie

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie stosuje się od dnia 2 marca 2016 r.

Załączniki stosuje się jednak od dnia 2 marca 2019 r., z wyjątkiem dodatku 16, który stosuje się od dnia 2 marca 2016 r.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 18 marca 2016 r.

W imieniu Komisji
Jean-Claude JUNCKER
Przewodniczący

ZAŁĄCZNIK I C

Wymagania w zakresie budowy, badań, instalacji i kontroli

WPROWADZENIE

Pierwsza generacja tachografów cyfrowych jest w użyciu od 1 maja 2006 r. Można z nich korzystać do czasu wycofania z eksploatacji w transporcie krajowym. 15 lat po wejściu w życie niniejszego rozporządzenia Komisji wszystkie pojazdy w transporcie międzynarodowym muszą być wyposażone w zgodne z przepisami tachografy inteligentne drugiej generacji, wprowadzone niniejszym rozporządzeniem.

Niniejszy załącznik zawiera wymagania dotyczące drugiej generacji urządzeń rejestrujących i kart do tachografów. Począwszy od daty wprowadzenia, w pojazdach rejestrowanych po raz pierwszy instaluje się urządzenia rejestrujące drugiej generacji i wydaje się karty do tachografów drugiej generacji.

Aby wprowadzenie systemu tachografów drugiej generacji przebiegło płynnie:

— karty do tachografów drugiej generacji zaprojektowane są w taki sposób, aby możliwe było ich używanie również w przyrządach rejestrujących pierwszej generacji,

— wraz z datą wprowadzenia nie wymaga się wymiany ważnych kart do tachografów pierwszej generacji.

Pozwoli to kierowcom na zachowanie jednej karty kierowcy, z której będą mogli korzystać w obu systemach.

Urządzenia rejestrujące drugiej generacji są natomiast kalibrowane tylko z użyciem kart warsztatowych drugiej generacji.

Niniejszy załącznik zawiera wszelkie wymogi związane z interoperacyjnością między pierwszą a drugą generacją systemu tachografów.

Dodatek 15 zawiera dodatkowe szczegółowe informacje dotyczące zarządzania współistnieniem dwóch systemów.

Wykaz dodatków

1 DEFINICJE

W niniejszym załączniku:

a) „aktywacja" oznacza:

fazę, gdy tachograf uzyskuje pełną funkcjonalność i uruchamia wszystkie funkcje, łącznie z funkcjami zabezpieczającymi, z wykorzystaniem karty warsztatowej;

b) „uwierzytelnienie"oznacza:

funkcję służącą ustanowieniu i kontroli tożsamości;

c) „autentyczność"oznacza:

właściwość polegającą na tym, że informacje przychodzą od strony, której tożsamość można zweryfikować;

d) „test wbudowany (BIT)"oznacza:

testy wykonywane na żądanie, uruchamiane przez operatora lub urządzenia zewnętrzne;

e) „dzień kalendarzowy" oznacza:

dzień zaczynający się o godzinie 00:00 i kończący o godzinie 24:00. Wszystkie dni kalendarzowe odnoszą się do czasu UTC (uniwersalny czas koordynowany);

f) „kalibracja" tachografu inteligentnego oznacza:

aktualizację lub potwierdzenie parametrów pojazdu przechowywanych w pamięci danych. Parametry pojazdu obejmują identyfikację pojazdu (numery VIN, VRN i kod rejestrującego państwa członkowskiego) i charakterystyki pojazdu, (w, k, l, wielkość opon, ustawienia urządzenia ograniczenia prędkości (w stosownych przypadkach), bieżący czas UTC, bieżąca wartość licznika kilometrów); podczas kalibracji urządzenia rejestrującego w pamięci danych zachowywane są również rodzaje i identyfikatory odpowiednich plomb homologacyjnych;

aktualizację lub potwierdzenie jedynie czasu UTC uważa się za korektę czasu, a nie za kalibrację, pod warunkiem że nie jest to sprzeczne z wymaganiem 409;

do kalibracji urządzenia rejestrującego niezbędna jest karta warsztatowa;

g) „numer karty"oznacza:

numer składający się z 16 znaków alfanumerycznych, który jednoznacznie identyfikuje kartę do tachografów w państwie członkowskim. Numer karty zawiera (w stosownych przypadkach) numer kolejny karty, numer wymiany karty i numer odnowienia karty;

tym samym karta jest jednoznacznie zidentyfikowana przez kod państwa członkowskiego wydającego i numer karty;

h) „numer kolejny karty"oznacza:

14. znak alfanumeryczny w numerze karty, który umożliwia rozróżnianie różnych kart firmie, warsztatowi lub organowi kontrolnemu uprawnionym do otrzymania kilku kart do tachografów. Firmę, warsztat lub organ kontrolny jednoznacznie identyfikuje pierwszych 13 znaków numeru karty;

i) „numer odnowienia karty"oznacza:

16. znak alfanumeryczny w numerze karty, który jest zmieniany przyrostowo przy każdym odnowieniu karty do tachografów;

j) „numer wymiany karty"oznacza:

15. znak alfanumeryczny w numerze karty, który jest zmieniany przyrostowo przy każdej wymianie karty do tachografów;

k) „współczynnik charakterystyczny pojazdu"oznacza:

wielkość liczbową określającą wartość sygnału dostarczanego przez część pojazdu podłączoną do urządzenia rejestrującego (wał główny skrzyni biegów lub oś) w czasie, gdy pojazd przebywa drogę o długości jednego kilometra mierzoną w normalnych warunkach testowych, zgodnie z definicją w wymaganiu 414. Współczynnik charakterystyczny pojazdu podaje się w impulsach na kilometr (w =… imp/km);

l) „karta firmowa" oznacza:

kartę do tachografu wydaną przez organy państwa członkowskiego przedsiębiorstwu transportowemu używającemu pojazdów wyposażonych w tachografy, która identyfikuje to przedsiębiorstwo transportowe i pozwala na wyświetlanie, pobieranie i drukowanie danych zapisanych w tachografie, który został zabezpieczony blokadą przez to przedsiębiorstwo transportowe;

m) „stała urządzenia rejestrującego" oznacza:

wielkość liczbową określającą wartość sygnału wejściowego wymaganą do wskazania i rejestracji przebytej odległości jednego kilometra; stała ta jest wyrażona w impulsach na kilometr (k =…imp/km);

n) „nieprzerwany czas prowadzenia pojazdu" obliczany jest przez urządzenie rejestrujące w następujący sposób ([1]):

nieprzerwany czas prowadzenia pojazdu obliczany jest jako bieżące, skumulowane czasy prowadzenia pojazdu przez danego kierowcę od końca jego ostatniego 45-minutowego lub dłuższego okresu GOTOWOŚCI lub PRZERWY/ODPOCZYNKU lub NIEOKREŚLONEGO ([2]) (okres ten może być rozbity zgodnie z rozporządzeniem (WE) nr 561/2006 Parlamentu Europejskiego i Rady ([3])). W obliczeniach uwzględnia się, stosownie do okoliczności, wcześniejsze czynności zapisane na karcie kierowcy. Jeżeli kierowca nie włoży swojej karty, obliczenia wykonuje się na podstawie znajdujących się w pamięci danych zapisów dla bieżącego okresu, w którym nie było włożonej karty, i dla stosownego czytnika;

o) „karta kontrolna" oznacza:

kartę do tachografu wydaną krajowemu właściwemu organowi kontrolnemu przez organy państwa członkowskiego, która identyfikuje organ kontrolny i fakultatywnie funkcjonariusza służb kontrolnych oraz umożliwia dostęp do danych zapisanych w pamięci danych lub na kartach kierowcy i fakultatywnie na kartach warsztatowych w celu odczytu, wydruku lub pobrania danych;

Daje ona również dostęp do funkcji kontroli drogowej kalibracji oraz do danych na czytniku wczesnego wykrywania na odległość.

p) **„skumulowany czas przerwy" obliczany jest przez urządzenie rejestrujące w następujący sposób** ([1])**:**

skumulowany czas przerwy w prowadzeniu pojazdu obliczany jest jako bieżące, zakumulowane, 15-minutowe lub dłuższe okresy GOTOWOŚCI lub PRZERWY/ODPOCZYNKU lub NIEOKREŚLONE ([2]) dla danego kierowcy, od końca jego ostatniego 45-minutowego lub dłuższego okresu GOTOWOŚCI lub PRZERWY/ODPOCZYNKU lub NIEOKREŚLONEGO ([2]) (okres ten może być rozbity zgodnie z rozporządzeniem (WE) nr 561/2006).

W obliczeniach uwzględnia się, stosownie do okoliczności, wcześniejsze czynności zapisane na karcie kierowcy. Do obliczeń nie bierze się nieokreślonych okresów o ujemnym czasie trwania (początek nieokreślonego okresu > koniec nieokreślonego okresu) wynikłych z nakładania się czasów z dwóch różnych urządzeń rejestrujących.

Jeżeli kierowca nie włoży swojej karty, obliczenia wykonuje się na podstawie znajdujących się w pamięci danych zapisów dla bieżącego okresu, w którym nie było włożonej karty, i dla stosownego czytnika.

([1]) Ten sposób obliczania nieprzerwanego czasu prowadzenia pojazdu oraz skumulowanego czasu przerwy służy urządzeniu rejestrującemu do obliczenia ostrzeżenia o nieprzerwanym czasie prowadzenia. Nie przesądza on o prawnej interpretacji tych czasów. Można stosować alternatywne sposoby obliczania nieprzerwanego czasu prowadzenia pojazdu i skumulowanego czasu przerw w celu zastąpienia niniejszych definicji, jeżeli definicje te stały się nieaktualne w wyniku nowelizacji innych stosownych przepisów.

([2]) Okresy NIEOKREŚLONE odpowiadają okresom, gdy karta kierowcy nie jest włożona do urządzenia rejestrującego, oraz w których nie dokonano ręcznej rejestracji czynności kierowcy.

([3]) Rozporządzenie (WE) nr 561/2006 Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie harmonizacji niektórych przepisów socjalnych odnoszących się do transportu drogowego oraz zmieniające rozporządzenia Rady (EWG) nr 3821/85 i (WE) 2135/98, jak również uchylające rozporządzenie Rady (EWG) nr 3820/85 (Dz.U. L 102 z 11.4.2006, s. 1).

q) „pamięć danych" oznacza:

elektroniczne urządzenie przechowywania danych wbudowane w urządzenie rejestrujące;

r) „podpis cyfrowy" oznacza:

dane dołączone do bloku danych lub kryptograficzne przekształcenie bloku danych, które umożliwiają odbiorcy bloku danych potwierdzenie autentyczności oraz integralności danego bloku danych;

s) „pobieranie" oznacza:

kopiowanie, wraz z podpisem cyfrowym, części lub kompletnego zestawu pliku danych zapisanych w pamięci danych przyrządu rejestrującego lub w pamięci karty do tachografu, pod warunkiem że proces ten nie zmienia ani nie usuwa żadnych zapisanych danych;

Producenci przyrządów rejestrujących tachografów inteligentnych oraz producenci urządzeń skonstruowanych i przeznaczonych do pobierania zbiorów danych podejmują wszelkie racjonalne działania zapewniające pobieranie takich danych przez przedsiębiorstwa transportowe lub kierowców z minimalnym opóźnieniem.

Pobieranie danych z pliku zawierającego dane szczegółowe dotyczące prędkości nie jest konieczne do celów zgodności z rozporządzeniem (WE) nr 561/2006, ale może być wykorzystane do innych celów, takich jak dochodzenie w sprawie wypadku;

t) „karta kierowcy" oznacza:

kartę do tachografu, która identyfikuje kierowcę i umożliwia przechowywanie danych dotyczących czynności kierowcy, wydaną konkretnemu kierowcy przez organy państwa członkowskiego;

u) „obwód toczny kół" oznacza:

wartość średnią długości drogi przebytej przez każde z kół (napędowych) poruszającego się pojazdu podczas jednego pełnego obrotu. Pomiar tych długości drogi jest wykonywany w normalnych warunkach testowych zgodnie z definicją w wymaganiu 414 i wyrażony jest w postaci „l = … mm". Producenci pojazdów mogą zastąpić pomiar odległości obliczeniem teoretycznym, w którym uwzględnia się rozkład ciężaru na osie dla pojazdu bez obciążenia w stanie gotowym do jazdy ([1]). Metody takiego obliczenia teoretycznego podlegają zatwierdzeniu przez właściwy organ państwa członkowskiego i mogą mieć miejsce tylko przed aktywacją tachografu;

v) „zdarzenie" oznacza:

odbiegające od normy działanie wykryte przez tachograf inteligentny, które może być spowodowane próbą oszustwa;

w) „urządzenie zewnętrzne GNSS" oznacza:

urządzenie, które zawiera odbiornik GNSS, jeżeli przyrząd rejestrujący nie jest pojedynczą jednostką oraz inne elementy niezbędne do ochrony przekazywania danych dotyczących pozycji do pozostałej części przyrządu rejestrującego;

x) „usterka" oznacza:

odbiegające od normy działanie wykryte przez tachograf inteligentny, które może być spowodowane wadliwą pracą lub awarią urządzeń;

y) „odbiornik GNSS" oznacza:

urządzenie elektroniczne, które odbiera i cyfrowo przetwarza sygnały z co najmniej jednego globalnego systemu nawigacji satelitarnej (ang. *GNSS*) w celu uzyskania informacji o pozycji, prędkości i czasie.

z) „instalacja" oznacza:

montaż tachografu w pojeździe;

([1]) Rozporządzenie Komisji (UE) nr 1230/2012 z dnia 12 grudnia 2012 r. w sprawie wykonania rozporządzenia (WE) nr 661/2009 Parlamentu Europejskiego i Rady w odniesieniu do wymagań w zakresie homologacji typu dotyczących mas i wymiarów pojazdów silnikowych oraz zmieniające dyrektywę 2007/46/WE Parlamentu Europejskiego i Rady (Dz.U. L 353 z 21.12.2012, s. 31), z późniejszymi zmianami.

aa) „interoperacyjność" oznacza:

zdolność systemów oraz będących ich podstawą procesów gospodarczych do wymiany danych oraz do wymiany informacji;

bb) „interfejs" oznacza:

połączenie między systemami, które zapewnia mechanizmy, za których pośrednictwem systemy te mogą się łączyć i wchodzić w interakcję;

cc) „pozycja" oznacza:

współrzędne geograficzne pojazdu w danym momencie;

dd) „czujnik ruchu" oznacza:

część tachografu dostarczającą sygnał odzwierciedlający prędkość pojazdu lub przebytą drogę;

ee) „karta nieważna" oznacza:

kartę wykrytą jako wadliwa lub kartę, której wstępne uwierzytelnienie nie jest możliwe lub której okres ważności jeszcze się nie rozpoczął lub już upłynął;

ff) „otwarty standard" oznacza:

standard określony w dokumencie specyfikacji standardów dostępnym bezpłatnie lub za symboliczną opłatą, który może być kopiowany, rozpowszechniany lub wykorzystywany bezpłatnie lub za symboliczną opłatą;

gg) „poza zakresem" oznacza:

że zgodnie z przepisami rozporządzenia (WE) nr 561/2006 użycie urządzenia rejestrującego nie jest wymagane;

hh) „przekroczenie prędkości" oznacza:

przekroczenie dozwolonej prędkości pojazdu definiowane jako dowolny przynajmniej 60-sekundowy okres, w którym zmierzona prędkość pojazdu przekracza wartość ograniczenia dla urządzenia ograniczenia prędkości ustanowioną w dyrektywie Rady 92/6/EWG z dnia 10 lutego 1992 r. w sprawie montowania i zastosowania urządzeń ograniczenia prędkości w niektórych kategoriach pojazdów silnikowych we Wspólnocie [1], z późniejszymi zmianami;

ii) „przegląd okresowy"oznacza:

zespół czynności wykonywanych w celu sprawdzenia, czy tachograf pracuje prawidłowo, czy jego ustawienia odpowiadają parametrom pojazdu i czy do tachografu nie podłączono urządzeń manipulacyjnych;

jj) „drukarka" oznacza:

element składowy urządzenia rejestrującego wykonujący wydruki danych zapisanych w pamięci;

kk) „wczesne wykrywanie na odległość" oznacza:

łączność między urządzeniem wczesnego wykrywania na odległość a czytnikiem wczesnego wykrywania na odległość podczas ukierunkowanych kontroli drogowych, mającą na celu zdalne wykrycie ewentualnych manipulacji lub niewłaściwego użycia urządzenia rejestrującego;

ll) „urządzenie do łączności na odległość" oznacza:

wyposażenie przyrządu rejestrującego, które jest używane do przeprowadzania ukierunkowanych kontroli drogowych;

[1] Dyrektywa Rady 92/6/EWG z dnia 10 lutego 1992 r. w sprawie montowania i zastosowania urządzeń ograniczenia prędkości w niektórych kategoriach pojazdów silnikowych we Wspólnocie (Dz.U. L 57 z 2.3.1992, s. 27).

mm) „czytnik wczesnego wykrywania na odległość" oznacza:

system stosowany przez funkcjonariuszy służb kontrolnych do ukierunkowanych kontroli drogowych;

nn) „odnowienie" oznacza:

wydanie nowej karty do tachografu po upływie terminu ważności dotychczasowej karty lub w przypadku nieprawidłowego działania karty i zwrócenia jej organowi wydającemu kartę. Odnowienie jest zawsze gwarancją, że dwie ważne karty nie współistnieją;

oo) „naprawa" oznacza:

każdą naprawę czujnika ruchu lub przyrządu rejestrującego lub przewodu, wymagającą odłączenia zasilania lub odłączenia od innych elementów składowych tachografu lub otwarcia czujnika ruchu lub przyrządu rejestrującego;

pp) „wymiana karty"oznacza:

wydanie karty do tachografu w celu zastąpienia dotychczasowej karty, której utratę, kradzież lub wadliwe działanie zgłoszono i której nie zwrócono organowi, który wydał kartę. Wymiana zawsze wiąże się z ryzykiem, że mogą współistnieć dwie ważne karty;

qq) „certyfikacja bezpieczeństwa" oznacza:

procedurę polegającą na potwierdzeniu przez jednostkę certyfikującą wspólnych kryteriów, że badane urządzenie rejestrujące (lub jego element składowy) lub karta do tachografu spełniają wymogi bezpieczeństwa określone w odpowiednich profilach zabezpieczenia;

rr) „autotest" oznacza:

testy wykonywane okresowo i automatycznie przez urządzenie rejestrujące w celu wykrycia usterek;

ss) „pomiar czasu" oznacza:

trwały cyfrowy zapis uniwersalnej daty koordynowanej i uniwersalnego czasu koordynowanego (UTC);

tt) „korekta czasu" oznacza:

automatyczną korektę bieżącego czasu dokonywaną w regularnych odstępach i z tolerancją maksymalnie jednej minuty lub korektę dokonaną podczas kalibracji;

uu) „rozmiar opon" oznacza:

oznaczenie wymiarów opon (na zewnętrznych kołach napędowych) zgodne z dyrektywą Rady 92/23/EWG z dnia 31 marca 1992 r. ([1]) z późniejszymi zmianami;

vv) „identyfikacja pojazdu" oznacza:

numery identyfikujące pojazd: numer rejestracyjny pojazdu (VRN) z oznaczeniem państwa członkowskiego rejestracji i numer identyfikacyjny pojazdu (VIN) ([2]);

ww) na potrzeby obliczeniowe w urządzeniu rejestrującym „tydzień"oznacza:

okres między godziną 00.00 UTC w poniedziałek a 24.00 UTC w niedzielę;

([1]) Dyrektywa Rady 92/23/EWG z dnia 31 marca 1992 r. odnosząca się do opon pojazdów silnikowych i ich przyczep oraz ich instalowania (Dz.U. L 129 z 14.5.1992, s. 95).

([2]) Dyrektywa Rady z dnia 18 grudnia 1975 r. w sprawie zbliżania ustawodawstw Państw Członkowskich odnoszących się do tabliczek znamionowych i oznakowania identyfikacyjnego pojazdów silnikowych i ich przyczep oraz sposobu i miejsca ich umieszczania (Dz.U. L 24 z 30.1.1976, s. 1).

xx) „karta warsztatowa" oznacza:

kartę do tachografu wydaną przez organy państwa członkowskiego wyznaczonemu personelowi producenta tachografu, instalatorowi, producentowi pojazdu lub warsztatowi zatwierdzonemu przez to państwo członkowskie, która identyfikuje posiadacza karty i umożliwia testowanie, kalibrację i aktywację tachografów lub pobieranie z nich danych;

yy) „adapter" oznacza:

urządzenie dostarczające sygnał w sposób ciągły odwzorowujący prędkość pojazdu lub przebytą drogę, inne niż urządzenie stosowane do niezależnego wykrywania ruchu, oraz:

— które jest zainstalowane i stosowane wyłącznie w pojazdach kategorii M1 i N1 (określonych w załączniku II do dyrektywy Rady 2007/46/WE Parlamentu Europejskiego i Rady ([1]) z późniejszymi zmianami) dopuszczonych do ruchu od dnia 1 maja 2006 r.,

— które jest zainstalowane w miejscu, w którym z mechanicznego punktu widzenia niemożliwy jest montaż stosowanych czujników ruchu innego rodzaju, pod innym względem zgodnych z wymaganiami przedstawionymi w niniejszym załączniku i w dodatkach 1–15 do niniejszego załącznika,

— które jest zainstalowane między przyrządem rejestrującym a miejscem, gdzie generowane są impulsy prędkości/drogi przez zintegrowane czujniki lub alternatywne interfejsy,

— z punktu widzenia przyrządu rejestrującego zachowanie adaptera jest takie samo jak czujnika ruchu zgodnego z wymaganiami w niniejszym załączniku i w dodatkach 1–16 do niniejszego załącznika, w przypadku podłączenia go do przyrządu rejestrującego;

zastosowanie takiego adaptera w wymienionych wyżej pojazdach musi umożliwiać montaż i poprawne zastosowanie przyrządu rejestrującego, zgodnego ze wszystkimi wymaganiami niniejszego załącznika,

w przypadku tych pojazdów tachograf inteligentny obejmuje przewody, adapter i przyrząd rejestrujący;

zz) „integralność danych" oznacza:

dokładność i spójność przechowywanych danych, których potwierdzeniem jest brak jakichkolwiek zmian w danych między dwoma aktualizacjami rekordu danych. Integralność oznacza, że dane są dokładną kopią wersji oryginalnej, np. że nie zostały zniekształcone w trakcie zapisu na karcie do tachografu lub urządzeniu dedykowanym lub w trakcie odczytu z nich lub w trakcie transmisji za pośrednictwem dowolnego kanału komunikacji;

aaa) „prywatność danych" oznacza:

ogólne środki techniczne podjęte w celu zapewnienia właściwego wdrożenia zasad określonych w dyrektywie 95/46/WE Parlamentu Europejskiego i Rady ([2]), a także zasad określonych w dyrektywie 2002/58/WE Parlamentu Europejskiego i Rady ([3]);

bbb) „system tachografu inteligentnego" oznacza:

urządzenia rejestrujące, karty do tachografów oraz zestaw wszelkich urządzeń współdziałających bezpośrednio lub pośrednio podczas ich budowy, instalacji, użytkowania, testowania i kontroli, takich jak karty, czytniki na odległość i wszelkie inne urządzenia do pobierania danych, analizy danych, kalibracji, generowania i wprowadzania elementów zabezpieczeń lub zarządzania tymi elementami itp.;

ccc) data wprowadzenia:

36 miesięcy po wejściu w życie szczegółowych przepisów, o których mowa w art. 11 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 165/2014 ([4]).

([1]) Dyrektywa 2007/46/WE Parlamentu Europejskiego i Rady z dnia 5 września 2007 r. ustanawiająca ramy dla homologacji pojazdów silnikowych i ich przyczep oraz układów, części i oddzielnych zespołów technicznych przeznaczonych do tych pojazdów (dyrektywa ramowa) (Dz.U. L 263 z 9.10.2007, s.1).

([2]) Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. L 281 z 23.11.1995, s. 31).

([3]) Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (Dz.U. L 201 z 31.7.2002, s. 37).

([4]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 165/2014 z dnia 4 lutego 2014 r. w sprawie tachografów stosowanych w transporcie drogowym i uchylające rozporządzenie Rady (EWG) nr 3821/85 w sprawie urządzeń rejestrujących stosowanych w transporcie drogowym oraz zmieniające rozporządzenie (WE) nr 561/2006 Parlamentu Europejskiego i Rady w sprawie harmonizacji niektórych przepisów socjalnych odnoszących się do transportu drogowego (Dz.U. L 60 z 28.2.2014, s. 1).

Jest to data, po której rejestrowane po raz pierwszy pojazdy:

— *muszą być wyposażone w tachograf podłączony do usługi określania pozycji opartej na systemie nawigacji satelitarnej,*

— *muszą mieć możliwość przekazywania danych właściwym organom kontrolnym na potrzeby ukierunkowanych kontroli drogowych podczas ruchu pojazdu.*

— *oraz mogą być wyposażone w znormalizowane interfejsy pozwalające na wykorzystywanie przez urządzenie zewnętrzne danych rejestrowanych lub generowanych przez tachografy w trybie operacyjnym.*

ddd) „profil zabezpieczenia" oznacza:

dokument używany w ramach procesu certyfikacyjnego zgodnie ze wspólnymi kryteriami, który określa niezależne od wdrożenia specyfikacje wymogów bezpieczeństwa w zakresie zabezpieczania informacji;

eee) dokładność GNSS:

w zapisywaniu pozycji z globalnego systemu nawigacji satelitarnej (GNSS) z użyciem tachografów, oznacza wartość Horizontal Dilution of Precision (HDOP) obliczaną jako najniższa z wartości HDOP pobranych z dostępnych systemów GNSS.

2 CHARAKTERYSTYKA OGÓLNA I FUNKCJE URZĄDZEŃ REJESTRUJĄCYCH

2.1 **Charakterystyka ogólna**

Celem urządzenia rejestrującego jest rejestrowanie, przechowywanie, wyświetlanie, drukowanie i wyprowadzanie danych związanych z czynnościami kierowcy.

Pojazd wyposażony w urządzenie rejestrujące spełniające wymagania niniejszego załącznika musi mieć prędkościomierz i licznik kilometrów. Funkcje te może spełniać urządzenie rejestrujące.

01) Urządzenie rejestrujące składa się z przewodów, czujnika ruchu i przyrządu rejestrującego.

02) Interfejs między czujnikami ruchu i przyrządami rejestrującymi musi być zgodny z wymogami określonymi w dodatku 11.

03) Przyrząd rejestrujący musi być podłączony do globalnego(-ych) systemu(-ów) nawigacji satelitarnej, jak określono w dodatku 12.

04) Przyrząd rejestrujący musi łączyć się z czytnikami wczesnego wykrywania na odległość, jak określono w dodatku 14.

05) Przyrząd rejestrujący może obejmować interfejs ITS, który został określony w dodatku 13.

Urządzenie rejestrujące może być podłączone do innych urządzeń poprzez dodatkowe interfejsy lub poprzez opcjonalny interfejs ITS.

06) Zawarcie w urządzeniu rejestrującym lub przyłączenie do niego jakiejkolwiek funkcji, urządzenia lub urządzeń, zatwierdzonych lub nie, nie może zakłócać, ani potencjalnie zakłócać, prawidłowego i bezpiecznego działania urządzenia rejestrującego ani uchybiać przepisom niniejszego rozporządzenia.

Użytkowników urządzenia rejestrującego identyfikują w sprzęcie ich karty do tachografów.

07) Urządzenie rejestrujące zapewnia selektywne prawa dostępu do danych i funkcji zależnie od rodzaju lub tożsamości użytkownika.

Urządzenie rejestrujące rejestruje i przechowuje dane w pamięci danych, w urządzeniu do łączności na odległość i na kartach do tachografów.

Odbywa się to zgodnie z dyrektywą 95/46/WE z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych [1], dyrektywą 2002/58/WE z dnia 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej [2] oraz zgodnie z art. 7 rozporządzenia (UE) nr 165/2014.

2.2 **Funkcje**

08) Urządzenie rejestrujące realizuje następujące funkcje:

— monitorowanie wkładania i wyjmowania kart,

— pomiar prędkości, odległości i pozycji,

— pomiar czasu,

— monitorowanie czynności kierowcy,

— monitorowanie stanu prowadzenia pojazdu,

— dane wprowadzane ręcznie przez kierowcę:

  — wprowadzanie miejsca rozpoczęcia lub zakończenia okresu pracy,

  — ręczne wprowadzanie danych o czynnościach kierowcy,

  — warunki szczególne,

— zarządzanie blokadami firmowymi,

— monitorowanie czynności kontrolnych,

— wykrywanie zdarzeń lub usterek,

— testy wbudowane i autotesty,

— odczyt z pamięci danych,

— rejestrowanie i przechowywanie w pamięci danych,

— odczyt z kart do tachografów,

— rejestrowanie i przechowywanie na kartach do tachografów,

— wyświetlanie,

— drukowanie,

— ostrzeganie,

— pobieranie danych na nośniki zewnętrzne,

— łączność na odległość na potrzeby ukierunkowanych kontroli drogowych,

— wyprowadzanie danych do dodatkowych urządzeń,

— kalibracja,

— kontrola drogowa kalibracji

— korekta czasu.

[1] Dz.U. L 281 z 23.11.1995, s. 31.
[2] Dz.U. L 201 z 31.7.2002, s. 37.

2.3 **Tryby pracy**

09) Urządzenie rejestrujące może pracować w czterech trybach pracy:

— tryb eksploatacyjny,

— tryb kontrolny,

— tryb kalibracyjny,

— tryb firmowy.

10) Urządzenie rejestrujące przełącza się do następujących trybów pracy zależnie od rodzaju ważnej karty do tachografów włożonej do czytników kart. Do określenia trybu pracy nie jest istotna generacja karty do tachografu, pod warunkiem że włożona karta jest ważna. Karta warsztatowa pierwszej generacji będzie zawsze uznawana za nieważną, jeżeli zostanie włożona do przyrządu rejestracyjnego drugiej generacji.

Tryb pracy		Czytnik karty kierowcy				
		Brak karty	Karta kierowcy	Karta kontrolna	Karta warsztatowa	Karta firmowa
Czytnik karty współkierowcy	Brak karty	eksploatacyjny	eksploatacyjny	kontrolny	kalibracyjny	firmowy
	Karta kierowcy	eksploatacyjny	eksploatacyjny	kontrolny	kalibracyjny	firmowy
	Karta kontrolna	kontrolny	kontrolny	kontrolny (*)	eksploatacyjny	eksploatacyjny
	Karta warsztatowa	kalibracyjny	kalibracyjny	eksploatacyjny	kalibracyjny (*)	eksploatacyjny
	Karta firmowa	firmowy	firmowy	eksploatacyjny	eksploatacyjny	firmowy (*)

(*) W tych sytuacjach urządzenie rejestrujące korzysta tylko z karty do tachografów w czytniku kierowcy.

11) Urządzenie rejestrujące ignoruje włożone karty nieważne, z wyjątkiem tego, że możliwe jest wyświetlanie, drukowanie lub pobieranie danych zgromadzonych na kartach, których termin ważności minął.

12) Wszystkie funkcje wymienione w 2.2. działają w każdym trybie pracy z następującymi wyjątkami:

— funkcja kalibracji dostępna jest tylko w trybie kalibracyjnym,

— funkcja kontroli drogowej kalibracji dostępna jest tylko w trybie kontrolnym,

— funkcja zarządzania blokadami firmowymi dostępna jest tylko w trybie firmowym,

— funkcja monitorowania czynności kontrolnych dostępna jest tylko w trybie kontrolnym,

— funkcja pobierania danych nie jest dostępna w trybie eksploatacyjnym, z wyjątkiem przypadków w wymaganiu 193 i z wyjątkiem pobierania danych z karty kierowcy, gdy żadna inna karta nie jest włożona do przyrządu rejestrującego.

13) Urządzenie rejestrujące może wyprowadzać dane na wyświetlacz, do drukarki lub interfejsów zewnętrznych z następującymi wyjątkami:

— w trybie eksploatacyjnym wszystkie dane identyfikujące osoby (nazwisko i imię/imiona) nieodpowiadające włożonej karcie do tachografu są wygaszone, a numer karty nieodpowiadający włożonej karcie do tachografu jest częściowo wygaszony (wszystkie nieparzyste znaki od lewej do prawej są wygaszone),

— w trybie firmowym, dane dotyczące kierowcy (wymagania 102, 105 i 108) mogą być wyprowadzane tylko dla okresów, w których nie ma żadnej blokady ani żadna inna firma nie założyła blokady (określona pierwszymi 13 cyframi numeru karty firmowej),

— przy braku karty w czytniku urządzenia rejestrującego dane dotyczące kierowcy mogą być wyprowadzane tylko dla bieżącego dnia kalendarzowego i 8 poprzednich dni kalendarzowych,

— dane osobowe pochodzące z przyrządu rejestrującego nie mogą być wyprowadzane poprzez interfejs ITS przyrządu, o ile nie sprawdzono, że zgodził się na to kierowca, którego dane dotyczą,

— normalny okres ważności operacji przyrządów rejestrujących wynosi 15 lat, począwszy od daty wydania świadectwa przyrządu rejestrującego, ale przyrządy rejestrujące mogą być wykorzystane przez kolejne 3 miesiące wyłącznie do pobierania danych.

2.4 **Zabezpieczenia**

Celem zabezpieczenia systemu jest taka ochrona pamięci danych, by uniemożliwić nieautoryzowany dostęp i manipulowanie danymi oraz wykrycie wszelkich takich prób, ochrona integralności i autentyczności danych wymienianych między czujnikiem ruchu a przyrządem rejestrującym, ochrona integralności i autentyczności danych wymienianych między urządzeniem rejestrującym a kartami do tachografów, ochrona integralności i autentyczności danych wymienianych między urządzeniem rejestrującym a urządzeniem zewnętrznym GNSS, ochrona poufności, integralności i autentyczności danych wymienianych w ramach wczesnego wykrywania na odległość na potrzeby kontroli oraz sprawdzenie integralności i autentyczności pobieranych danych.

14) W celu osiągnięcia bezpieczeństwa systemu, następujące elementy składowe muszą spełniać wymogi bezpieczeństwa określone w ich profilach zabezpieczenia, zgodnie z wymaganiami w dodatku 10:

— przyrząd rejestrujący,

— karta do tachografu,

— czujnik ruchu,

— urządzenie zewnętrzne GNSS (profil ten jest tylko konieczny i stosowany do zewnętrznego wariantu GNSS).

3 WYMAGANIA KONSTRUKCYJNE I FUNKCJONALNE URZĄDZEŃ REJESTRUJĄCYCH

3.1 **Monitorowanie wkładania i wyjmowania kart**

15) Urządzenie rejestrujące monitoruje czytniki kart w celu wykrycia wkładania i wyjmowania kart.

16) Po włożeniu karty urządzenie rejestrujące sprawdza, czy włożona karta jest ważną kartą do tachografu i w przypadku ważnej karty sprawdza typ i generację karty.

Jeżeli do urządzenia rejestrującego włożona już była karta o tym samym numerze karty i wyższym numerze odnowienia, karta jest zgłaszana jako nieważna.

Jeżeli do urządzenia rejestrującego włożona już była karta o tym samym numerze karty i numerze odnowienia, ale wyższym numerze wymiany, karta jest zgłaszana jako nieważna.

17) Karty do tachografu pierwszej generacji są uznawane przez urządzenie rejestrujące za nieważne, po tym jak możliwość korzystania z kart do tachografu pierwszej generacji została wyłączona przez warsztat, zgodnie z dodatkiem 15 (wym. MIG003).

18) Karty warsztatowe pierwszej generacji wkładane do urządzeń rejestrujących drugiej generacji są uznawane za nieważne.

19) Urządzenie rejestrujące musi być skonstruowane tak, aby po prawidłowym włożeniu do czytnika kart do tachografów były one blokowane we właściwej pozycji.

20) Odblokowanie kart do tachografów jest możliwe tylko przy zatrzymanym pojeździe i po zapisaniu odpowiednich danych na kartach. Odblokowanie karty wymaga wykonania przez użytkownika odpowiedniej czynności.

3.2 **Pomiar prędkości, pozycji i odległości**

21) Czujnik ruchu (ewentualnie wbudowany w adapter) jest głównym źródłem pomiaru prędkości i odległości.

22) Funkcja ta nieprzerwanie mierzy i dostarcza wartość stanu licznika kilometrów odpowiadającą całkowitej drodze przebytej przez pojazd za pomocą impulsów przekazywanych przez czujnik ruchu.

23) Funkcja ta nieprzerwanie mierzy i dostarcza wartość prędkości pojazdu za pomocą impulsów przekazywanych przez czujnik ruchu.

24) Funkcja pomiaru prędkości podaje także informacje o tym, czy pojazd porusza się, czy stoi. Uznaje się, że pojazd porusza się, gdy funkcja ta wykrywa więcej niż 1 impuls na sekundę z czujnika ruchu przez co najmniej 5 sekund, w przeciwnym razie uważa się, że pojazd stoi.

25) Urządzenia do pokazywania prędkości (prędkościomierz) i łącznej drogi przebytej (licznik kilometrów) zainstalowane w pojeździe wyposażonym w urządzenie rejestrujące, spełniające wymagania niniejszego rozporządzenia, spełniają wymagania odnośnie do maksymalnych tolerancji (zob. 3.2.1 i 3.2.2) określone w niniejszym załączniku.

26) W celu wykrycia manipulowania danymi dotyczącymi ruchu informacje z czujnika ruchu są potwierdzane przez informacje dotyczące ruchu pojazdu pochodzące z odbiornika GNSS i opcjonalnie z innych źródeł niezależnych od czujnika ruchu.

27) Funkcja ta mierzy pozycję pojazdu w celu umożliwienia automatycznej rejestracji:

— pozycji, w których kierowca lub współkierowca rozpoczynają dzienny okres pracy;

— pozycji, w których nieprzerwany czas prowadzenia pojazdu przez kierowcę osiągnie wielokrotność trzech godzin;

— pozycji, w których kierowca lub współkierowca kończą dzienny okres pracy;

3.2.1 *Pomiar przebytej drogi*

28) Długość przebytej drogi może być mierzona, gdy pojazd porusza się:

— do przodu i do tyłu, albo

— tylko do przodu.

29) Urządzenie rejestrujące mierzy odległość w zakresie 0–9 999 999,9 km.

30) Pomiar odległości jest wykonywany z następującą dokładnością (odległości co najmniej 1 000 m):

— ± 1 % przed instalacją,

— ± 2 % po instalacji i przeglądzie okresowym,

— ± 4 % podczas eksploatacji.

31) Pomiar odległości jest wykonywany z rozdzielczością co najmniej 0,1 km lub większą.

3.2.2 *Pomiar prędkości*

32) Urządzenie rejestrujące mierzy prędkość w zakresie od 0 do 220 km/h.

33) W celu zapewnienia maksymalnej tolerancji wskazywanej prędkości ± 6 km/h podczas eksploatacji i uwzględniając:

— tolerancję ± 2 km/h na zmiany sygnału wejściowego (zmiany opon, …),

— tolerancję ± 1 km/h dla pomiarów wykonywanych w czasie instalacji lub przeglądów okresowych,

urządzenie rejestrujące, dla zakresu prędkości między 20 a 180 km/h i dla współczynników charakterystycznych pojazdu między 4 000 a 25 000 impulsów na km, mierzy prędkość z dokładnością ± 1 km/godz. (przy stałej prędkości).

Uwaga: Rozdzielczość przechowywania danych wprowadza dodatkową tolerancję ± 0,5 km/h do prędkości zapisanej przez urządzenie rejestrujące.

34) Prędkość jest mierzona prawidłowo w zakresie normalnych tolerancji w czasie nie dłuższym niż 2 sekundy od zakończenia zmiany prędkości, jeżeli prędkość zmieniła się w tempie 2 m/s^2.

35) Pomiar prędkości jest wykonywany z dokładnością co najmniej 1 km/h lub wyższą.

3.2.3 *Pomiar pozycji*

36) Urządzenie rejestrujące mierzy bezwzględną pozycję pojazdu za pomocą odbiornika GNSS.

37) Bezwzględną pozycję mierzy się we współrzędnych szerokości i długości geograficznej, w stopniach i minutach, z dokładnością do 1/10 minuty.

3.3 **Pomiar czasu**

38) Funkcja pomiaru czasu mierzy czas nieprzerwanie i cyfrowo podaje czas UTC.

39) Do datowania w urządzeniu rejestrującym (rejestracja, wymiana danych) i do wszystkich wydruków wymienionych w dodatku 4 „Wydruki" używany jest czas UTC.

40) W celu wizualizacji czasu lokalnego możliwa jest zmiana przesunięcia wyświetlanego czasu skokowo co pół godziny. Nie dopuszcza się innych przesunięć poza przesunięciami wstecz lub do przodu o wielokrotność połowy godziny;

41) Dryft czasu musi mieścić się w granicach ± 2 sek. dziennie w warunkach homologacyjnych, przy braku korekty czasu.

42) Pomiar czasu jest wykonywany z dokładnością co najmniej 1 sekundy lub większą.

43) Odcięcie zewnętrznego źródła zasilania na czas nie krótszy niż 12 miesięcy w warunkach homologacyjnych nie może wpływać na pomiar czasu.

3.4 **Monitorowanie czynności kierowcy**

44) Funkcja ta nieprzerwanie i odrębnie monitoruje czynności jednego kierowcy i jednego współkierowcy.

45) Czynnościami kierowcy są PROWADZENIE, PRACA, GOTOWOŚĆ lub PRZERWA/ODPOCZYNEK.

46) Kierowca lub współkierowca mogą ręcznie wybierać PRACĘ, GOTOWOŚĆ lub PRZERWĘ/ODPOCZYNEK.

47) Gdy pojazd porusza się następuje automatyczne wybór czynności PROWADZENIE dla kierowcy i GOTOWOŚĆ dla współkierowcy.

48) Gdy pojazd zatrzymuje się, następuje automatyczne wybranie czynności PRACA dla kierowcy.

49) Jeżeli w czasie 120 sekund od automatycznej zmiany na PRACĘ, wskutek zatrzymania pojazdu, nastąpi zmiana czynności na ODPOCZYNEK lub GOTOWOŚĆ, przyjmuje się, że pierwsza taka zmiana zaistniała w czasie postoju pojazdu (w ten sposób można anulować zmianę czynności na PRACA).

50) Funkcja ta przekazuje zmiany czynności do funkcji rejestrującej w odstępach co jedną minutę.

51) W danej minucie zegarowej, jeżeli PROWADZENIE jest zarejestrowane jako czynność w minucie bezpośrednio ją poprzedzającej i następującej bezpośrednio po niej, to cała ta minuta liczy się jako PROWADZENIE.

52) W danej minucie zegarowej, nietraktowanej jako PROWADZENIE zgodnie z wymaganiem 051, cała taka minuta liczy się jako jedna czynność, która trwała najdłużej w ciągu tej minuty (lub była najpóźniejsza w przypadku czynności o jednakowym czasie trwania).

53) Funkcja ta także nieprzerwanie monitoruje zarówno nieprzerwany czas prowadzenia pojazdu, jak i skumulowany czas przerwy dla kierowcy.

3.5 **Monitorowanie stanu prowadzenia pojazdu**

54) Funkcja ta nieprzerwanie i automatycznie monitoruje stan prowadzenia pojazdu.

55) Po włożeniu dwóch ważnych kart kierowcy wybierany jest stan prowadzenia pojazdu ZAŁOGA, w każdym innym przypadku wybierany jest stan prowadzenia pojazdu JEDEN KIEROWCA.

3.6 **Dane wprowadzane przez kierowców**

3.6.1 *Wprowadzanie miejsca rozpoczęcia lub zakończenia okresu pracy*

56) Funkcja ta umożliwia wprowadzanie miejsc, gdzie według kierowcy lub współkierowcy rozpoczyna się lub kończy dzienny okres pracy.

57) Miejsca definiuje się jako kraj i dodatkowo, w stosownych przypadkach, region; są one wprowadzane lub potwierdzane ręcznie.

58) W chwili wyjęcia karty kierowcy urządzenie rejestrujące sygnalizuje, że oczekuje od (współ)kierowcy wprowadzenia „miejsca zakończenia dziennego okresu pracy".

59) Kierowca wprowadza wówczas bieżące miejsce pojazdu, a wpis ten uznaje się za tymczasowy.

60) Możliwe jest wprowadzenie miejsca rozpoczęcia lub zakończenia dziennego okresu pracy przez wybranie polecenia w menu. Jeżeli w ciągu jednej minuty zegarowej wydane zostaje więcej poleceń niż jedno, zarejestrowane zostaje tylko ostatnie miejsce rozpoczęcia i ostatnie miejsce zakończenia wybrane w tym czasie.

3.6.2 *Ręczne wprowadzanie czynności kierowcy i zgoda kierowcy na interfejs ITS*

61) Po włożeniu karty kierowcy (lub warsztatowej), i tylko w tym czasie, urządzenie rejestrujące umożliwia ręczne wprowadzanie czynności. Ręczne wprowadzanie czynności wykonuje się, stosując lokalny czas i datę strefy czasowej (przesunięcie UTC) aktualnie ustawione w przyrządzie rejestrującym.

Po włożeniu karty kierowcy lub warsztatowej przyrząd rejestrujący przypomina posiadaczowi karty:

— datę i godzinę ostatniego wyjęcia jego karty;

— opcjonalnie: przesunięcie czasu lokalnego aktualnie ustawionego w przyrządzie rejestrującym.

Przy pierwszym włożeniu danej karty kierowcy lub warsztatowej, nieznanej przyrządowi rejestrującemu, posiadacz karty jest proszony o wyrażenie zgody na wyprowadzenie danych osobowych związanych z tachografem poprzez opcjonalny interfejs ITS.

W dowolnym momencie istnieje możliwość potwierdzenia lub wycofania zgody kierowcy (ew. warsztatu) przez wybranie polecenia w menu, pod warunkiem że karta kierowcy (lub warsztatowa) jest włożona.

Wprowadzanie czynności jest możliwe z następującymi ograniczeniami:

— rodzajem czynności musi być PRACA, GOTOWOŚĆ lub PRZERWA/ODPOCZYNEK;

— godzina rozpoczęcia i zakończenia każdej czynności zawarta jest wyłącznie w okresie między ostatnim wyjęciem a obecnym włożeniem karty;

— niedopuszczalne jest nakładanie się na siebie w czasie okresów wykonywania tych czynności.

W razie potrzeby możliwe jest ręczne wprowadzanie czynności przy pierwszym włożeniu uprzednio nieużywanej karty kierowcy (lub warsztatowej).

Procedura ręcznego wprowadzania czynności zawiera tyle kolejnych etapów, ile jest konieczne do ustawienia rodzaju każdej czynności, godziny jej rozpoczęcia i godziny jej zakończenia. Dla całego okresu między ostatnim wyjęciem a obecnym włożeniem karty posiadacz karty może nie zgłaszać żadnej czynności.

Podczas ręcznego wprowadzania danych związanego z włożeniem karty, posiadacz karty ma, w stosownych przypadkach, możliwość wprowadzenia:

— miejsca, w którym zakończył się poprzedni dzienny okres pracy powiązany z odnośnym czasem (czyli nadpisania wpisu przy ostatnim wyjęciu karty),

— miejsca, w którym rozpoczyna się obecny dzienny okres pracy powiązany z odnośnym czasem.

Jeżeli posiadacz karty nie wprowadzi miejsca rozpoczęcia lub zakończenia okresu pracy podczas ręcznego wprowadzania danych związanego z włożeniem karty, będzie to równoważne z potwierdzeniem, że okres pracy nie zmienił się od ostatniego wyjęcia karty. Kolejne wprowadzenie miejsca zakończenia poprzedniego dziennego okresu pracy nadpisze wówczas wpis tymczasowy wprowadzony przy ostatnim wyjęciu karty.

Jeżeli wprowadza się miejsce, rejestruje się je na stosownej karcie do tachografu.

Ręczne wprowadzanie zostaje przerwane, jeżeli:

— karta zostaje wyjęta lub

— pojazd porusza się i karta znajduje się w czytniku karty kierowcy.

Dozwolone są dodatkowe przerwy, np. przekroczenie dozwolonego czasu po pewnym okresie braku aktywności użytkownika. Jeżeli ręczne wprowadzanie zostanie przerwane, urządzenie rejestrujące dokonuje walidacji wszystkich kompletnych miejsc i czynności (mających przypisane jednoznaczne miejsce i godzinę lub rodzaj czynności, godzinę rozpoczęcia i godzinę zakończenia).

Jeżeli podczas ręcznego wprowadzania czynności dla wcześniej włożonej karty zostanie włożona karta drugiego kierowcy lub karta warsztatowa, dopuszcza się uzupełnienie ręcznego wprowadzania dla karty włożonej wcześniej przed rozpoczęciem ręcznego wprowadzania dla drugiej karty.

Posiadacz karty ma możliwość ręcznego wprowadzenia zgodnie z następującą procedurą minimalną:

— Ręczne wprowadzenie czynności w kolejności chronologicznej w okresie między ostatnim wyjęciem a obecnym włożeniem karty.

— Godzina rozpoczęcia pierwszej czynności jest ustawiona na godzinę wyjęcia karty. Dla każdego kolejnego zapisu godzina rozpoczęcia jest wstępnie ustawiona tak, aby następowała bezpośrednio po godzinie zakończenia poprzedniego zapisu. Rodzaj czynności i godzinę zakończenia wybiera się dla każdej czynności.

Procedura kończy się, gdy godzina zakończenia ręcznie wprowadzanej czynności pokrywa się z godziną włożenia karty. Urządzenie rejestrujące umożliwia opcjonalnie posiadaczowi karty modyfikowanie ręcznie wprowadzonej czynności aż do zatwierdzenia przez wybranie odpowiedniego polecenia. W późniejszym czasie wprowadzenie takich zmian jest zabronione.

3.6.3 *Wprowadzanie warunków szczególnych*

62) Urządzenie rejestrujące umożliwia kierowcy wprowadzenie w czasie rzeczywistym następujących dwóch warunków szczególnych:

— „POZA ZAKRESEM" (początek, koniec)

— „PRZEPRAWA PROMOWA / PRZEJAZD KOLEJOWY" (początek, koniec).

Jeżeli wybrany jest warunek „POZA ZAKRESEM", nie może równocześnie występować warunek „PRZEPRAWA PROMOWA / PRZEJAZD KOLEJOWY".

Włożenie lub wyjęcie karty kierowcy powoduje automatycznie zakończenie wybranego stanu „POZA ZAKRESEM".

Wybrany stan „POZA ZAKRESEM" blokuje następujące zdarzenia i ostrzeżenia:

— prowadzenie pojazdu bez prawidłowej karty,

— ostrzeżenia związane z nieprzerwanym czasem prowadzenia pojazdu.

Znacznik rozpoczęcia PRZEPRAWY PROMOWEJ / PRZEJAZDU KOLEJOWEGO ustawia się przed wyłączeniem silnika na promie/w pociągu.

Zamknięcie otwartego stanu PRZEPRAWA PROMOWA / PRZEJAZD KOLEJOWY musi nastąpić, jeżeli wystąpi jedna z następujących sytuacji:

— kierowca ręcznie kończy stan PRZEPRAWA PROMOWA / PRZEJAZD KOLEJOWY;

— kierowca wyjmuje swoją kartę.

Otwarty stan PRZEPRAWA PROMOWA / PRZEJAZD KOLEJOWY kończy się w momencie, gdy przystaje być on ważny na podstawie zasad określonych w rozporządzeniu (WE) nr 561/2006.

3.7 **Zarządzanie blokadami firmowymi**

63) Funkcja ta umożliwia zarządzanie blokadami umieszczanymi przez firmę w celu ograniczenia dostępu do danych, gdy urządzenie pracuje w trybie firmowym.

64) Blokady firmowe polegają na ustawieniu daty/godziny rozpoczęcia (włączenie blokady) i daty/godziny zakończenia (zwolnienie blokady) związanych z identyfikacją firmy pobraną z numeru karty firmowej (przy włączeniu blokady).

65) Blokady można włączać i zwalniać tylko w czasie rzeczywistym.

66) Blokadę może zwolnić tylko ta firma, która ją włączyła (identyfikowana na podstawie pierwszych 13 cyfr numeru karty firmowej), lub

67) Zwolnienie następuje automatycznie po włączeniu blokady przez inną firmę.

68) W przypadku gdy firma włącza blokadę, a poprzednia blokada była włączona przez tę samą firmę, przyjmuje się, że poprzednia blokada nie została zwolniona i nadal jest włączona.

3.8 **Monitorowanie czynności kontrolnych**

69) Funkcja ta monitoruje wykonywane w trybie kontrolnym czynności WYŚWIETLANIA, DRUKOWANIA, POBIERANIA DANYCH z przyrządu rejestrującego i karty oraz KONTROLI DROGOWEJ KALIBRACJI.

70) Funkcja ta również monitoruje KONTROLE PRZEKROCZENIA PRĘDKOŚCI wykonywane w trybie kontrolnym. Uznaje się, że kontrola przekroczenia prędkości została przeprowadzona, gdy w trybie kontrolnym komunikat „przekroczenie prędkości" zostaje wysłany do drukarki lub wyświetlony na monitorze, lub gdy dane o „zdarzeniach i usterkach" zostały pobrane z pamięci danych przyrządu rejestrującego.

3.9 **Wykrywanie zdarzeń lub usterek**

71) Funkcja ta wykrywa następujące zdarzenia lub usterki:

3.9.1 *Zdarzenie „włożenie nieważnej karty"*

72) Zdarzenie to uruchamiane jest przez włożenie nieważnej karty, włożenie karty kierowcy, która została wymieniona, lub wygaśnięcie ważności włożonej, ważnej karty.

3.9.2 *Zdarzenie „konflikt kart"*

73) Zdarzenie to uruchamiane jest przez każdą kombinację ważnych kart zaznaczoną X w tabeli poniżej:

Konflikt kart		Czytnik karty kierowcy				
		Brak karty	Karta kierowcy	Karta kontrolna	Karta warsztatowa	Karta firmowa
Czytnik karty współkierowcy	Brak karty					
	Karta kierowcy				X	
	Karta kontrolna			X	X	X
	Karta warsztatowa		X	X	X	X
	Karta firmowa			X	X	X

3.9.3 *Zdarzenie„nakładające się czasy*

74) Zdarzenie to uruchamiane jest w sytuacji, gdy data/godzina ostatniego wyjęcia karty kierowcy, odczytana z karty, jest późniejsza niż bieżąca data/godzina urządzenia rejestrującego, do którego karta jest wkładana.

3.9.4 *Zdarzenie „prowadzenie pojazdu bez prawidłowej karty"*

75) Zdarzenie to uruchamiane jest przez każdą kombinację ważnych kart do tachografów zaznaczoną X w poniższej tabeli, gdy czynność kierowcy zmienia się na PROWADZENIE lub w przypadku zmiany trybu pracy, w czasie gdy czynnością wykonywaną przez kierowcę jest PROWADZENIE:

Prowadzenie pojazdu bez prawidłowej karty		Czytnik karty kierowcy				
		Brak karty (lub karta nieważna)	Karta kierowcy	Karta kontrolna	Karta warsztatowa	Karta firmowa
Czytnik karty współkierowcy	Brak karty (lub karta nieważna)	X		X		X
	Karta kierowcy	X		X	X	X
	Karta kontrolna	X	X	X	X	X
	Karta warsztatowa	X	X	X		X
	Karta firmowa	X	X	X	X	X

3.9.5 *Zdarzenie „włożenie karty podczas prowadzenia pojazdu"*

76) Zdarzenie to uruchamia się, gdy do dowolnego czytnika włożona zostaje karta do tachografu, a czynnością kierowcy jest PROWADZENIE.

3.9.6 *Zdarzenie „Sesja ostatniej karty niezamknięta prawidłowo"*

77) Zdarzenie to uruchamia się, gdy przy wkładaniu karty urządzenie rejestrujące wykryje, że pomimo przepisów określonych w pkt 3.1 sesja poprzedniej karty nie została prawidłowo zamknięta (karta została wyjęta przed zapisaniem na karcie wszystkich wymaganych danych). Zdarzenie to uruchamiają tylko karty kierowcy i warsztatowe.

3.9.7 *Zdarzenie „przekroczenie prędkości"*

78) Zdarzenie to uruchamia się przy każdym przekroczeniu prędkości.

3.9.8 *Zdarzenie „przerwa w zasilaniu"*

79) Z wyjątkiem trybu kalibracyjnego lub kontrolnego, zdarzenie to uruchamia się w przypadku przekraczającej 200 ms przerwy w zasilaniu czujnika ruchu lub przyrządu rejestrującego. Wartość progową przerwy definiuje producent. Przerwa w zasilaniu spowodowana uruchamianiem silnika pojazdu nie może uruchamiać tego zdarzenia.

3.9.9 *Zdarzenie „błąd połączenia z urządzeniem do łączności na odległość"*

80) **Z wyjątkiem trybu kalibracyjnego**, zdarzenie to uruchamia się w przypadku gdy urządzenie do łączności na odległość nie potwierdza odbioru danych przesyłanych zdalnie z przyrządu rejestrującego podczas więcej niż trzech prób.

3.9.10 *Zdarzenie „brak informacji o pozycji z odbiornika GNSS"*

81) **Z wyjątkiem trybu kalibracyjnego**, zdarzenie to uruchamia się w przypadku braku informacji o pozycji pochodzących z odbiornika GNSS (wewnętrznego lub zewnętrznego) przez ponad trzy godziny skumulowanego czasu prowadzenia pojazdu.

3.9.11 *Zdarzenie „błąd połączenia z urządzeniem zewnętrznym GNSS"*

82) **Z wyjątkiem trybu kalibracyjnego**, zdarzenie to uruchamia się w przypadku przerwy w łączności między urządzeniem zewnętrznym GNSS a przyrządem rejestrującym przez ponad 20 kolejnych minut, kiedy pojazd jest w ruchu.

3.9.12 *Zdarzenie „błąd danych dotyczących ruchu"*

83) **Z wyjątkiem trybu kalibracyjnego**, zdarzenie to uruchamia się w przypadku przerwy w normalnym przepływie danych między czujnikiem ruchu a przyrządem rejestrującym lub w przypadku błędu integralności danych lub błędu uwierzytelnienia danych wymienianych między czujnikiem ruchu a przyrządem rejestrującym.

3.9.13 *Zdarzenie „konflikt ruchu pojazdu"*

84) **Z wyjątkiem trybu kalibracyjnego**, zdarzenie to uruchamia się, jeżeli informacje o ruchu z czujnika ruchu są sprzeczne z informacjami o ruchu obliczonymi z wewnętrznego odbiornika GNSS lub urządzenia zewnętrznego GNSS i ewentualnie z innych niezależnych źródeł, jak określono w dodatku 12. Zdarzenie to nie uruchamia się podczas przeprawy promowej lub przejazdu kolejowego, w przypadku stanu POZA ZAKRESEM, ani w razie niedostępności informacji o pozycji z odbiornika GNSS.

3.9.14 *Zdarzenie „próba naruszenia zabezpieczenia"*

85) Zdarzenie to uruchamiane jest przez każde inne zdarzenie naruszające zabezpieczenie czujnika ruchu lub przyrządu rejestrującego lub urządzenia zewnętrznego GNSS, zgodnie z wymogami w dodatku 10, z wyjątkiem trybu kalibracyjnego.

3.9.15 *Zdarzenie „konflikt czasu"*

86) **Z wyjątkiem trybu kalibracyjnego**, zdarzenie to uruchamia się, jeżeli przyrząd rejestrujący wykryje rozbieżność większą niż 1 min. między czasem określonym przez funkcję pomiaru czasu w przyrządzie rejestrującym a czasem pochodzącym z odbiornika GNSS. Wydarzenie to jest rejestrowane wraz z wartością zegara wewnętrznego przyrządu rejestrującego oraz z automatyczną korektą czasu. Po uruchomieniu zdarzenia konfliktu czasu przyrząd rejestrujący nie generuje innych zdarzeń konfliktu czasu przez kolejnych 12 godzin. Wydarzenie to nie uruchamia się, jeżeli odbiornik GNSS nie wykrywał prawidłowego sygnału GNSS w ciągu ostatnich 30 dni. Jednakże w momencie gdy informacja o pozycji z odbiornika GNSS stanie się ponownie dostępna, ma miejsce automatyczna korekta czasu.

3.9.16 *Usterka „karta"*

87) Usterkę tę uruchamia błąd karty do tachografu podczas pracy.

3.9.17 *Usterka „urządzenie rejestrujące"*

88) Usterkę tę uruchamia dowolny z następujących błędów, z wyjątkiem pracy w trybie kalibracyjnym:

— usterka wewnętrzna przyrządu rejestrującego

— usterka drukarki

— usterka wyświetlacza

— usterka pobierania danych

— usterka czujnika

— usterka odbiornika GNSS lub urządzenia zewnętrznego GNSS

— usterka urządzenia do łączności na odległość

3.10 **Testy wbudowane i autotesty**

89) Urządzenie rejestrujące samoczynnie wykrywa usterki, wykonując autotesty i testy wbudowane, zgodnie z poniższą tabelą:

Testowany podzespół	Autotest	Test wbudowany
Oprogramowanie		Integralność
Pamięć danych	Dostęp	Dostęp, integralność danych
Czytniki kart	Dostęp	Dostęp
Klawiatura		Kontrola ręczna
Drukarka	(w gestii producenta)	Wydruk
Wyświetlacz		Kontrola wzrokowa
Pobieranie danych (wykonywane tylko podczas pobierania)	Prawidłowa praca	
Czujnik	Prawidłowa praca	Prawidłowa praca
Urządzenie do łączności na odległość	Prawidłowa praca	Prawidłowa praca
Urządzenie GNSS	Prawidłowa praca	Prawidłowa praca

3.11 **Odczyt z pamięci danych**

90) Urządzenie rejestrujące umożliwia odczyt danych przechowywanych w jego pamięci danych.

3.12 **Rejestracja i przechowywanie w pamięci danych**

Do celów niniejszego pkt:

— „365 dni" definiuje się jako 365 dni kalendarzowych przeciętnych czynności wykonywanych przez kierowców w pojeździe. Przeciętne czynności na dzień w pojeździe definiuje się jako co najmniej 6 kierowców lub współkierowców, 6 cykli wkładania i wyjmowania karty i 256 zmian czynności. „365 dni" obejmuje zatem co najmniej 2 190 (współ)kierowców, 2 190 cykli wkładania i wyjmowania karty i 93 440 zmian czynności,

— średnia liczba pozycji na dzień jest definiowana jako co najmniej 6 pozycji, w których rozpoczyna się dzienny okres pracy, 6 pozycji, w których nieprzerwany czas prowadzenia pojazdu kierowcy osiąga wielokrotność trzech godzin oraz 6 pozycji, w których kończy się dzienny okres pracy, tak więc „365 dni" obejmuje co najmniej 6 570 pozycji,

— czas jest rejestrowany z dokładnością do jednej minuty, chyba że ustalono inaczej,

— stany licznika kilometrów rejestruje się z dokładnością do jednego kilometra,

— prędkości rejestruje się z dokładnością do 1 km/h,

— pozycje (szerokość i długość) rejestruje się w stopniach i minutach, z dokładnością do 1/10 minuty, z powiązaną dokładnością GNSS i czasem pobrania danych.

91) Odcięcie zewnętrznego źródła zasilania na czas krótszy niż dwanaście miesięcy, w warunkach homologacyjnych, nie może wpływać na dane przechowywane w pamięci danych. Ponadto odcięcie zasilania na czas krótszy niż 28 dni nie może mieć wpływu na dane przechowywane w zewnętrznym urządzeniu do łączności na odległość, zgodnie z definicją w dodatku 14.

92) Urządzenie rejestrujące umożliwia rejestrowanie, pośrednio lub bezpośrednio, w pamięci danych następujących informacji:

3.12.1 *Dane identyfikujące sprzęt*

3.12.1.1 Dane identyfikujące przyrząd rejestrujący

93) Urządzenie rejestrujące umożliwia przechowywanie w pamięci danych następujących danych identyfikujących przyrząd rejestrujący:

— nazwa producenta,

— adres producenta,

— numer części,

— numer seryjny,

— generacja przyrządu rejestrującego,

— możliwość korzystania z kart do tachografów pierwszej generacji,

— numer wersji oprogramowania,

— data instalacji wersji oprogramowania,

— rok produkcji urządzenia,

— numer homologacji,

94) Dane identyfikujące przyrząd rejestrujący są rejestrowane i zapisywane w pamięci definitywnie przez producenta przyrządu rejestrującego, z wyjątkiem danych dotyczących oprogramowania i numeru homologacji, które mogą zmieniać się w przypadku aktualizacji oprogramowania, oraz z wyjątkiem możliwości korzystania z kart do tachografów pierwszej generacji.

3.12.1.2 Dane identyfikujące czujnik ruchu

95) Czujnik ruchu umożliwia przechowywanie w pamięci następujących danych identyfikujących:

— nazwa producenta,

— numer seryjny,

— numer homologacji,

— identyfikator wbudowanego elementu zabezpieczenia (np. numer części wewnętrznego mikroprocesora),

— identyfikator systemu operacyjnego (np. numer wersji oprogramowania).

96) Dane identyfikujące czujnik ruchu są rejestrowane i zapisywane w czujniku ruchu definitywnie przez producenta czujnika ruchu.

97) Przyrząd rejestrujący musi mieć możliwość rejestrowania i zachowywania w pamięci następujących danych związanych z 20 ostatnimi sparowaniami czujników ruchu (jeżeli podczas jednego dnia kalendarzowego miało miejsce wiele sparowań, zachowywane jest tylko pierwsze i ostatnie z danego dnia):

Przy każdym sparowaniu rejestruje się następujące dane:

— dane identyfikujące czujnik ruchu:

— numer seryjny

— numer homologacji

— dane sparowania czujnika ruchu:

— data sparowania.

3.12.1.3 Dane identyfikujące globalnego systemu nawigacji satelitarnej

98) Urządzenie zewnętrzne GNSS umożliwia przechowywanie w pamięci następujących danych identyfikujących:

— nazwa producenta,

— numer seryjny,

— numer homologacji,

— identyfikator wbudowanego elementu zabezpieczenia (np. numer części wewnętrznego mikroprocesora),

— identyfikator systemu operacyjnego (np. numer wersji oprogramowania).

99) Dane identyfikujące są rejestrowane i zapisywane w urządzeniu zewnętrznym GNSS definitywnie przez producenta urządzenia zewnętrznego GNSS.

100) Przyrząd rejestrujący musi mieć możliwość rejestrowania i zachowywania w pamięci następujących danych związanych z 20 ostatnimi powiązaniami urządzeń zewnętrznych GNSS (jeżeli podczas jednego dnia kalendarzowego miało miejsce wiele powiązań, zachowywane jest tylko pierwsze i ostatnie z danego dnia).

Przy każdym powiązaniu rejestruje się następujące dane:

— dane identyfikujące urządzenia zewnętrznego GNSS:

— numer seryjny,

— numer homologacji,

— dane dotyczące powiązania z urządzeniem zewnętrznym GNSS:

— data powiązania.

3.12.2 *Klucze i certyfikaty*

101) Urządzenie rejestrujące umożliwia przechowywanie szeregu kluczy i certyfikatów kryptograficznych, jak określono w dodatku 11 część A i część B.

3.12.3 *Dane rejestrowane przy wkładaniu i wyjmowaniu karty kierowcy lub warsztatowej*

102) Przy każdym cyklu wkładania/wyjmowania karty kierowcy lub warsztatowej do urządzenia, urządzenie rejestrujące rejestruje i przechowuje w pamięci danych następujące informacje:

— nazwisko i imię (imiona) posiadacza karty zapisane na karcie,

— numer karty, państwo członkowskie wydające kartę i termin ważności zapisane na karcie,

— generację karty,

— datę i godzinę włożenia karty,

— stan licznika kilometrów przy wkładaniu karty,

— szczelinę czytnika, do której karta jest wkładana,

— datę i godzinę wyjęcia karty,

— stan licznika kilometrów przy wyjęciu karty,

— następujące informacje o poprzednim pojeździe używanym przez kierowcę, zapisane na karcie:

— numer VRN i państwo członkowskie rejestracji,

— generacja przyrządu rejestrującego (w razie dostępności),

— datę i godzinę wyjęcia karty,

— wskaźnik stanu pokazujący, czy przy wkładaniu karty posiadacz karty wprowadził ręcznie informacje o wykonywaniu czynności.

103) Pamięć danych wystarcza do przechowywania tych danych przez co najmniej 365 dni.

104) W przypadku zapełnienia pamięci danych nowe dane zastępują dane najstarsze.

3.12.4 *Dane dotyczące czynności kierowcy*

105) Urządzenie rejestrujące rejestruje i przechowuje w pamięci danych za każdym razem, kiedy następuje zmiana czynności kierowcy lub współkierowcy, lub za każdym razem, kiedy następuje zmiana stanu prowadzenia pojazdu, lub za każdym razem, kiedy następuje włożenie lub wyjęcie karty kierowcy lub karty warsztatowej:

— stan prowadzenia pojazdu (ZAŁOGA, JEDEN KIEROWCA),

— szczelinę czytnika (KIEROWCA, WSPÓŁKIEROWCA),

— status karty w odpowiedniej szczelinie czytnika kart (WŁOŻONA, NIEWŁOŻONA),

— czynność (PROWADZENIE, GOTOWOŚĆ, PRACA, PRZERWA/ODPOCZYNEK),

— datę i godzinę zmiany.

WŁOŻONA oznacza, że do czytnika jest włożona ważna karta kierowcy lub warsztatowa. NIEWŁOŻONA oznacza sytuację przeciwną, tzn. że do czytnika nie jest włożona ważna karta kierowcy ani warsztatowa (np. włożona jest karta firmowa lub brak jest karty).

Dane dotyczące czynności ręcznie wprowadzone przez kierowcę nie są rejestrowane w pamięci danych.

106) Pamięć danych wystarcza do przechowywania danych dotyczących czynności kierowcy przez co najmniej 365 dni.

107) W przypadku zapełnienia pamięci danych nowe dane zastępują dane najstarsze.

3.12.5 *Miejsca i pozycje, w których zaczynają się i kończą dzienne okresy pracy lub w których osiągnięto 3 godziny nieprzerwanego czasu prowadzenia pojazdu*

108) Urządzenie rejestrujące rejestruje i przechowuje w pamięci następujące dane:

— miejsca i pozycje, w których kierowca lub współkierowca rozpoczynają dzienny okres pracy;

— pozycje, w których nieprzerwany czas prowadzenia pojazdu przez kierowcę osiągnie wielokrotność trzech godzin;

— miejsca i pozycje, w których kierowca lub współkierowca kończą dzienny okres pracy;

109) Jeżeli w danym momencie pozycja pojazdu nie jest dostępna z odbiornika GNSS, urządzenie rejestrujące korzysta z ostatniej dostępnej pozycji i odpowiadającej jej daty i godziny.

110) Wraz z miejscem lub pozycją urządzenie rejestrujące rejestruje i przechowuje w pamięci następujące dane:

— numer karty (współ)kierowcy i państwo członkowskie wydające kartę,

— generację karty,

— datę i godzinę wpisu,

— rodzaj wpisu (rozpoczęcie, zakończenie lub 3 godziny nieprzerwanego czasu prowadzenia pojazdu),

— w stosownych przypadkach odpowiednią dokładność GNSS, datę i godzinę,

— stan licznika kilometrów.

111) Pamięć danych wystarcza do przechowywania miejsc i pozycji, w których zaczynają się i kończą dzienne okresy pracy lub w których osiągnięto 3 godziny nieprzerwanego czasu prowadzenia pojazdu, przez co najmniej 365 dni.

112) W przypadku zapełnienia pamięci danych nowe dane zastępują dane najstarsze.

3.12.6 *Dane dotyczące licznika kilometrów*

113) Urządzenie rejestrujące rejestruje w pamięci danych stan licznika kilometrów i odpowiednią datę o północy każdego dnia kalendarzowego.

114) Pamięć danych wystarcza do przechowywania danych dotyczących stanu licznika o północy przez co najmniej 365 dni kalendarzowych.

115) W przypadku zapełnienia pamięci danych nowe dane zastępują dane najstarsze.

3.12.7 *Dane szczegółowe dotyczące prędkości*

116) Urządzenie rejestrujące rejestruje i przechowuje w pamięci danych prędkość chwilową pojazdu wraz z datą i godziną, rejestrowane co sekundę przez okres co najmniej ostatnich 24 godzin, w których pojazd był w ruchu.

3.12.8 *Dane dotyczące zdarzeń*

Do celów niniejszego podpunktu czas rejestruje się z dokładnością do 1 sekundy.

117) Urządzenie rejestrujące rejestruje i przechowuje w pamięci danych następujące dane dla każdego zdarzenia wykrytego zgodnie z poniższymi zasadami przechowywania danych:

Zdarzenie	Zasady przechowywania	Dane rejestrowane dla zdarzenia
Włożenie nieważnej karty	— 10 ostatnich zdarzeń	— data i godzina zdarzenia — typ karty, numer, państwo członkowskie wydające kartę i generacja karty, która wywołała zdarzenie — liczba podobnych zdarzeń w tym dniu
Konflikt kart	— 10 ostatnich zdarzeń	— data i godzina początku zdarzenia — data i godzina końca zdarzenia — typ karty, numer, państwo członkowskie wydające kartę i generacja dwóch kart, które wywołały konflikt
Prowadzenie pojazdu bez prawidłowej karty	— najdłuższe zdarzenie w każdym z ostatnich 10 dni ich występowania — 5 najdłuższych zdarzeń w ciągu ostatnich 365 dni	— data i godzina początku zdarzenia — data i godzina końca zdarzenia — typ karty, numer, państwo członkowskie wydające kartę i generacja dla każdej karty wprowadzonej na początku lub pod koniec zdarzenia — liczba podobnych zdarzeń w tym dniu

Zdarzenie	Zasady przechowywania	Dane rejestrowane dla zdarzenia
Włożenie karty podczas jazdy	— ostatnie zdarzenie dla każdego z 10 ostatnich dni ich występowania	— data i godzina zdarzenia — typ karty, numer, państwo członkowskie wydające kartę i generacja — liczba podobnych zdarzeń w tym dniu
Sesja ostatniej karty niezamknięta prawidłowo	— 10 ostatnich zdarzeń	— data i godzina włożenia karty — typ karty, numer, państwo członkowskie wydające kartę i generacja — dane dotyczące ostatniej sesji odczytane z karty: — data i godzina włożenia karty — numer VRN, państwo członkowskie rejestracji i generacja przyrządu rejestrującego
Przekroczenie prędkości (1)	— najpoważniejsze zdarzenie dla każdego z 10 ostatnich dni od zaistnienia zdarzenia (tzn. zdarzenie o najwyższej przeciętnej prędkości) — 5 najpoważniejszych zdarzeń w ciągu ostatnich 365 dni — pierwsze zdarzenie zaistniałe po ostatniej kalibracji	— data i godzina początku zdarzenia — data i godzina końca zdarzenia — maksymalna prędkość zmierzona w czasie zdarzenia — średnia arytmetyczna prędkość zmierzona w czasie zdarzenia — typ karty, numer, państwo członkowskie wydające kartę i generacja karty kierowcy (w stosownych przypadkach) — liczba podobnych zdarzeń w tym dniu
Przerwa w zasilaniu (2)	— najdłuższe zdarzenie w każdym z ostatnich 10 dni ich występowania — 5 najdłuższych zdarzeń w ciągu ostatnich 365 dni	— data i godzina początku zdarzenia — data i godzina końca zdarzenia — typ karty, numer, państwo członkowskie wydające kartę i generacja dla każdej karty wprowadzonej na początku lub pod koniec zdarzenia — liczba podobnych zdarzeń w tym dniu
Błąd połączenia z urządzeniem do łączności na odległość	— najdłuższe zdarzenie w każdym z ostatnich 10 dni ich występowania — 5 najdłuższych zdarzeń w ciągu ostatnich 365 dni	— data i godzina początku zdarzenia — data i godzina końca zdarzenia — typ karty, numer, państwo członkowskie wydające kartę i generacja dla każdej karty wprowadzonej na początku lub pod koniec zdarzenia — liczba podobnych zdarzeń w tym dniu
Brak informacji o pozycji z odbiornika GNSS	— najdłuższe zdarzenie w każdym z ostatnich 10 dni ich występowania — 5 najdłuższych zdarzeń w ciągu ostatnich 365 dni	— data i godzina początku zdarzenia — data i godzina końca zdarzenia — typ karty, numer, państwo członkowskie wydające kartę i generacja dla każdej karty wprowadzonej na początku lub pod koniec zdarzenia — liczba podobnych zdarzeń w tym dniu

Zdarzenie	Zasady przechowywania	Dane rejestrowane dla zdarzenia
Błąd danych dotyczących ruchu	— najdłuższe zdarzenie w każdym z ostatnich 10 dni ich występowania — 5 najdłuższych zdarzeń w ciągu ostatnich 365 dni	— data i godzina początku zdarzenia — data i godzina końca zdarzenia — typ karty, numer, państwo członkowskie wydające kartę i generacja dla każdej karty wprowadzonej na początku lub pod koniec zdarzenia — liczba podobnych zdarzeń w tym dniu
Konflikt ruchu pojazdu	— najdłuższe zdarzenie w każdym z ostatnich 10 dni ich występowania — 5 najdłuższych zdarzeń w ciągu ostatnich 365 dni	— data i godzina początku zdarzenia — data i godzina końca zdarzenia — typ karty, numer, państwo członkowskie wydające kartę i generacja dla każdej karty wprowadzonej na początku lub pod koniec zdarzenia — liczba podobnych zdarzeń w tym dniu
Próba naruszenia zabezpieczenia	— 10 ostatnich zdarzeń wg typu zdarzenia	— data i godzina początku zdarzenia — data i godzina zakończenia zdarzenia (jeżeli jest istotna) — typ karty, numer, państwo członkowskie wydające kartę i generacja dla każdej karty wprowadzonej na początku lub pod koniec zdarzenia — typ zdarzenia
Konflikt czasu	— najdłuższe zdarzenie w każdym z ostatnich 10 dni ich występowania — 5 najdłuższych zdarzeń w ciągu ostatnich 365 dni	— data i godzina z urządzenia rejestrującego — data i godzina z GNSS, — typ karty, numer, państwo członkowskie wydające kartę i generacja dla każdej karty wprowadzonej na początku lub pod koniec zdarzenia — liczba podobnych zdarzeń w tym dniu

(1) Urządzenie rejestrujące rejestruje i przechowuje również w pamięci następujące dane:

— datę i godzinę ostatniej KONTROLI PRZEKROCZENIA PRĘDKOŚCI,

— datę i godzinę pierwszego przekroczenia prędkości po tej ostatniej KONTROLI PRZEKROCZENIA PRĘDKOŚCI.

— liczbę zdarzeń przekroczenia prędkości od ostatniej KONTROLI PRZEKROCZENIA PRĘDKOŚCI.

(2) Dane te mogą być rejestrowane wyłącznie po przywróceniu zasilania, czas może być znany z dokładnością do minuty.

3.12.9 *Dane dotyczące usterek*

Do celów niniejszego podpunktu czas rejestruje się z dokładnością do 1 sekundy.

118) Urządzenie rejestrujące próbuje rejestrować i przechowywać w pamięci danych następujące dane dla każdej wykrytej usterki zgodnie z następującymi zasadami przechowywania danych:

Usterka	Zasady przechowywania	Dane rejestrowane dla usterki
Usterka karty	— 10 ostatnich usterek karty kierowcy	— data i godzina początku usterki — data i godzina końca usterki — typ karty, numer, państwo członkowskie wydające kartę i generacja
Usterki urządzenia rejestrującego	— 10 ostatnich usterek dla każdego typu usterki — pierwsza usterka po ostatniej kalibracji	— data i godzina początku usterki — data i godzina końca usterki — rodzaj usterki — typ karty, numer, państwo członkowskie wydające kartę i generacja dla każdej karty wprowadzonej na początku lub pod koniec usterki

3.12.10 *Dane kalibracyjne*

119) Urządzenie rejestrujące rejestruje i przechowuje w pamięci następujące dane:

— parametry kalibracyjne znane w momencie aktywacji,

— pierwszą kalibrację po aktywacji urządzenia,

— pierwszą kalibrację w obecnym pojeździe (identyfikowanym numerem VIN),

— 20 ostatnich kalibracji (jeżeli w czasie jednego dnia kalendarzowego jest kilka kalibracji, zapamiętywana jest tylko pierwsza i ostatnia kalibracja z tego dnia).

120) Przy każdej z tych kalibracji rejestruje się następujące dane:

— cel kalibracji (aktywacja, pierwsza instalacja, instalacja, przegląd okresowy),

— nazwa i adres warsztatu,

— numer karty warsztatowej, państwo członkowskie wydające kartę i termin ważności karty,

— identyfikacja pojazdu,

— parametry uaktualnione lub potwierdzone: w, k, l, rozmiar opon, ustawienia urządzenia ograniczenia prędkości, licznik kilometrów (wartości stare i nowe), data i godzina (wartości stare i nowe),

— rodzaje i identyfikatory wszystkich założonych plomb.

121) Ponadto urządzenie rejestrujące rejestruje i przechowuje w pamięci danych zdolność do użytkowania kart do tachografów pierwszej generacji (aktywowaną lub nie).

122) Czujnik ruchu rejestruje i przechowuje w pamięci następujące dane instalacyjne czujnika ruchu:

— pierwsze sparowanie z przyrządem rejestrującym (data, godzina, numer homologacji przyrządu rejestrującego, numer seryjny przyrządu rejestrującego),

— ostatnie sparowanie z przyrządem rejestrującym (data, godzina, numer homologacji przyrządu rejestrującego, numer seryjny przyrządu rejestrującego).

123) Urządzenie zewnętrzne GNSS rejestruje i przechowuje w pamięci następujące dane instalacyjne urządzenia zewnętrznego GNSS:

— pierwsze powiązanie z przyrządem rejestrującym (data, godzina, numer homologacji przyrządu rejestrującego, numer seryjny przyrządu rejestrującego),

— ostatnie powiązanie z przyrządem rejestrującym (data, godzina, numer homologacji przyrządu rejestrującego, numer seryjny przyrządu rejestrującego).

3.12.11 *Dane dotyczące korekty czasu*

124) Urządzenie rejestrujące rejestruje i przechowuje w pamięci danych dane dotyczące korekty czasu przeprowadzonej w trybie kalibracyjnym, poza ramami regularnej kalibracji (def. f)):

— ostatnia korekta czasu,

— 5 największych korekt czasu.

125) Przy każdej z tych korekt czasu rejestruje się następujące dane:

— data i godzina, stara wartość,

— data i godzina, nowa wartość,

— nazwa i adres warsztatu,

— numer karty warsztatowej, państwo członkowskie wydające kartę, generacja karty i termin ważności karty.

3.12.12 *Dane dotyczące czynności kontrolnych*

126) Urządzenie rejestrujące rejestruje i przechowuje w pamięci danych następujące dane dotyczące ostatnich 20 czynności kontrolnych:

— data i godzina kontroli,

— numer karty kontrolnej, państwo członkowskie wydające kartę i generacja karty,

— rodzaj kontroli (wyświetlanie lub drukowanie lub pobieranie danych z przyrządu rejestrującego lub karty lub kontrola drogowa kalibracji).

127) W przypadku pobierania danych rejestruje się także daty najstarszych i najnowszych dni, z których dane są pobierane.

3.12.13 *Dane dotyczące blokad firmowych*

128) Urządzenie rejestrujące rejestruje i przechowuje w pamięci następujące dane dotyczące 255 ostatnich blokad firmowych:

— data i godzina założenia blokady,

— data i godzina zdjęcia blokady,

— numer karty firmowej, państwo członkowskie wydające kartę i generacja karty,

— nazwa i adres firmy.

Dane wcześniej zabezpieczone przez blokadę usunięte z pamięci z powodu powyższego ograniczenia traktuje się jako niezabezpieczone.

3.12.14 *Dane dotyczące pobierania danych*

129) Urządzenie rejestrujące rejestruje i przechowuje w pamięci danych następujące dane dotyczące ostatniego pobierania danych z pamięci urządzenia na nośnik zewnętrzny, wykonanego w trybie firmowym lub kalibracyjnym:

— data i godzina pobrania danych,

— numer karty firmowej lub warsztatowej, państwo członkowskie wydające kartę i generacja karty,

— nazwa firmy lub warsztatu.

3.12.15 *Dane dotyczące warunków szczególnych*

130) Urządzenie rejestrujące rejestruje i przechowuje w pamięci danych następujące dane dotyczące warunków szczególnych:

— data i godzina wprowadzenia danych,

— rodzaj warunku szczególnego.

131) Pamięć danych umożliwia przechowywanie danych dotyczących warunków szczególnych przez co najmniej 365 dni (przy założeniu, że przeciętnie otwiera się i zamyka jeden warunek dziennie). W przypadku zapełnienia pamięci danych nowe dane zastępują dane najstarsze.

3.12.16 *Dane karty do tachografu*

132) Urządzenie rejestrujące umożliwia przechowywanie następujących danych dotyczących różnych kart do tachografów, które zostały użyte w przyrządzie rejestrującym:

— numer karty do tachografu i jej numer seryjny,

— producent karty do tachografu,

— typ karty do tachografu,

— wersja karty do tachografu.

133) Urządzenie rejestrujące umożliwia przechowywanie co najmniej 88 takich rekordów danych.

3.13 **Odczyt kart do tachografów**

134) Urządzenie rejestrujące umożliwia odczyt z kart do tachografów pierwszej i drugiej generacji, w odpowiednich przypadkach, danych niezbędnych do:

— rozpoznania typu karty, posiadacza karty, wcześniej używanego pojazdu, daty i godziny ostatniego wyjęcia karty i czynności wybranej dla tego czasu,

— sprawdzenia, czy ostatnia sesja karty została prawidłowo zamknięta,

— wyliczenia dla kierowcy: nieprzerwanego czasu prowadzenia pojazdu, skumulowanego czasu przerwy i skumulowanego czasu prowadzenia za poprzedni i obecny tydzień,

— wydrukowania żądanych wydruków związanych z danymi zarejestrowanymi na karcie kierowcy,

— pobrania danych z karty kierowcy na zewnętrzny nośnik.

Wymóg ten ma zastosowanie tylko do kart do tachografów pierwszej generacji, jeżeli ich stosowanie nie zostało wyłączone przez warsztat.

135) W przypadku błędu odczytu urządzenie rejestrujące maksymalnie trzykrotnie powtarza to samo polecenie odczytu i w przypadku gdy odczyt nadal nie jest możliwy, uznaje kartę za uszkodzoną i nieważną.

3.14 **Rejestrowanie i przechowywanie danych na kartach do tachografów**

3.14.1 *Rejestrowanie i przechowywanie danych na kartach do tachografów pierwszej generacji*

136) O ile karty do tachografów pierwszej generacji nie zostały wyłączone przez warsztat, urządzenie rejestrujące rejestruje i przechowuje dane dokładnie w ten sam sposób co urządzenie rejestrujące pierwszej generacji.

137) Urządzenie rejestrujące ustawia „dane sesji karty" na karcie kierowcy lub warsztatowej bezpośrednio po włożeniu karty.

138) Urządzenie rejestrujące aktualizuje dane zapisane na ważnej karcie kierowcy, warsztatowej, firmowej lub kontrolnej, wprowadzając wszystkie niezbędne dane odnośnie do okresu, w którym karta pozostaje włożona, i odnośnie do posiadacza karty. Dane, które są przechowywane na tych kartach, określono w rozdziale 4.

139) Urządzenie rejestrujące aktualizuje dane dotyczące czynności kierowcy i miejsc (jak określono w pkt 4.5.3.1.9 i 4.5.3.1.11), zapisane na ważnej karcie kierowcy lub warsztatowej, danymi dotyczącymi czynności i miejsc wprowadzonymi ręcznie przez posiadacza karty.

140) Wszystkie wydarzenia niezdefiniowane dla urządzeń rejestrujących pierwszej generacji nie są zapisywane na karcie kierowcy ani na karcie warsztatowej.

141) Aktualizacja kart do tachografów odbywa się w taki sposób, że gdy zaistnieje taka potrzeba i biorąc pod uwagę rzeczywistą zdolność przechowywania danych, najstarsze dane są zastępowanymi najnowszymi danymi.

142) W przypadku błędu zapisu urządzenie rejestrujące maksymalnie trzykrotnie powtarza to samo polecenie zapisu i w przypadku gdy zapis nadal nie jest możliwy, uznaje kartę za uszkodzoną i nieważną.

143) Przed odblokowaniem karty kierowcy i po zapisaniu na karcie wszystkich stosownych danych urządzenie rejestrujące zeruje „dane sesji karty".

3.14.2 *Rejestrowanie i przechowywanie danych na kartach do tachografów drugiej generacji*

144) Karty do tachografów drugiej generacji zawierają 2 różne aplikacje kart, z których pierwsza jest dokładnie taka sama jak aplikacja TACHO w kartach do tachografów pierwszej generacji, a druga aplikacja „TACHO_G2" jest zgodna ze specyfikacjami w rozdziale 4 i dodatku 2.

145) Urządzenie rejestrujące ustawia „dane sesji karty" na karcie kierowcy lub warsztatowej bezpośrednio po włożeniu karty.

146) Urządzenie rejestrujące aktualizuje dane zapisane w 2 aplikacjach ważnej karty kierowcy, warsztatowej, firmowej lub kontrolnej, wprowadzając wszystkie niezbędne dane odnośnie do okresu, w którym karta pozostaje włożona, i odnośnie do posiadacza karty. Dane, które są przechowywane na tych kartach, określono w rozdziale 4.

147) Urządzenie rejestrujące aktualizuje dane dotyczące miejsc i pozycji czynności kierowcy (jak określono w pkt 4.5.3.1.9, 4.5.3.1.11, 4.5.3.2.9 i 4.5.3.2.11), zapisane na ważnej karcie kierowcy lub warsztatowej, danymi dotyczącymi czynności i miejsc wprowadzonymi ręcznie przez posiadacza karty.

148) Aktualizacja kart do tachografów odbywa się w taki sposób, że gdy zaistnieje taka potrzeba i biorąc pod uwagę rzeczywistą zdolność przechowywania danych, najstarsze dane są zastępowanymi najnowszymi danymi.

149) W przypadku błędu zapisu urządzenie rejestrujące maksymalnie trzykrotnie powtarza to samo polecenie zapisu i w przypadku gdy zapis nadal nie jest możliwy, uznaje kartę za uszkodzoną i nieważną.

150) Przed odblokowaniem karty kierowcy i po zapisaniu wszystkich stosownych danych w 2 aplikacjach karty urządzenie rejestrujące zeruje „dane sesji karty".

3.15 **Wyświetlanie**

151) Wyświetlacz umożliwia wyświetlanie co najmniej 20 znaków.

152) Wyświetlane znaki mają wymiary co najmniej 5 mm wysokości i 3,5 mm szerokości.

153) Wyświetlacz umożliwia wyświetlanie znaków określonych w dodatku 1 rozdział 4 „Zestawy znaków". Wyświetlacz może wyświetlać uproszczone glify (np. znaki z akcentami można wyświetlać bez akcentu, a małe litery może wyświetlać jako duże).

154) Wyświetlacz musi mieć nieoślepiające oświetlenie.

155) Wskazania są widoczne spoza urządzenia rejestrującego.

156) Urządzenie rejestrujące umożliwia wyświetlanie:

— informacji standardowych,

— informacji związanych z ostrzeżeniami,

— informacji związanych z dostępem do menu,

— innych informacji, których zażąda użytkownik.

Urządzenie rejestrujące może wyświetlać również dodatkowe informacje, z tym jednak, że muszą być one łatwe do odróżnienia od wymienionych powyżej, wymaganych informacji.

157) Na wyświetlaczu urządzenia rejestrującego używa się piktogramów lub kombinacji piktogramów wymienionych w dodatku 3. Dopuszcza się także dodatkowe piktogramy lub kombinacje piktogramów, jeżeli są one łatwe do odróżnienia od wymaganych piktogramów lub kombinacji piktogramów.

158) Gdy pojazd jest w ruchu, wyświetlacz jest stale włączony.

159) Urządzenie rejestrujące może gasić wyświetlacz automatycznie lub umożliwiać gaszenie ręczne, gdy pojazd nie jest w ruchu.

Format wyświetlania określono w dodatku 5.

3.15.1 *Domyślne informacje na wyświetlaczu*

160) Gdy nie istnieje potrzeba wyświetlania żadnych innych informacji, urządzenie rejestrujące domyślnie wyświetla następujące informacje:

— czas lokalny (wynik czasu UTC + przesunięcie wprowadzone przez kierowcę),

— tryb pracy,

— bieżącą czynność kierowcy i bieżącą czynność współkierowcy,

— informacje odnoszące się do kierowcy:

— jeżeli jego bieżącą czynnością jest PROWADZENIE, jego bieżący nieprzerwany czas prowadzenia pojazdu i jego bieżący skumulowany czas przerwy,

— jeżeli jego bieżącą czynnością nie jest PROWADZENIE, bieżący czas trwania tej czynności (od momentu wybrania) i jego bieżący skumulowany czas przerwy.

161) Prezentacja informacji odnoszących się do każdego kierowcy jest wyraźna, prosta i jednoznaczna. W przypadku gdy informacji odnoszących się do kierowcy i współkierowcy nie można wyświetlić w tym samym czasie, urządzenie rejestrujące pokazuje domyślnie informacje odnoszące się do kierowcy i pozwala użytkownikowi wyświetlić informacje odnoszące się do współkierowcy.

162) W przypadku gdy wyświetlacz nie pozwala na domyślne pokazywanie trybu pracy, to przy zmianie trybu pracy urządzenie rejestrujące przez krótki czas pokazuje informację o nowym trybie pracy.

163) Przy wkładaniu karty urządzenie rejestrujące przez krótki czas pokazuje nazwisko jej posiadacza.

164) W przypadku otwarcia warunku „POZA ZAKRESEM" lub „PRZEPRAWA PROMOWA/PRZEJAZD KOLEJOWY" na domyślnym wyświetlaczu musi pojawić się informacja w postaci stosownego piktogramu o tym, że warunek ten jest rozpoczęty (dopuszcza się, że w tym samym czasie nie jest pokazywana bieżąca czynność kierowcy).

3.15.2 *Wyświetlanie ostrzeżeń*

165) Przy wyświetlaniu ostrzeżeń urządzenie rejestrujące korzysta przede wszystkim z piktogramów w dodatku 3, w razie potrzeby uzupełnionych informacjami w postaci kodów liczbowych. Można też dodać wyszczególnienie słowne w preferowanym języku kierowcy.

3.15.3 *Dostęp do menu*

166) Urządzenie rejestrujące udostępnia niezbędne polecenia poprzez odpowiednie menu.

3.15.4 *Inne wyświetlane informacje*

167) Na żądanie możliwe jest selektywne wyświetlanie:

— czasu UTC oraz przesunięcia czasu lokalnego,

— treści każdego z sześciu wydruków w takim samym formacie jak wydruki,

— nieprzerwanego czasu prowadzenia pojazdu i skumulowanego czasu przerwy kierowcy,

— nieprzerwanego czasu prowadzenia pojazdu i skumulowanego czasu przerwy współkierowcy,

— skumulowanego czasu prowadzenia pojazdu kierowcy za poprzedni i bieżący tydzień,

— skumulowanego czasu prowadzenia pojazdu współkierowcy za poprzedni i bieżący tydzień,

opcjonalnie:

— bieżącego czasu trwania czynności współkierowcy (od momentu wybrania),

— skumulowanego czasu prowadzenia pojazdu kierowcy za bieżący tydzień,

— skumulowanego czasu prowadzenia pojazdu współkierowcy za bieżący dzienny okres pracy,

— skumulowanego czasu prowadzenia pojazdu kierowcy za bieżący dzienny okres pracy.

168) Treść wydruku jest wyświetlana sekwencyjnie, wiersz po wierszu. Jeżeli w szerokości wyświetlacza mieści się mniej niż 24 znaki, użytkownik musi mieć dostęp do pełnej informacji w odpowiedni sposób (w kilku wierszach, przy pomocy przewijania itp.).

Wiersze wydruku przeznaczone na ręczne adnotacje można pominąć na wyświetlaczu.

3.16 **Drukowanie**

169) Urządzenie rejestrujące umożliwia drukowanie siedmiu określonych poniżej wydruków, na podstawie informacji zgromadzonych w pamięci urządzenia lub na kartach do tachografów:

— wydruk dzienny czynności kierowcy z karty,

— wydruk dzienny czynności kierowcy z przyrządu rejestrującego,

— wydruk zdarzeń i usterek z karty,

— wydruk zdarzeń i usterek z przyrządu rejestrującego,

— wydruk danych technicznych,

— wydruk przekroczenia prędkości,

— historia danych karty do tachografu dla danego przyrządu rejestrującego (zob. rozdział 3.12.16).

Szczegóły formatu i treści tych wydruków określono w dodatku 4.

Pod koniec wydruku mogą być umieszczane informacje dodatkowe.

Urządzenie rejestrujące może wykonywać także dodatkowe wydruki, jeżeli są one łatwe do odróżnienia od siedmiu określonych powyżej wydruków.

170) „Wydruk dzienny czynności kierowcy z karty" i „wydruk zdarzeń i usterek z karty" dostępne są jedynie wtedy, gdy do urządzenia rejestrującego włożona jest karta kierowcy lub karta warsztatowa. Przed uruchomieniem drukowania urządzenie rejestrujące aktualizuje dane przechowywane na stosownej karcie.

171) W celu sporządzenia „wydruku dziennego czynności kierowcy z karty" lub „wydruku zdarzeń i usterek z karty" urządzenie rejestrujące:

— automatycznie wybiera kartę kierowcy lub kartę warsztatową, jeżeli tylko jedna z tych kart jest włożona do urządzenia rejestrującego,

— lub umożliwia wybór karty źródłowej albo wybiera kartę znajdującą się w czytniku karty kierowcy, jeżeli obie te karty włożone są do urządzenia rejestrującego.

172) Drukarka umożliwia drukowanie 24 znaków w wierszu.

173) Drukowane znaki mają wymiary co najmniej 2,1 mm wysokości i 1,5 mm szerokości.

174) Drukarka umożliwia drukowanie znaków określonych w dodatku 1 rozdział 4 „Zestawy znaków".

175) Konstrukcja drukarki umożliwia sporządzanie wydruków z rozdzielczością eliminującą niejednoznaczność przy odczycie.

176) Wydruki zachowują wymiary i treść w warunkach normalnej wilgotności (10–90 %) i temperatury.

177) Papier homologowany używany w urządzeniu rejestrującym musi mieć odpowiedni znak homologacji typu i oznakowanie typu (typów) urządzenia rejestrującego, w którym może być używany.

178) Wydruki muszą być łatwe do odczytania i rozróżnienia, gdy są przechowywane w normalnych warunkach przechowywania, w normalnym oświetleniu, wilgotności i temperaturze, przez okres co najmniej dwóch lat.

179) Wydruki muszą być zgodne co najmniej ze specyfikacjami testów podanymi w dodatku 9.

180) Na wydruku musi być również możliwość umieszczenia ręcznych adnotacji, takich jak podpis kierowcy.

181) Urządzenie rejestrujące obsługuje zdarzenia „brak papieru" w czasie drukowania, a po założeniu papieru, uruchamia drukowanie od początku wydruku lub kontynuuje drukowanie i umieszcza jednoznaczne odniesienie do części wcześniej wydrukowanej.

3.17 **Ostrzeżenia**

182) Urządzenie rejestrujące ostrzega kierowcę o wykryciu zdarzenia lub usterki.

183) Ostrzeżenie o przerwie w zasilaniu może być opóźnione do czasu przywrócenia zasilania.

184) Urządzenie rejestrujące ostrzega kierowcę na 15 minut przed przekroczeniem i w momencie przekroczenia maksymalnego dopuszczalnego nieprzerwanego czasu prowadzenia pojazdu.

185) Ostrzeżenia są wizualne. Oprócz ostrzeżeń wizualnych dopuszcza się ostrzeżenia akustyczne.

186) Ostrzeżenia wizualne muszą być łatwo rozpoznawalne przez użytkownika, znajdować się w polu widzenia kierowcy i być łatwe do odczytania tak w dzień, jak i w nocy.

187) Ostrzeżenia wizualne mogą być emitowane bezpośrednio przez urządzenie rejestrujące lub zdalnie od urządzenia rejestrującego.

188) W tym ostatnim przypadku są oznaczone symbolem „T".

189) Ostrzeżenia trwają przez przynajmniej 30 sekund, chyba że są potwierdzone przez użytkownika poprzez wciśnięcie jednego lub większej liczby specjalnych przycisków w urządzeniu rejestrującym. To pierwsze potwierdzenie nie usuwa z wyświetlacza informacji o przyczynie ostrzeżenia, o której mowa w następnym punkcie.

190) Urządzenie rejestrujące wyświetla informację o przyczynie ostrzeżenia, aż do momentu potwierdzenia przez użytkownika przy pomocy specjalnego przycisku lub polecenia urządzenia rejestrującego.

191) Dopuszcza się dodatkowe ostrzeżenia, pod warunkiem że nie są mylące dla kierowców w odniesieniu do wcześniej zdefiniowanych ostrzeżeń.

3.18 **Pobieranie danych na nośnik zewnętrzny**

192) Urządzenie rejestrujące umożliwia, na żądanie, pobieranie danych z pamięci danych lub karty kierowcy na zewnętrzny nośnik poprzez gniazdo kalibracji/pobierania danych. Przed pobraniem danych urządzenie rejestrujące aktualizuje dane przechowywane na stosownej karcie.

193) Dodatkowo i opcjonalnie, urządzenie rejestrujące może w dowolnym trybie pracy przesyłać dane w dowolny inny sposób do firmy uwierzytelnionej do korzystania z tego kanału. W takim przypadku do tak przesyłanych danych stosuje się prawa dostępu obowiązujące dla trybu firmowego.

194) Przy pobieraniu danych nie może mieć miejsca zmienianie ani usuwanie jakichkolwiek przechowywanych danych.

195) Specyfikacje elektrycznego interfejsu dla gniazda kalibracji/pobierania danych są określone w dodatku 6.

196) Protokoły pobierania danych są określone w dodatku 7.

3.19 **Łączność na odległość na potrzeby ukierunkowanych kontroli drogowych**

197) Przy włączonym zapłonie przyrząd rejestrujący co 60 sekund zachowuje na urządzeniu do łączności na odległość najnowsze dane niezbędne na potrzeby ukierunkowanych kontroli drogowych. Dane takie są szyfrowane i podpisywane zgodnie z dodatkiem 11 i dodatkiem 14.

198) Kontrolowane zdalnie dane muszą być dostępne dla czytników na odległość za pośrednictwem łączności bezprzewodowej, jak określono w dodatku 14.

199) Dane niezbędne na potrzeby ukierunkowanych kontroli drogowych odnoszą się do:

— ostatniej próby naruszenia zabezpieczenia,

— najdłuższej przerwy w zasilaniu,

— usterki czujnika,

— błędu danych dotyczących ruchu,

— konfliktu ruchu pojazdu,

— prowadzenia pojazdu bez ważnej karty,

— włożenia karty podczas prowadzenia pojazdu,

— danych dotyczących korekty czasu,

— danych kalibracyjnych, w tym dat dwóch ostatnio zapisanych rekordów danych kalibracji,

— numeru rejestracyjnego pojazdu,

— prędkości zarejestrowanej przez tachograf.

3.20 **Wyprowadzanie danych do dodatkowych urządzeń zewnętrznych**

200) Urządzenie rejestrujące może być również wyposażone w znormalizowane interfejsy pozwalające na wykorzystywanie przez urządzenie zewnętrzne danych rejestrowanych lub generowanych przez tachograf w trybie operacyjnym lub kalibracyjnym.

W dodatku 13 określono i podano normę dla opcjonalnego interfejsu ITS. Inne podobne interfejsy mogą współistnieć, pod warunkiem że są w pełni zgodne z wymogami określonymi w dodatku 13 w odniesieniu do minimalnego wykazu danych, zabezpieczeń i zgody kierowcy.

Następujące wymagania mają zastosowanie do danych ITS udostępnianych za pośrednictwem tego interfejsu:

— dane te stanowią zbiór wybranych istniejących danych ze słownika danych tachografu (dodatek 1),

— podzbiór tych wybranych danych jest oznaczony jako „dane osobowe",

— podzbiór „danych osobowych" jest dostępny jedynie w przypadku, gdy włączona jest opcja podlegającej weryfikacji zgody kierowcy na wyprowadzenie jego danych osobowych z sieci pojazdu,

— w dowolnym momencie istnieje możliwość potwierdzenia lub wycofania zgody kierowcy przez wybranie polecenia w menu, pod warunkiem że karta kierowcy jest włożona,

— zbiór i podzbiór danych są przekazywane za pośrednictwem protokołu bezprzewodowego Bluetooth w promieniu kabiny pojazdu, z częstotliwością odświeżania co 1 minutę,

— sparowanie urządzenia zewnętrznego z interfejsem ITS jest zabezpieczone dedykowanym losowym kodem PIN składającym się z co najmniej 4 cyfr, zapisywanym i dostępnym przez wyświetlacz każdego przyrządu rejestrującego,

— w żadnych okolicznościach obecność interfejsu ITS nie może zakłócać prawidłowego funkcjonowania i bezpieczeństwa przyrządu rejestrującego, ani oddziaływać na niego.

Można wyprowadzać również inne dane oprócz zbioru wybranych istniejących danych, uznawanych za wykaz minimalny, pod warunkiem że nie można ich uważać za dane osobowe.

Urządzenie rejestrujące powiadamia inne urządzenia zewnętrzne o zgodzie kierowcy.

Przy włączonym zapłonie pojazdu dane te udostępniane są nieprzerwanie.

201) Do celów kompatybilności wstecznej możliwe jest wyposażenie tachografów w interfejs szeregowy, jak określono w załączniku 1B do rozporządzenia (EWG) nr 3821/85. Nadal wymagana jest zgoda kierowcy w przypadku gdy przekazywane są dane osobowe.

3.21 **Kalibracja**

202) Funkcja kalibracji umożliwia:

— automatyczne sparowanie czujnika ruchu z przyrządem rejestrującym,

— automatyczne powiązanie urządzenia zewnętrznego GNSS z przyrządem rejestrującym w stosownych przypadkach,

— cyfrowe dostosowanie stałej urządzenia rejestrującego (k) do współczynnika charakterystycznego pojazdu (w),

— regulację bieżącego wskazania czasu w zakresie okresu ważności włożonej karty warsztatowej,

— regulację bieżącego wskazania licznika kilometrów,

— aktualizację danych identyfikacyjnych czujnika ruchu zapisanych w pamięci danych,

— aktualizację, w stosownych przypadkach, danych identyfikacyjnych urządzenia zewnętrznego GNSS zapisanych w pamięci danych,

— aktualizację rodzajów i identyfikatorów wszystkich założonych plomb,

— aktualizację lub potwierdzenie innych parametrów używanych przez urządzenie rejestrujące: identyfikację pojazdu, w, l, rozmiar opon i ustawienie urządzenia ograniczenia prędkości, w stosownych przypadkach.

203) Ponadto funkcja kalibracji umożliwia wyłączenie stosowania kart do tachografów pierwszej generacji w urządzeniu rejestrującym pod warunkiem spełnienia wymogów określonych w dodatku 15.

204) Parowanie czujnika ruchu z przyrządem rejestrującym obejmuje co najmniej:

— aktualizację danych instalacyjnych czujnika ruchu zapisanych w pamięci czujnika ruchu (w razie potrzeby),

— skopiowanie z czujnika ruchu do pamięci danych przyrządu rejestrującego niezbędnych danych identyfikacyjnych czujnika ruchu.

205) Powiązanie urządzenia zewnętrznego GNSS z przyrządem rejestrującym obejmuje co najmniej:

— aktualizację danych instalacyjnych urządzenia zewnętrznego GNSS przechowywanych na urządzeniu zewnętrznym GNSS (w razie potrzeby),

— skopiowanie z urządzenia zewnętrznego GNSS do pamięci danych przyrządu rejestrującego niezbędnych danych identyfikacyjnych GNSS, w tym numeru seryjnego urządzenia zewnętrznego GNSS.

Po powiązaniu następuje weryfikacja informacji o pozycji GNSS.

206) Funkcja kalibracji umożliwia wprowadzanie niezbędnych danych poprzez gniazdo kalibracji/pobierania danych zgodnie z protokołem kalibracji zdefiniowanym w dodatku 8. Funkcja kalibracji może także umożliwiać wprowadzanie niezbędnych danych w inny sposób.

3.22 **Kontrola drogowa kalibracji**

207) Funkcja kontroli drogowej kalibracji umożliwia odczyt numeru seryjnego czujnika (ewentualnie wbudowanego w adapter) oraz numeru seryjnego urządzenia zewnętrznego GNSS (w odpowiednich przypadkach), podłączonych do przyrządu rejestrującego w momencie wysłania żądania.

208) Odczyt musi być możliwy na wyświetlaczu przyrządu rejestrującego przynajmniej przez wybranie poleceń w menu.

209) Funkcja kontroli drogowej kalibracji umożliwia również kontrolowanie wybranego trybu we/wy linii sygnałowej we/wy kalibracji, określonej w dodatku 6, za pośrednictwem interfejsu K-line. Wykonuje się to poprzez ECUAdjustmentSession, jak określono w dodatku 8 sekcja 7 Sterowanie impulsami testującymi – Jednostka funkcjonalna sterowania we/wy.

3.23 **Korekta czasu**

210) Funkcja korekty czasu umożliwia automatyczną korektę bieżącego czasu. W urządzeniu rejestrującym korzysta się z dwóch źródeł czasu do celów korekty czasu: 1) wewnętrznego zegara przyrządu rejestrującego, 2) odbiornika GNSS.

211) Ustawienia czasu zegara wewnętrznego przyrządu rejestrującego są automatycznie korygowane w odstępach maksymalnie 12 godzin. Jeżeli ten odstęp czasu upłynie, a sygnał GNSS nie jest dostępny, ustawienie czasu wprowadza się, jak tylko przyrząd rejestrujący uzyska dostęp do prawidłowego czasu z odbiornika GNSS, zależnie od stanu włączenia zapłonu pojazdu. Czasem odniesienia dla automatycznego ustawienia wewnętrznego zegara przyrządu rejestrującego jest czas pobrany z odbiornika GNSS. Zdarzenie konfliktu czasu uruchamia się, jeżeli bieżący czas odbiega o ponad jedną (1) minutę od informacji przekazywanych przez odbiornik GNSS.

212) W trybie kalibracyjnym funkcja korekty czasu umożliwia również wymuszoną korektę bieżącego czasu.

3.24 **Parametry pracy**

213) Przyrząd rejestrujący musi być w pełni funkcjonalny w zakresie temperatur – 20–70 °C, urządzenie zewnętrzne GNSS w zakresie temperatur – 20–70 °C, a czujnik ruchu w zakresie temperatur – 40–135 °C. Zawartość pamięci danych jest zachowywana w temperaturach do – 40 °C.

214) Tachograf zachowuje pełną funkcjonalność w zakresie wilgotności 10–90 %.

215) Plomby używane w tachografach inteligentnych muszą być wytrzymałe w takich samych warunkach, co warunki stosowane względem elementów składowych tachografu, do których są dołączone.

216) Urządzenie rejestrujące jest zabezpieczone przed przepięciami, odwróceniem biegunowości zasilania i zwarciami.

217) Czujniki ruchu muszą:

— reagować na pole magnetyczne, które zakłóca wykrywanie ruchu pojazdu. W takich okolicznościach przyrząd rejestrujący zarejestruje i zapisze w pamięci usterkę czujnika (wymaganie 88); albo

— posiadać czujnik, który jest chroniony przed polami magnetycznymi lub odporny na nie.

218) Urządzenie rejestrujące oraz urządzenie zewnętrzne GNSS muszą być zgodne z międzynarodowym regulaminem EKG ONZ nr 10 oraz być zabezpieczone przed skutkami wyładowań elektrostatycznych oraz stanów nieustalonych.

3.25 **Materiały**

219) Wszystkie części składowe urządzenia rejestrującego są wykonane z materiałów o wystarczającej stabilności i wytrzymałości mechanicznej oraz stabilnych właściwościach elektrycznych i magnetycznych.

220) W normalnych warunkach eksploatacji wszystkie części wewnętrzne urządzeń są zabezpieczone przed wilgocią i pyłem.

221) Przyrząd rejestrujący i urządzenie zewnętrzne GNSS muszą spełniać wymagania klasy ochrony IP 40, a czujnik ruchu musi spełniać wymagania klasy ochrony IP 64 zgodnie z normą IEC 60529:1989 łącznie z A1:1999 i A2:2013.

222) Urządzenie rejestrujące musi spełniać odpowiednie wymagania techniczne odnoszące się do ergonomii.

223) Urządzenie rejestrujące jest zabezpieczone przed przypadkowym uszkodzeniem.

3.26 **Oznakowania**

224) Jeżeli urządzenie rejestrujące pokazuje stan licznika kilometrów i prędkość, na wyświetlaczu widoczne są następujące informacje:

— przy liczbie pokazującej odległość, jednostka miary odległości wskazana skrótem „km”,

— przy liczbie pokazującej prędkość, jednostka „km/h”.

Urządzenie rejestrujące może być również przełączane na wskazywanie prędkości w milach na godzinę, w takim przypadku jednostka pomiaru prędkości jest wskazana skrótem „mph”. Urządzenie rejestrujące może być również przełączane na wskazywanie odległości w milach, w takim przypadku jednostka pomiaru odległości jest wskazana skrótem „mi”.

225) Do każdego odrębnego elementu składowego urządzenia rejestrującego jest przymocowana tabliczka zawierająca następujące informacje:

— nazwę i adres producenta urządzenia,

— numer części producenta i rok produkcji urządzenia,

— numer seryjny urządzenia,

— znak homologacji typu dla urządzenia.

226) Jeżeli dostępna powierzchnia nie wystarcza do umieszczenia wszystkich powyższych informacji, na tabliczce umieszcza się przynajmniej: nazwę producenta lub jego logo i numer części.

4 WYMAGANIA KONSTRUKCYJNE I FUNKCJONALNE KART DO TACHOGRAFÓW

4.1 **Dane widzialne**

Na awersie znajdują się:

227) słowa „Karta kierowcy” lub „Karta kontrolna” lub „Karta warsztatowa” lub „Karta firmowa” nadrukowane wersalikiem w języku urzędowym lub językach urzędowych państwa członkowskiego wydającego kartę, odpowiednio do rodzaju karty;

228) nazwa państwa członkowskiego wydającego kartę (nieobowiązkowo);

229) wyróżniający znak państwa członkowskiego wydającego kartę, drukowany w negatywie w niebieskim prostokącie i otoczony 12 żółtymi gwiazdami. Obowiązują następujące oznaczenia:

B	Belgia	LV	Łotwa
BG	Bułgaria	L	Luksemburg
CZ	Republika Czeska	LT	Litwa
CY	Cypr	M	Malta
DK	Dania	NL	Niderlandy

D EST	Niemcy Estonia	A PL	Austria Polska
GR	Grecja	P RO SK SLO	Portugalia Rumunia Słowacja Słowenia
E	Hiszpania	FIN	Finlandia
F HR H	Francja Chorwacja Węgry	S	Szwecja
IRL	Irlandia	UK	Zjednoczone Królestwo
I	Włochy		

230) informacje szczególne dla wydanej karty, ponumerowane jak następuje:

	Karta kierowcy	Karta kontrolna	Karta firmowa lub warsztatowa
1.	Nazwisko kierowcy	Nazwa organu kontrolnego	Nazwa firmy lub warsztatu
2.	Imię (imiona) kierowcy	Nazwisko kontrolera (w stosownych przypadkach)	Nazwisko posiadacza karty (w stosownych przypadkach)
3.	Data urodzenia kierowcy	Imię (imiona) kontrolera (w stosownych przypadkach)	Imię (imiona) posiadacza karty (w stosownych przypadkach)
4.a	Data początku okresu ważności karty		
4.b	Termin ważności karty		
4.c	Nazwa organu wydającego (może być wydrukowana na rewersie)		
4.d	Numer inny niż w pozycji 5 do celów administracyjnych (fakultatywnie)		
5.a	Numer prawa jazdy (w dniu wydania karty kierowcy)	—	—
5.b	Numer karty		
6.	Zdjęcie kierowcy	Zdjęcie kontrolera (fakultatywnie)	Zdjęcie instalatora (fakultatywnie)

	Karta kierowcy	Karta kontrolna	Karta firmowa lub warsztatowa
7.	Podpis posiadacza karty (fakultatywnie)		
8.	Miejsce stałego zamieszkania lub adres pocztowy posiadacza (fakultatywnie)	Adres pocztowy organu kontrolnego	Adres pocztowy firmy lub warsztatu

231) daty podaje się w formacie „dd/mm/rrrr” lub „dd.mm.rrrr” (dzień, miesiąc, rok).

Na rewersie znajdują się:

232) objaśnienia numerowanych pozycji znajdujących się na awersie karty;

233) za szczególną pisemną zgodą posiadacza karty, na karcie można dodatkowo umieścić informacje, które nie wiążą się z administrowaniem kartą; takie dodatkowe informacje w żaden sposób nie zmieniają sposobu używania danego modelu jako karty do tachografów;

234) Karty do tachografów drukuje się w następujących dominujących kolorach tła:

— karta kierowcy: biały,

— karta kontrolna: niebieski,

— karta warsztatowa: czerwony,

— karta firmowa: żółty.

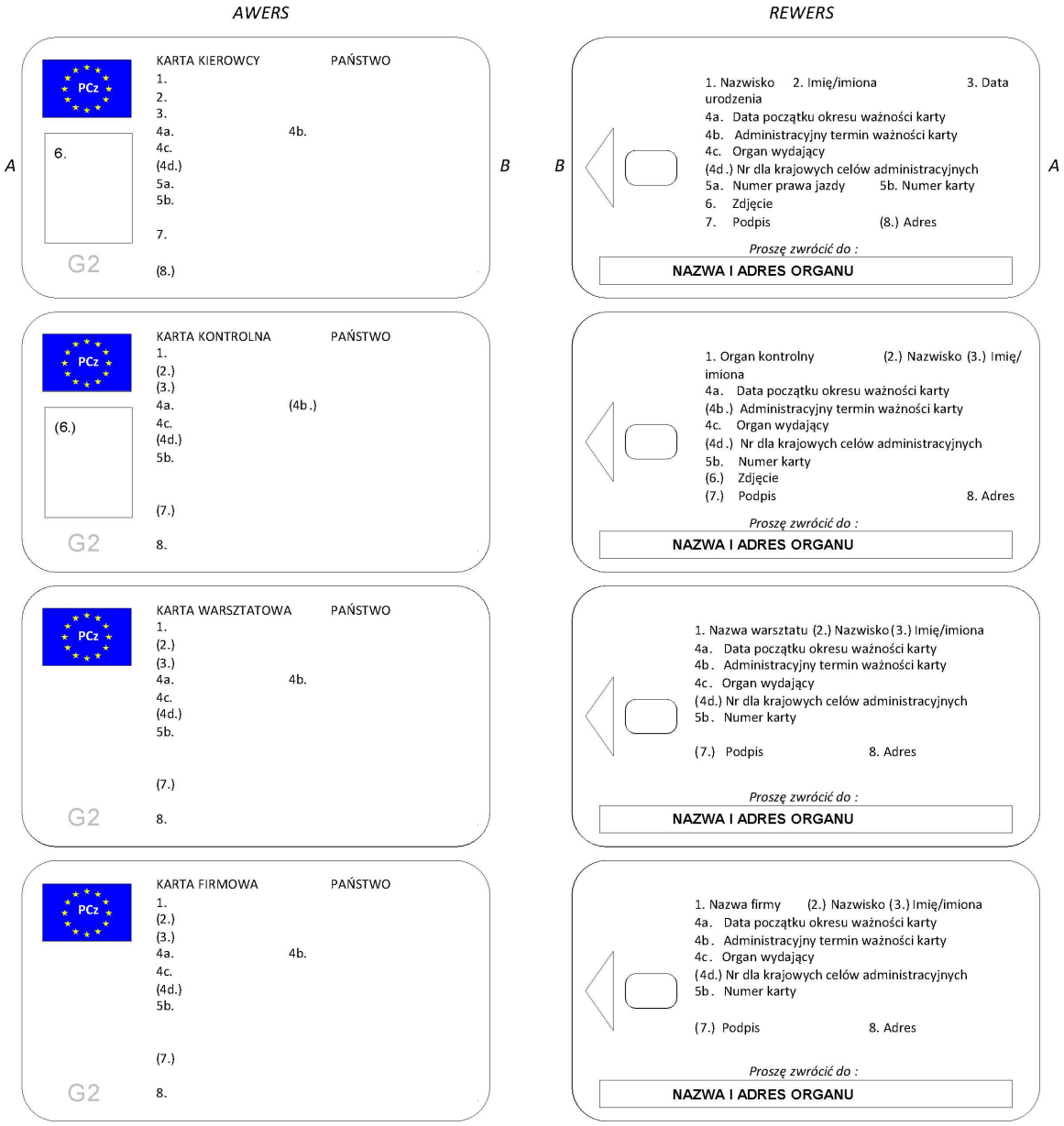
235) Karty do tachografów muszą mieć przynajmniej następujące zabezpieczenia przed fałszowaniem i manipulacjami:

— zabezpieczający wzór tła z drukowanym drobnym giloszem i drukiem irysowym,

— w obszarze zdjęcia zabezpieczający wzór tła i zdjęcie zachodzą na siebie,

— przynajmniej dwubarwną linię wykonaną techniką mikrodruku.

WZORY WSPÓLNOTOWYCH KART DO TACHOGRAFÓW



236) Po konsultacji z Komisją państwa członkowskie mogą dodać kolory lub oznakowania, takie jak symbole państwowe i zabezpieczenia, bez uszczerbku dla innych przepisów w niniejszym załączniku.

237) Karty czasowe, o których mowa w art. 26 ust. 4 rozporządzenia (UE) nr 165/2014, muszą być zgodne z przepisami niniejszego załącznika.

4.2 Zabezpieczenia

Celem systemu zabezpieczenia jest ochrona integralności i autentyczności danych wymienianych między kartami a urządzeniem rejestrującym, ochrona integralności i autentyczności danych pobieranych z kart, umożliwienie niektórych czynności zapisu na kartach tylko urządzeniu rejestrującemu, odszyfrowywania niektórych danych, uniemożliwienie fałszowania danych przechowywanych na kartach, uniemożliwienie manipulacji i wykrycie wszelkich prób takiego działania.

238) Aby możliwe było osiągnięcie bezpieczeństwa systemu, karty do tachografów muszą spełniać wymogi bezpieczeństwa określone w dodatkach 10 i 11.

239) Karty do tachografów muszą umożliwiać odczyt przy pomocy innych urządzeń, takich jak komputer osobisty.

4.3 **Normy**

240) Karty do tachografów muszą spełniać wymagania następujących norm:

— ISO/IEC 7810 Karty identyfikacyjne – Charakterystyki fizyczne,

— ISO/IEC 7816 Karty identyfikacyjne – Karty stykowe:

— Część 1: Charakterystyki fizyczne,

— Część 2: Wymiary i rozmieszczenie styków (ISO/IEC 7816-2:2007),

— Część 3: Interfejs elektryczny i protokoły transmisji (ISO/IEC 7816-3:2006),

— Część 4: Organizacja, zabezpieczenia i polecenia wymiany (ISO/IEC 7816-4:2013 + Cor 1:2014),

— Część 6: Elementy danych wymieniane z otoczeniem, niezależne od dziedziny zastosowań (ISO/IEC 7816-6:2004 + Cor 1:2006),

— Część 8: Polecenia operacji zabezpieczających (ISO/IEC 7816-8:2004).

— Karty do tachografów bada się zgodnie z normą SO/IEC 10373-3:2010 Karty identyfikacyjne – Metody badań – część 3: Elektroniczne karty stykowe i powiązane z nimi urządzenia interfejsowe.

4.4 **Wymagania środowiskowe i elektryczne**

241) Karty do tachografów muszą prawidłowo działać w warunkach klimatycznych normalnie występujących na terytorium Wspólnoty, przynajmniej w zakresie temperatur od – 25– + 70 °C ze sporadycznymi temperaturami szczytowymi do + 85 °C, przy czym „sporadyczny" oznacza nie dłużej niż 4 godziny jednorazowo i nie więcej niż 100 razy w okresie eksploatacji karty.

242) Karty do tachografów muszą działać prawidłowo w warunkach wilgotności 10 %–90 %.

243) Karty do tachografów muszą prawidłowo działać przez okres pięciu lat, jeżeli są używane w zgodnie z warunkami środowiskowymi i elektrycznymi.

244) W trakcie stosowania karty do tachografów muszą spełniać wymogi regulaminu EKG ONZ nr 10 w odniesieniu do kompatybilności elektromagnetycznej oraz muszą być chronione przed wyładowaniami elektrostatycznymi.

4.5 **Przechowywanie danych**

Do celów niniejszego pkt:

— czas jest rejestrowany z dokładnością do jednej minuty, chyba że ustalono inaczej,

— stany licznika kilometrów rejestruje się z dokładnością do jednego kilometra,

— prędkości rejestruje się z dokładnością do 1 km/h,

— pozycje (szerokość i długość) rejestruje się w stopniach i minutach, z dokładnością do 1/10 minuty.

Funkcje kart do tachografów, polecenia i struktury logiczne, spełniające wymagania dotyczące przechowywania danych wyszczególniono w dodatku 2.

O ile nie określono inaczej, przechowywanie danych na kartach do tachografów odbywa się w taki sposób, że najstarsze dane są zastępowane nowymi danymi, jeżeli wyczerpie się pamięć przewidziana na określone rekordy danych.

245) W niniejszym punkcie określono minimalną pojemność przechowywania danych dla różnych zbiorów danych aplikacyjnych. Karty do tachografów przekazują do urządzenia rejestrującego bieżącą pojemność przechowywania danych dla tych zbiorów danych.

246) Wszelkie dodatkowe dane, które mogą być zapisywane na kartach do tachografów, związane z innymi aplikacjami ewentualnie zamieszczonymi na karcie, są przechowywane zgodnie z dyrektywą 95/46/WE oraz dyrektywą 2002/58/WE oraz zgodnie z art. 7 rozporządzenia (UE) nr 165/2014.

247) Każdy plik główny (MF) na każdej karcie do tachografu zawiera maksymalnie pięć plików elementarnych (EF) do zarządzania kartą, identyfikacji aplikacji i mikroprocesora oraz dwa pliki dedykowane (DF):

— DF Tachograph, który zawiera aplikację dostępną dla przyrządów rejestrujących pierwszej generacji, używaną również w kartach do tachografów pierwszej generacji,

— DF Tachograph_G2, który zawiera aplikację dostępną tylko dla przyrządów rejestrujących drugiej generacji, używaną tylko w kartach do tachografów drugiej generacji,

Szczegółowe informacje o strukturze kart do tachografów określono w dodatku 2.

4.5.1 *Pliki elementarne do identyfikacji i zarządzania kartą*

4.5.2 *Identyfikacja kart mikroprocesorowych*

248) Karty do tachografów umożliwiają przechowywanie następujących danych identyfikujących kartę elektroniczną:

— zatrzymanie zegara,

— numer seryjny karty (łącznie z numerem producenta),

— numer homologacji typu dla karty,

— identyfikator jednostki personalizującej kartę,

— identyfikator wbudowującego,

— identyfikator układu scalonego.

4.5.2.1 Identyfikacja mikroprocesora

249) Karty do tachografów umożliwiają przechowywanie następujących danych identyfikujących układ scalony (IC):

— numer seryjny układu scalonego,

— oznaczenie fabryczne układu scalonego.

4.5.2.2 DIR (tylko w kartach do tachografów drugiej generacji)

250) Karty do tachografów umożliwiają przechowywanie obiektów danych identyfikujących aplikacje określonych w dodatku 2.

4.5.2.3 Informacje ATR (warunkowe, dostępne tylko w kartach do tachografów drugiej generacji)

251) Karty do tachografów umożliwiają przechowywanie następujących obiektów danych informacji o rozszerzonej długości:

— jeżeli karta do tachografów obsługuje pola o rozszerzonej długości, obiekt danych informacji o rozszerzonej długości określony w dodatku 2.

4.5.2.4 Informacje o rozszerzonej długości (warunkowe, dostępne tylko w kartach do tachografów drugiej generacji)

252) Karty do tachografów umożliwiają przechowywanie następujących obiektów danych informacji o rozszerzonej długości:

— jeżeli karta do tachografów obsługuje pola o rozszerzonej długości, obiekty danych informacji o rozszerzonej długości określony w dodatku 2.

4.5.3 *Karta kierowcy*

4.5.3.1 Aplikacja tachograficzna (dostępna dla przyrządów rejestrujących pierwszej i drugiej generacji)

4.5.3.1.1 Identyfikacja aplikacji

253) Karta kierowcy umożliwia przechowywanie następujących danych identyfikujących aplikację:

— identyfikacja aplikacji tachograficznej,

— identyfikacja typu karty do tachografów.

4.5.3.1.2 Klucz i certyfikaty

254) Karta kierowcy umożliwia przechowywanie szeregu kluczy i certyfikatów kryptograficznych, jak określono w dodatku 11 część A.

4.5.3.1.3 Identyfikacja karty

255) Karta kierowcy umożliwia przechowywanie następujących danych identyfikujących kartę:

— numer karty,

— państwo członkowskie wydające kartę, nazwa organu wydającego, data wydania,

— data rozpoczęcia okresu ważności karty, termin ważności karty.

4.5.3.1.4 Identyfikacja posiadacza karty

256) Karta kierowcy umożliwia przechowywanie następujących danych identyfikujących posiadacza karty:

— nazwisko posiadacza karty,

— imię (imiona) posiadacza karty,

— data urodzenia,

— preferowany język.

4.5.3.1.5 Pobieranie danych z karty

257) Karta kierowcy umożliwia przechowywanie następujących danych dotyczących pobierania danych:

— data i godzina ostatniego pobrania danych z karty (do innych celów niż kontrola).

258) Karta kierowcy umożliwia przechowywanie jednego takiego rekordu danych.

4.5.3.1.6 Dane dotyczące prawa jazdy

259) Karta kierowcy umożliwia przechowywanie następujących danych dotyczących prawa jazdy:

— państwo członkowskie wydające, nazwa organu wydającego,

— numer prawa jazdy (w dniu wydania karty).

4.5.3.1.7 Dane dotyczące zdarzeń

Do celów niniejszego podpunktu czas zachowuje się z dokładnością do 1 sekundy.

260) Karta kierowcy umożliwia przechowywanie następujących danych dotyczących zdarzeń wykrytych przez urządzenie rejestrujące przy włożonej karcie:

— nakładające się czasy (w przypadku gdy dana karta jest przyczyną zdarzenia),

— włożenie karty podczas jazdy (w przypadku gdy dana karta jest przedmiotem zdarzenia),

— sesja ostatniej karty niezamknięta prawidłowo (w przypadku gdy dana karta jest przedmiotem zdarzenia),

— przerwa w zasilaniu,

— błąd danych dotyczących ruchu,

— próby naruszenia zabezpieczenia.

261) Karta kierowcy umożliwia przechowywanie następujących danych dla tych zdarzeń:

— kod zdarzenia,

— data i godzina rozpoczęcia zdarzenia (lub włożenia karty, jeżeli zdarzenie trwało w tym czasie),

— data i godzina zakończenia zdarzenia (lub wyjęcia karty, jeżeli zdarzenie trwało w tym czasie),

— numer VRN i państwo członkowskie rejestracji pojazdu, w którym wystąpiło zdarzenie.

Uwaga: dla zdarzenia „nakładające się czasy":

— data i godzina rozpoczęcia zdarzenia musi odpowiadać dacie i godzinie wyjęcia karty z poprzedniego pojazdu,

— data i godzina zakończenia zdarzenia musi odpowiadać dacie i godzinie włożenia karty w bieżącym pojeździe,

— dane pojazdu muszą odpowiadać bieżącemu pojazdowi powodującemu zdarzenie.

Uwaga: dla zdarzenia „sesja ostatniej karty niezamknięta prawidłowo":

— data i godzina rozpoczęcia zdarzenia musi odpowiadać dacie i godzinie włożenia karty dla sesji niezamkniętej prawidłowo,

— data i godzina zakończenia zdarzenia musi odpowiadać dacie i godzinie włożenia karty dla sesji, w czasie której wykryto zdarzenie (bieżąca sesja),

— dane pojazdu muszą odpowiadać pojazdowi, w którym sesja nie została zamknięta prawidłowo.

262) Karta kierowcy umożliwia przechowywanie danych dotyczących sześciu ostatnich zdarzeń każdego typu (łącznie 36 zdarzeń).

4.5.3.1.8 Dane dotyczące usterek

Do celów niniejszego podpunktu czas rejestruje się z dokładnością do 1 sekundy.

263) Karta kierowcy umożliwia przechowywanie następujących danych dotyczących usterek wykrytych przez urządzenie rejestrujące przy włożonej karcie:

— usterka karty (w przypadku gdy dana karta jest przedmiotem zdarzenia),

— usterka urządzenia rejestrującego.

264) Karta kierowcy umożliwia przechowywanie następujących danych dotyczących tych usterek:

— kod usterki,

— data i godzina rozpoczęcia usterki (lub włożenia karty, jeżeli usterka trwała w tym czasie),

— data i godzina zakończenia usterki (lub wyjęcia karty, jeżeli usterka trwała w tym czasie),

— numer VRN i państwo członkowskie rejestracji pojazdu, w którym wystąpiła usterka.

265) Karta kierowcy umożliwia przechowywanie następujących danych dotyczących dwunastu ostatnich usterek każdego rodzaju (łącznie 24 usterki).

4.5.3.1.9 Dane dotyczące czynności kierowcy

266) Karta kierowcy umożliwia przechowywanie, dla każdego dnia kalendarzowego, w którym karta jest użyta, lub dla każdego dnia, dla którego kierowca ręcznie wprowadza informacje dotyczące czynności, następujących danych:

— data,

— dzienny licznik obecności (zwiększony o jeden dla każdego z tych dni kalendarzowych),

— całkowita droga przebyta przez kierowcę w ciągu tego dnia,

— status kierowcy o godzinie 00:00,

— za każdym razem, kiedy kierowca zmienia czynność lub stan prowadzenia pojazdu lub wkłada lub wyjmuje swoją kartę:

— stan prowadzenia pojazdu (ZAŁOGA, JEDEN KIEROWCA),

— szczelina czytnika (KIEROWCA, WSPÓŁKIEROWCA),

— status karty (WŁOŻONA, NIEWŁOŻONA),

— czynność (PROWADZENIE, GOTOWOŚĆ, PRACA, PRZERWA/ODPOCZYNEK),

— godzina zmiany.

267) Pamięć karty kierowcy wystarcza do przechowywania danych dotyczących czynności kierowcy przez co najmniej 28 dni (przeciętną aktywność kierowcy definiuje się jako 93 zmiany czynności dziennie).

268) Dane wyszczególnione w wymaganiach 261, 264 i 266 przechowuje się w sposób umożliwiający wyszukiwanie czynności w kolejności chronologicznej, nawet w przypadku nakładania się czasów.

4.5.3.1.10 Dane dotyczące używanych pojazdów

269) Karta kierowcy umożliwia przechowywanie, dla każdego dnia kalendarzowego, w którym karta jest użyta, i dla każdego okresu używania danego pojazdu w tym dniu (okres używania obejmuje wszystkie następujące po sobie cykle włożenia i wyjęcia karty w danym pojeździe, z perspektywy danych zapisanych na karcie), następujących danych:

— data i godzina pierwszego użycia pojazdu (tj. pierwsze włożenie karty w tym okresie używania pojazdu lub 00:00, jeżeli okres używania trwał w tym czasie),

— stan licznika kilometrów o tej godzinie,

— data i godzina ostatniego użycia pojazdu, (tj. ostatnie wyjęcie karty w tym okresie używania pojazdu lub 23:59, jeżeli okres używania trwał w tym czasie),

— stan licznika kilometrów o tej godzinie,

— numer VRN i państwo członkowskie rejestracji pojazdu.

270) Karta kierowcy umożliwia przechowywanie co najmniej 84 takich rekordów danych.

4.5.3.1.11 Miejsca rozpoczęcia lub zakończenia dziennych okresów pracy

271) Karta kierowcy umożliwia przechowywanie następujących danych dotyczących miejsc rozpoczęcia lub zakończenia dziennych okresów pracy, wprowadzanych przez kierowcę:

— data i godzina wprowadzenia danych (lub data/godzina odnosząca się do wpisu, jeżeli wpis wprowadza się w procedurze ręcznego wprowadzania danych),

— rodzaj wpisu (rozpoczęcie lub zakończenie, status wpisu),

— kraj i region,

— stan licznika kilometrów.

272) Pamięć karty kierowcy umożliwia przechowywanie co najmniej 42 par takich rekordów danych.

4.5.3.1.12 Dane sesji karty

273) Karta kierowcy umożliwia przechowywanie następujących danych dotyczących pojazdu, dla którego otwarto bieżącą sesję:

— data i godzina otwarcia sesji (tj. włożenia karty) z dokładnością do jednej sekundy,

— numer VRN i państwo członkowskie rejestracji.

4.5.3.1.13 Dane dotyczące czynności kontrolnych

274) Karta kierowcy umożliwia przechowywanie następujących danych dotyczących czynności kontrolnych:

— data i godzina kontroli,

— numer karty kontrolnej i państwo członkowskie wydające kartę,

— rodzaj kontroli (wyświetlanie lub drukowanie lub pobieranie danych z przyrządu rejestrującego lub pobieranie danych z karty – patrz uwaga),

— okres, dla którego pobrano dane, w przypadku pobierania danych,

— numer VRN i państwo członkowskie rejestracji pojazdu, w którym miała miejsce kontrola.

Uwaga: pobieranie danych z karty jest rejestrowane wyłącznie wtedy, gdy jest wykonywane przez urządzenie rejestrujące.

275) Karta kierowcy umożliwia przechowywanie jednego takiego rekordu danych.

4.5.3.1.14 Dane dotyczące warunków szczególnych

276) Karta kierowcy umożliwia przechowywanie następujących danych dotyczących warunków szczególnych wprowadzonych przy włożonej karcie (niezależnie od tego, do której szczeliny czytnika):

— data i godzina wprowadzenia danych,

— rodzaj warunku szczególnego.

277) Karta kierowcy umożliwia przechowywanie co najmniej 56 takich rekordów danych.

4.5.3.2 Aplikacja tachograficzna 2. generacji (niedostępna dla przyrządów rejestrujących pierwszej generacji)

4.5.3.2.1 Identyfikacja aplikacji

278) Karta kierowcy umożliwia przechowywanie następujących danych identyfikujących aplikację:

— identyfikacja aplikacji tachograficznej,

— identyfikacja typu karty do tachografów.

4.5.3.2.2 Klucze i certyfikaty

279) Karta kierowcy umożliwia przechowywanie szeregu kluczy i certyfikatów kryptograficznych, jak określono w dodatku 11 część B.

4.5.3.2.3 Identyfikacja karty

280) Karta kierowcy umożliwia przechowywanie następujących danych identyfikujących kartę:

— numer karty,

— państwo członkowskie wydające kartę, nazwa organu wydającego, data wydania,

— data rozpoczęcia okresu ważności karty, termin ważności karty.

4.5.3.2.4 Identyfikacja posiadacza karty

281) Karta kierowcy umożliwia przechowywanie następujących danych identyfikujących posiadacza karty:

— nazwisko posiadacza karty,

— imię (imiona) posiadacza karty,

— data urodzenia,

— preferowany język.

4.5.3.2.5 Pobieranie danych z karty

282) Karta kierowcy umożliwia przechowywanie następujących danych dotyczących pobierania danych:

— data i godzina ostatniego pobrania danych z karty (do innych celów niż kontrola).

283) Karta kierowcy umożliwia przechowywanie jednego takiego rekordu danych.

4.5.3.2.6 Dane dotyczące prawa jazdy

284) Karta kierowcy umożliwia przechowywanie następujących danych dotyczących prawa jazdy:

— państwo członkowskie wydające, nazwa organu wydającego,

— numer prawa jazdy (w dniu wydania karty).

4.5.3.2.7 Dane dotyczące zdarzeń

Do celów niniejszego podpunktu czas zachowuje się z dokładnością do 1 sekundy.

285) Karta kierowcy umożliwia przechowywanie następujących danych dotyczących zdarzeń wykrytych przez urządzenie rejestrujące przy włożonej karcie:

— nakładające się czasy (w przypadku gdy dana karta jest przyczyną zdarzenia),

— włożenie karty podczas jazdy (w przypadku gdy dana karta jest przedmiotem zdarzenia),

— sesja ostatniej karty niezamknięta prawidłowo (w przypadku gdy dana karta jest przedmiotem zdarzenia),

— przerwa w zasilaniu,

— błąd połączenia z urządzeniem do łączności na odległość,

— brak informacji o pozycji z odbiornika GNSS,

— błąd połączenia z urządzeniem zewnętrznym GNSS,

— błąd danych dotyczących ruchu,

— konflikt ruchu pojazdu,

— próba naruszenia zabezpieczenia,

— konflikt czasu.

286) Karta kierowcy umożliwia przechowywanie następujących danych dla tych zdarzeń:

— kod zdarzenia,

— data i godzina rozpoczęcia zdarzenia (lub włożenia karty, jeżeli zdarzenie trwało w tym czasie),

— data i godzina zakończenia zdarzenia (lub wyjęcia karty, jeżeli zdarzenie trwało w tym czasie),

— numer VRN i państwo członkowskie rejestracji pojazdu, w którym wystąpiło zdarzenie.

Uwaga: dla zdarzenia „nakładające się czasy":

— data i godzina rozpoczęcia zdarzenia musi odpowiadać dacie i godzinie wyjęcia karty z poprzedniego pojazdu,

— data i godzina zakończenia zdarzenia musi odpowiadać dacie i godzinie włożenia karty w bieżącym pojeździe,

— dane pojazdu muszą odpowiadać bieżącemu pojazdowi powodującemu zdarzenie.

Uwaga: dla zdarzenia „sesja ostatniej karty niezamknięta prawidłowo":

— data i godzina rozpoczęcia zdarzenia musi odpowiadać dacie i godzinie włożenia karty dla sesji niezamkniętej prawidłowo,

— data i godzina zakończenia zdarzenia musi odpowiadać dacie i godzinie włożenia karty dla sesji, w czasie której wykryto zdarzenie (bieżąca sesja),

— dane pojazdu muszą odpowiadać pojazdowi, w którym sesja nie została zamknięta prawidłowo.

287) Karta kierowcy umożliwia przechowywanie danych dotyczących sześciu ostatnich zdarzeń każdego typu (łącznie 66 zdarzeń).

4.5.3.2.8 Dane dotyczące usterek

Do celów niniejszego podpunktu czas rejestruje się z dokładnością do 1 sekundy.

288) Karta kierowcy umożliwia przechowywanie następujących danych dotyczących usterek wykrytych przez urządzenie rejestrujące przy włożonej karcie:

— usterka karty (w przypadku gdy dana karta jest przedmiotem zdarzenia),

— usterka urządzenia rejestrującego.

289) Karta kierowcy umożliwia przechowywanie następujących danych dotyczących tych usterek:

— kod usterki,

— data i godzina rozpoczęcia usterki (lub włożenia karty, jeżeli usterka trwała w tym czasie),

— data i godzina zakończenia usterki (lub wyjęcia karty, jeżeli usterka trwała w tym czasie),

— numer VRN i państwo członkowskie rejestracji pojazdu, w którym wystąpiła usterka.

290) Karta kierowcy umożliwia przechowywanie następujących danych dotyczących dwunastu ostatnich usterek każdego rodzaju (łącznie 24 usterki).

4.5.3.2.9 Dane dotyczące czynności kierowcy

291) Karta kierowcy umożliwia przechowywanie, dla każdego dnia kalendarzowego, w którym karta jest użyta, lub dla każdego dnia, dla którego kierowca ręcznie wprowadza informacje dotyczące czynności, następujących danych:

— data,

— dzienny licznik obecności (zwiększony o jeden dla każdego z tych dni kalendarzowych),

— całkowita droga przebyta przez kierowcę w ciągu tego dnia,

— status kierowcy o godzinie 00:00,

— za każdym razem, kiedy kierowca zmienia czynność lub stan prowadzenia pojazdu lub wkłada lub wyjmuje swoją kartę:

— stan prowadzenia pojazdu (ZAŁOGA, JEDEN KIEROWCA),

— szczelina czytnika (KIEROWCA, WSPÓŁKIEROWCA),

— status karty (WŁOŻONA, NIEWŁOŻONA),

— czynność (PROWADZENIE, GOTOWOŚĆ, PRACA, PRZERWA/ODPOCZYNEK),

— godzina zmiany.

292) Pamięć karty kierowcy wystarcza do przechowywania danych dotyczących czynności kierowcy przez co najmniej 28 dni (przeciętną aktywność kierowcy definiuje się jako 93 zmiany czynności dziennie).

293) Dane wyszczególnione w wymaganiach 286, 289 i 291 przechowuje się w sposób umożliwiający wyszukiwanie czynności w kolejności chronologicznej, nawet w przypadku nakładania się czasów.

4.5.3.2.10 Dane dotyczące używanych pojazdów

294) Karta kierowcy umożliwia przechowywanie, dla każdego dnia kalendarzowego, w którym karta jest użyta, i dla każdego okresu używania danego pojazdu w tym dniu (okres używania obejmuje wszystkie następujące po sobie cykle włożenia i wyjęcia karty w danym pojeździe, z perspektywy danych zapisanych na karcie), następujących danych:

— data i godzina pierwszego użycia pojazdu (tj. pierwsze włożenie karty w tym okresie używania pojazdu lub 00:00, jeżeli okres używania trwał w tym czasie),

— stan licznika kilometrów w chwili pierwszego użycia,

— data i godzina ostatniego użycia pojazdu, (tj. ostatnie wyjęcie karty w tym okresie używania pojazdu lub 23:59, jeżeli okres używania trwał w tym czasie),

— stan licznika kilometrów w chwili ostatniego użycia,

— numer VRN i państwo członkowskie rejestracji pojazdu,

— numer VIN pojazdu.

295) Karta kierowcy umożliwia przechowywanie co najmniej 84 takich rekordów danych.

4.5.3.2.11 Miejsca i pozycje rozpoczęcia lub zakończenia dziennych okresów pracy

296) Karta kierowcy umożliwia przechowywanie następujących danych dotyczących miejsc rozpoczęcia lub zakończenia dziennych okresów pracy, wprowadzanych przez kierowcę:

— data i godzina wprowadzenia danych (lub data/godzina odnosząca się do wpisu, jeżeli wpis wprowadza się w procedurze ręcznego wprowadzania danych),

— rodzaj wpisu (rozpoczęcie lub zakończenie, status wpisu),

— kraj i region,

— stan licznika kilometrów,

— pozycja pojazdu,

— dokładność GNSS, data i godzina określenia pozycji.

297) Pamięć karty kierowcy umożliwia przechowywanie co najmniej 84 par takich rekordów danych.

4.5.3.2.12 Dane sesji karty

298) Karta kierowcy umożliwia przechowywanie następujących danych dotyczących pojazdu, dla którego otwarto bieżącą sesję:

— data i godzina otwarcia sesji (tj. włożenia karty) z dokładnością do jednej sekundy,

— numer VRN i państwo członkowskie rejestracji.

4.5.3.2.13 Dane dotyczące czynności kontrolnych

299) Karta kierowcy umożliwia przechowywanie następujących danych dotyczących czynności kontrolnych:

— data i godzina kontroli,

— numer karty kontrolnej i państwo członkowskie wydające kartę,

— rodzaj kontroli (wyświetlanie lub drukowanie lub pobieranie danych z przyrządu rejestrującego lub pobieranie danych z karty – patrz uwaga),

— okres, dla którego pobrano dane, w przypadku pobierania danych,

— numer VRN i państwo członkowskie rejestracji pojazdu, w którym miała miejsce kontrola.

Uwaga: zgodnie z wymogami bezpieczeństwa pobieranie danych z karty jest rejestrowane wyłącznie wtedy, gdy jest wykonywane przez urządzenie rejestrujące.

300) Karta kierowcy umożliwia przechowywanie jednego takiego rekordu danych.

4.5.3.2.14 Dane dotyczące warunków szczególnych

301) Karta kierowcy umożliwia przechowywanie następujących danych dotyczących warunków szczególnych wprowadzonych przy włożonej karcie (niezależnie od tego, do której szczeliny czytnika):

— data i godzina wprowadzenia danych,

— rodzaj warunku szczególnego.

302) Karta kierowcy umożliwia przechowywanie co najmniej 56 takich rekordów danych.

4.5.3.2.15 Dane dotyczące używanych przyrządów rejestrujących

303) Karta kierowcy umożliwia przechowywanie następujących danych dotyczących różnych przyrządów rejestrujących, w których dana karta była używana:

— data i godzina rozpoczęcia okresu używania przyrządu rejestrującego (tj. pierwsze włożenie karty do przyrządu rejestrującego dla danego okresu),

— producent przyrządu rejestrującego,

— rodzaj przyrządu rejestrującego,

— numer wersji oprogramowania przyrządu rejestrującego.

304) Karta kierowcy umożliwia przechowywanie co najmniej 84 takich rekordów danych.

4.5.3.2.16 Dane miejsc, w których minęły trzy godziny nieprzerwanego czasu prowadzenia pojazdu

305) Karta kierowcy umożliwia przechowywanie następujących danych dotyczących pozycji pojazdu, w których nieprzerwany czas prowadzenia pojazdu przez kierowcę osiąga wielokrotność trzech godzin:

— data i godzina, o której nieprzerwany czas prowadzenia pojazdu przez posiadacza karty osiąga wielokrotność trzech godzin,

— pozycja pojazdu,

— dokładność GNSS, data i godzina określenia pozycji.

306) Karta kierowcy umożliwia przechowywanie co najmniej 252 takich rekordów danych.

4.5.4 *Karta warsztatowa*

4.5.4.1 Aplikacja tachograficzna (dostępna dla przyrządów rejestrujących pierwszej i drugiej generacji)

4.5.4.1.1 Identyfikacja aplikacji

307) Karta warsztatowa umożliwia przechowywanie następujących danych identyfikujących aplikację:

— identyfikacja aplikacji tachograficznej,

— identyfikacja typu karty do tachografów.

4.5.4.1.2 Klucze i certyfikaty

308) Karta warsztatowa umożliwia przechowywanie szeregu kluczy i certyfikatów kryptograficznych, jak określono w dodatku 11 część A.

309) Karta warsztatowa umożliwia przechowywanie osobistego numeru identyfikacyjnego (kodu PIN).

4.5.4.1.3 Identyfikacja karty

310) Karta warsztatowa umożliwia przechowywanie następujących danych identyfikujących kartę:

— numer karty,

— państwo członkowskie wydające kartę, nazwa organu wydającego, data wydania,

— data rozpoczęcia okresu ważności karty, termin ważności karty.

4.5.4.1.4 Identyfikacja posiadacza karty

311) Karta warsztatowa umożliwia przechowywanie następujących danych identyfikujących posiadacza karty:

— nazwa warsztatu,

— adres warsztatu,

— nazwisko posiadacza karty,

— imię (imiona) posiadacza karty,

— preferowany język.

4.5.4.1.5 Pobieranie danych z karty

312) Karta warsztatowa umożliwia przechowywanie rekordu danych pobranych z karty, w taki sam sposób jak karta kierowcy.

4.5.4.1.6 Dane dotyczące kalibracji i korekty czasu

313) Karta warsztatowa umożliwia przechowywanie zapisów dotyczących kalibracji lub korekty czasu wykonanych przy karcie włożonej do urządzenia rejestrującego.

314) Każdy rekord danych kalibracji może zawierać następujące dane:

— cel kalibracji (aktywacja, pierwsza instalacja, instalacja, przegląd okresowy),

— identyfikacja pojazdu,

— parametry uaktualnione lub potwierdzone (w, k, l, rozmiar opon, ustawienie urządzenia ograniczenia prędkości, licznik kilometrów (nowe i stare wartości), data i godzina (nowe i stare wartości)),

— identyfikacja urządzenia rejestrującego (numer części VU, numer seryjny VU, numer seryjny czujnika ruchu).

315) Karta warsztatowa umożliwia przechowywanie co najmniej 88 takich rekordów danych.

316) Karta warsztatowa jest wyposażona w licznik pokazujący łączną liczbę kalibracji wykonanych przy użyciu tej karty.

317) Karta warsztatowa jest wyposażona w licznik pokazujący liczbę kalibracji wykonanych od ostatniego pobrania danych.

4.5.4.1.7 Dane dotyczące zdarzeń i usterek

318) Karta warsztatowa umożliwia przechowywanie rekordów danych zdarzeń i usterek, w taki sam sposób jak karta kierowcy.

319) Karta warsztatowa umożliwia przechowywanie danych dotyczących trzech ostatnich zdarzeń każdego rodzaju (łącznie 18 zdarzeń) i sześciu ostatnich usterek każdego rodzaju (łącznie 12 usterek).

4.5.4.1.8 Dane dotyczące czynności kierowcy

320) Karta warsztatowa umożliwia przechowywanie danych dotyczących czynności kierowcy, w taki sam sposób jak karta kierowcy.

321) Karta warsztatowa umożliwia przechowywanie danych dotyczących czynności kierowcy za co najmniej 1 dzień przeciętnej aktywności kierowcy.

4.5.4.1.9 Dane dotyczące używanych pojazdów

322) Karta warsztatowa umożliwia przechowywanie rekordów danych dotyczących używanego pojazdu, w taki sam sposób jak karta kierowcy.

323) Karta warsztatowa umożliwia przechowywanie co najmniej 4 takich rekordów.

4.5.4.1.10 Dane dotyczące rozpoczęcia lub zakończenia dziennych okresów pracy

324) Karta warsztatowa umożliwia przechowywanie rekordów danych dotyczących rozpoczęcia lub zakończenia dziennych okresów pracy, w taki sam sposób jak karta kierowcy.

325) Karta warsztatowa umożliwia przechowywanie co najmniej 3 par takich rekordów danych.

4.5.4.1.11 Dane sesji karty

326) Karta warsztatowa umożliwia przechowywanie rekordu danych sesji karty, w taki sam sposób jak karta kierowcy.

4.5.4.1.12 Dane dotyczące czynności kontrolnych

327) Karta warsztatowa umożliwia przechowywanie rekordu danych czynności kontrolnych, w taki sam sposób jak karta kierowcy.

4.5.4.1.13 Dane dotyczące warunków szczególnych

328) Karta warsztatowa umożliwia przechowywanie danych dotyczących warunków szczególnych, w taki sam sposób jak karta kierowcy.

329) Karta warsztatowa umożliwia przechowywanie co najmniej 2 takich rekordów.

4.5.4.2 Aplikacja tachograficzna 2. generacji (niedostępna dla przyrządów rejestrujących pierwszej generacji)

4.5.4.2.1 Identyfikacja aplikacji

330) Karta warsztatowa umożliwia przechowywanie następujących danych identyfikujących aplikację:

— identyfikacja aplikacji tachograficznej,

— identyfikacja typu karty do tachografów.

4.5.4.2.2 Klucze i certyfikaty

331) Karta warsztatowa umożliwia przechowywanie szeregu kluczy i certyfikatów kryptograficznych, jak określono w dodatku 11 część B.

332) Karta warsztatowa umożliwia przechowywanie osobistego numeru identyfikacyjnego (kodu PIN).

4.5.4.2.3 Identyfikacja karty

333) Karta warsztatowa umożliwia przechowywanie następujących danych identyfikujących kartę:

— numer karty,

— państwo członkowskie wydające kartę, nazwa organu wydającego, data wydania,

— data rozpoczęcia okresu ważności karty, termin ważności karty.

4.5.4.2.4 Identyfikacja posiadacza karty

334) Karta warsztatowa umożliwia przechowywanie następujących danych identyfikujących posiadacza karty:

— nazwa warsztatu,

— adres warsztatu,

— nazwisko posiadacza karty,

— imię (imiona) posiadacza karty,

— preferowany język.

4.5.4.2.5 Pobieranie danych z karty

335) Karta warsztatowa umożliwia przechowywanie rekordu danych pobranych z karty, w taki sam sposób jak karta kierowcy.

4.5.4.2.6 Dane dotyczące kalibracji i korekty czasu

336) Karta warsztatowa umożliwia przechowywanie zapisów dotyczących kalibracji lub korekty czasu wykonanych przy karcie włożonej do urządzenia rejestrującego.

337) Każdy rekord danych kalibracji może zawierać następujące dane:

— cel kalibracji (aktywacja, pierwsza instalacja, instalacja, przegląd okresowy),

— identyfikacja pojazdu,

— parametry uaktualnione lub potwierdzone (w, k, l, rozmiar opon, ustawienie urządzenia ograniczenia prędkości, licznik kilometrów (nowe i stare wartości), data i godzina (nowe i stare wartości)),

— identyfikacja urządzenia rejestrującego (numer części VU, numer seryjny VU, numer seryjny czujnika ruchu, numer seryjny urządzenia do łączności na odległość, numer seryjny urządzenia zewnętrznego GNSS, w stosownych przypadkach),

— rodzaje i identyfikatory wszystkich założonych plomb,

— możliwość korzystania przez przyrząd rejestrujący z kart do tachografów pierwszej generacji (włączona lub nie).

338) Karta warsztatowa umożliwia przechowywanie co najmniej 88 takich rekordów danych.

339) Karta warsztatowa jest wyposażona w licznik pokazujący łączną liczbę kalibracji wykonanych przy użyciu tej karty.

340) Karta warsztatowa jest wyposażona w licznik pokazujący liczbę kalibracji wykonanych od ostatniego pobrania danych.

4.5.4.2.7 Dane dotyczące zdarzeń i usterek

341) Karta warsztatowa umożliwia przechowywanie rekordów danych zdarzeń i usterek, w taki sam sposób jak karta kierowcy.

342) Karta warsztatowa umożliwia przechowywanie danych dotyczących trzech ostatnich zdarzeń każdego rodzaju (łącznie 33 zdarzenia) i sześciu ostatnich usterek każdego rodzaju (łącznie 12 usterek).

4.5.4.2.8 Dane dotyczące czynności kierowcy

343) Karta warsztatowa umożliwia przechowywanie danych dotyczących czynności kierowcy, w taki sam sposób jak karta kierowcy.

344) Karta warsztatowa umożliwia przechowywanie danych dotyczących czynności kierowcy za co najmniej 1 dzień przeciętnej aktywności kierowcy.

4.5.4.2.9 Dane dotyczące używanych pojazdów

345) Karta warsztatowa umożliwia przechowywanie rekordów danych dotyczących używanego pojazdu, w taki sam sposób jak karta kierowcy.

346) Karta warsztatowa umożliwia przechowywanie co najmniej 4 takich rekordów.

4.5.4.2.10 Dane dotyczące rozpoczęcia lub zakończenia dziennych okresów pracy

347) Karta warsztatowa umożliwia przechowywanie rekordów danych dotyczących rozpoczęcia lub zakończenia dziennych okresów pracy, w taki sam sposób jak karta kierowcy.

348) Karta warsztatowa umożliwia przechowywanie co najmniej 3 par takich rekordów danych.

4.5.4.2.11 Dane sesji karty

349) Karta warsztatowa umożliwia przechowywanie rekordu danych sesji karty, w taki sam sposób jak karta kierowcy.

4.5.4.2.12 Dane dotyczące czynności kontrolnych

350) Karta warsztatowa umożliwia przechowywanie rekordu danych czynności kontrolnych, w taki sam sposób jak karta kierowcy.

4.5.4.2.13 Dane dotyczące używanych przyrządów rejestrujących

351) Karta warsztatowa umożliwia przechowywanie następujących danych dotyczących różnych przyrządów rejestrujących, w których dana karta była używana:

— data i godzina rozpoczęcia okresu używania przyrządu rejestrującego (tj. pierwsze włożenie karty do przyrządu rejestrującego dla danego okresu),

— producent przyrządu rejestrującego,

— rodzaj przyrządu rejestrującego,

— numer wersji oprogramowania przyrządu rejestrującego.

352) Karta warsztatowa umożliwia przechowywanie co najmniej 4 takich rekordów.

4.5.4.2.14 Dane miejsc, w których minęły trzy godziny nieprzerwanego czasu prowadzenia pojazdu

353) Karta warsztatowa umożliwia przechowywanie następujących danych dotyczących pozycji pojazdu, w których nieprzerwany czas prowadzenia pojazdu przez kierowcę osiąga wielokrotność trzech godzin:

— data i godzina, o której nieprzerwany czas prowadzenia pojazdu przez posiadacza karty osiąga wielokrotność trzech godzin,

— pozycja pojazdu,

— dokładność GNSS, data i godzina określenia pozycji.

354) Karta warsztatowa umożliwia przechowywanie co najmniej 18 takich rekordów.

4.5.4.2.15 Dane dotyczące warunków szczególnych

355) Karta warsztatowa umożliwia przechowywanie danych dotyczących warunków szczególnych, w taki sam sposób jak karta kierowcy.

356) Karta warsztatowa umożliwia przechowywanie co najmniej 2 takich rekordów.

4.5.5 *Karta kontrolna*

4.5.5.1 Aplikacja tachograficzna (dostępna dla przyrządów rejestrujących pierwszej i drugiej generacji)

4.5.5.1.1 Identyfikacja aplikacji

357) Karta kontrolna umożliwia przechowywanie następujących danych identyfikujących aplikację:

— identyfikacja aplikacji tachograficznej,

— identyfikacja typu karty do tachografów.

4.5.5.1.2 Klucze i certyfikaty

358) Karta kontrolna umożliwia przechowywanie szeregu kluczy i certyfikatów kryptograficznych, jak określono w dodatku 11 część A.

4.5.5.1.3 Identyfikacja karty

359) Karta kontrolna umożliwia przechowywanie następujących danych identyfikujących kartę:

— numer karty,

— państwo członkowskie wydające kartę, nazwa organu wydającego, data wydania,

— data rozpoczęcia okresu ważności karty, termin ważności karty (jeżeli jest określony).

4.5.5.1.4 Identyfikacja posiadacza karty

360) Karta kontrolna umożliwia przechowywanie następujących danych identyfikujących posiadacza karty:

— nazwa organu kontrolnego,

— adres organu kontrolnego,

— nazwisko posiadacza karty,

— imię (imiona) posiadacza karty,

— preferowany język.

4.5.5.1.5 Dane dotyczące czynności kontrolnych

361) Karta kontrolna umożliwia przechowywanie następujących danych dotyczących czynności kontrolnych:

— data i godzina kontroli,

— rodzaj kontroli (wyświetlanie lub drukowanie lub pobieranie danych z przyrządu rejestrującego lub karty lub kontrola drogowa kalibracji),

— okres, dla którego pobrano dane (jeżeli ma zastosowanie),

— numer VRN i państwo członkowskie rejestracji kontrolowanego pojazdu,

— numer karty i państwo członkowskie wydające kontrolowaną kartę kierowcy.

362) Karta kontrolna umożliwia przechowywanie co najmniej 230 takich rekordów danych.

4.5.5.2 Aplikacja tachograficzna 2. generacji (niedostępna dla przyrządów rejestrujących pierwszej generacji)

4.5.5.2.1 Identyfikacja aplikacji

363) Karta kontrolna umożliwia przechowywanie następujących danych identyfikujących aplikację:

— identyfikacja aplikacji tachograficznej,

— identyfikacja typu karty do tachografów.

4.5.5.2.2 Klucze i certyfikaty

364) Karta kontrolna umożliwia przechowywanie szeregu kluczy i certyfikatów kryptograficznych, jak określono w dodatku 11 część B.

4.5.5.2.3 Identyfikacja karty

365) Karta kontrolna umożliwia przechowywanie następujących danych identyfikujących kartę:

— numer karty,

— państwo członkowskie wydające kartę, nazwa organu wydającego, data wydania,

— data rozpoczęcia okresu ważności karty, termin ważności karty (jeżeli jest określony).

4.5.5.2.4 Identyfikacja posiadacza karty

366) Karta kontrolna umożliwia przechowywanie następujących danych identyfikujących posiadacza karty:

— nazwa organu kontrolnego,

— adres organu kontrolnego,

— nazwisko posiadacza karty,

— imię (imiona) posiadacza karty,

— preferowany język.

4.5.5.2.5 Dane dotyczące czynności kontrolnych

367) Karta kontrolna umożliwia przechowywanie następujących danych dotyczących czynności kontrolnych:

— data i godzina kontroli,

— rodzaj kontroli (wyświetlanie lub drukowanie lub pobieranie danych z przyrządu rejestrującego lub karty lub kontrola drogowa kalibracji),

— okres, dla którego pobrano dane (jeżeli ma zastosowanie),

— numer VRN i państwo członkowskie rejestracji kontrolowanego pojazdu,

— numer karty i państwo członkowskie wydające kontrolowaną kartę kierowcy.

368) Karta kontrolna umożliwia przechowywanie co najmniej 230 takich rekordów danych.

4.5.6 *Karta firmowa*

4.5.6.1 Aplikacja tachograficzna (dostępna dla przyrządów rejestrujących pierwszej i drugiej generacji)

4.5.6.1.1 Identyfikacja aplikacji

369) Karta firmowa umożliwia przechowywanie następujących danych identyfikujących aplikację:

— identyfikacja aplikacji tachograficznej,

— identyfikacja typu karty do tachografów.

4.5.6.1.2 Klucze i certyfikaty

370) Karta firmowa umożliwia przechowywanie szeregu kluczy i certyfikatów kryptograficznych, jak określono w dodatku 11 część A.

4.5.6.1.3 Identyfikacja karty

371) Karta firmowa umożliwia przechowywanie następujących danych identyfikujących kartę:

— numer karty,

— państwo członkowskie wydające kartę, nazwa organu wydającego, data wydania,

— data rozpoczęcia okresu ważności karty, termin ważności karty (jeżeli jest określony).

4.5.6.1.4 Identyfikacja posiadacza karty

372) Karta firmowa umożliwia przechowywanie następujących danych identyfikujących posiadacza karty:

— nazwa firmy,

— adres firmy.

4.5.6.1.5 Dane dotyczące czynności wykonywanych przez firmę

373) Karta firmowa umożliwia przechowywanie następujących danych dotyczących czynności wykonywanych przez firmę:

— data i godzina czynności,

— typ czynności (blokowanie lub zdejmowanie blokady z przyrządu rejestrującego lub pobieranie danych z przyrządu rejestrującego lub pobieranie danych z karty),

— okres, dla którego pobrano dane (jeżeli ma zastosowanie),

— numer VRN i państwo członkowskie rejestracji pojazdu,

— numer karty i państwo członkowskie wydające kartę (w przypadku pobierania danych z karty).

374) Karta firmowa umożliwia przechowywanie co najmniej 230 takich rekordów danych.

4.5.6.2 Aplikacja tachograficzna 2. generacji (niedostępna dla przyrządów rejestrujących pierwszej generacji)

4.5.6.2.1 Identyfikacja aplikacji

375) Karta firmowa umożliwia przechowywanie następujących danych identyfikujących aplikację:

— identyfikacja aplikacji tachograficznej,

— identyfikacja typu karty do tachografów.

4.5.6.2.2 Klucze i certyfikaty

376) Karta firmowa umożliwia przechowywanie szeregu kluczy i certyfikatów kryptograficznych, jak określono w dodatku 11 część B.

4.5.6.2.3 Identyfikacja karty

377) Karta firmowa umożliwia przechowywanie następujących danych identyfikujących kartę:

— numer karty,

— państwo członkowskie wydające kartę, nazwa organu wydającego, data wydania,

— data rozpoczęcia okresu ważności karty, termin ważności karty (jeżeli jest określony).

4.5.6.2.4 Identyfikacja posiadacza karty

378) Karta firmowa umożliwia przechowywanie następujących danych identyfikujących posiadacza karty:

— nazwa firmy,

— adres firmy.

4.5.6.2.5 Dane dotyczące czynności wykonywanych przez firmę

379) Karta firmowa umożliwia przechowywanie następujących danych dotyczących czynności wykonywanych przez firmę:

— data i godzina czynności,

— typ czynności (blokowanie lub zdejmowanie blokady z przyrządu rejestrującego lub pobieranie danych z przyrządu rejestrującego lub pobieranie danych z karty),

— okres, dla którego pobrano dane (jeżeli ma zastosowanie),

— numer VRN i państwo członkowskie rejestracji pojazdu,

— numer karty i państwo członkowskie wydające kartę (w przypadku pobierania danych z karty).

380) Karta firmowa umożliwia przechowywanie co najmniej 230 takich rekordów danych.

5 INSTALACJA URZĄDZENIA REJESTRUJĄCEGO

5.1 **Instalacja**

381) Nowe urządzenie rejestrujące dostarcza się instalatorom lub producentom pojazdów w stanie nieaktywowanym, ze wszystkimi parametrami kalibracyjnymi, wyszczególnionymi w rozdziale 3.21, ustawionymi na odpowiednie i prawidłowe wartości domyślne. W przypadku gdy nie ma konkretnej odpowiedniej wartości, parametry literowe należy ustawić jako łańcuchy znaków „?", a parametry liczbowe jako „0". Dostawę części układu zabezpieczającego urządzeń rejestrujących można w razie konieczności ograniczyć podczas certyfikacji bezpieczeństwa.

382) Przed aktywacją urządzenie rejestrujące umożliwia dostęp do funkcji kalibracji, nawet jeśli nie jest w trybie kalibracyjnym.

383) Przed aktywacją urządzenie rejestrujące nie może rejestrować ani przechowywać danych, o których mowa w pkt 3.12.3, 3.12.9 oraz 3.12.12–3.12.15.

384) W czasie instalacji producenci pojazdów wstępnie ustawiają wszystkie znane parametry.

385) Producenci pojazdów lub instalatorzy aktywują zainstalowane urządzenie rejestrujące najpóźniej przed rozpoczęciem korzystania z pojazdu w zakresie objętym rozporządzeniem (WE) nr 561/2006.

386) Aktywacja urządzenia rejestrującego uruchamiana jest automatycznie przez pierwsze włożenie ważnej karty warsztatowej do któregokolwiek czytnika karty.

387) Szczególne czynności parujące, wymagane między czujnikiem ruchu a przyrządem rejestrującym, odbywają się w razie potrzeby automatycznie przed aktywacją lub w trakcie aktywacji.

388) Podobnie szczególne czynności powiązania, wymagane między urządzeniem zewnętrznym GNSS a przyrządem rejestrującym, odbywają się w razie potrzeby automatycznie przed aktywacją lub w czasie aktywacji.

389) Po aktywowaniu urządzenia rejestrującego wszystkie funkcje i prawa dostępu do danych muszą być w pełni wdrożone.

390) Po aktywowaniu urządzenie rejestrujące przekazuje do urządzenia do łączności na odległość zabezpieczone dane niezbędne na potrzeby ukierunkowanych kontroli drogowych.

391) Po aktywowaniu urządzenia rejestrującego funkcje rejestrowania i przechowywania muszą być w pełni funkcjonalne.

392) Następnym krokiem po instalacji jest kalibracja. Podczas pierwszej kalibracji nie jest konieczne wprowadzenie numeru rejestracyjnego pojazdu (VRN), jeżeli nie jest on znany zatwierdzonemu warsztatowi mającemu przeprowadzić kalibrację. W tej sytuacji, i tylko wtedy, właściciel pojazdu może wprowadzić numer VRN, używając swojej karty firmowej przed rozpoczęciem korzystania z pojazdu w zakresie objętym rozporządzeniem (WE) nr 561/2006 (np. używając poleceń poprzez odpowiednie menu interfejsu człowiek-maszyna przyrządu rejestrującego) ([1]). Każda aktualizacja lub potwierdzenie wprowadzonych w ten sposób danych są możliwe jedynie przy użyciu karty warsztatowej.

393) Instalacja urządzenia zewnętrznego GNSS wymaga powiązania z przyrządem rejestrującym, a następnie weryfikacji informacji o pozycji GNSS.

394) Urządzenie rejestrujące musi być umieszczone w pojeździe w taki sposób, aby kierowca miał ze swojego siedzenia dostęp do niezbędnych funkcji.

([1]) Dz.U. L 102 z 11.4.2006, s. 1.

5.2 **Tabliczka instalacyjna**

395) Po zainstalowaniu i sprawdzeniu urządzenia rejestrującego mocuje się na nim dobrze widoczną i łatwo dostępną tabliczkę instalacyjną, wygrawerowaną lub nadrukowaną w trwały sposób. Jeżeli nie jest to możliwe, tabliczkę mocuje się na słupku „B" pojazdu, tak aby była dobrze widoczna. W przypadku pojazdów, które nie posiadają słupka „B", tabliczkę instalacyjną należy umocować na ościeżnicy po stronie kierowcy pojazdu, tak aby zawsze była dobrze widoczna.

Po każdym przeglądzie przeprowadzonym przez zatwierdzonego instalatora lub warsztat, w miejsce starej tabliczki mocuje się nową.

396) Tabliczka zawiera co najmniej następujące dane:

— nazwa, adres lub nazwa handlowa zatwierdzonego instalatora lub warsztatu,

— współczynnik charakterystyczny pojazdu, w postaci „w = …imp/km",

— stała urządzenia rejestrującego, w postaci „k = …imp/km",

— obwód toczny opon, w postaci „l = …mm",

— rozmiar opon,

— data pomiaru współczynnika charakterystycznego pojazdu i obwodu tocznego opon,

— numer identyfikacyjny pojazdu,

— obecność (lub brak) urządzenia zewnętrznego GNSS,

— numer seryjny urządzenia zewnętrznego GNSS,

— numer seryjny urządzenia do łączności na odległość,

— numer seryjny wszystkich założonych plomb,

— część pojazdu, w której zamontowany jest ewentualny adapter,

— część pojazdu, w której zamontowany jest czujnik ruchu, jeżeli nie jest podłączony do skrzyni biegów lub w przypadku niezastosowania adaptera,

— kolor przewodu łączącego adapter z częścią pojazdu, z której dochodzą impulsy,

— numer seryjny czujnika ruchu wbudowanego w adapter.

397) Drugą dodatkową tabliczkę można użyć tylko w pojazdach M1 i N1, w których zainstalowany jest adapter zgodnie z rozporządzeniem Komisji (WE) nr 68/2009 ([1]) z późniejszymi zmianami, oraz gdy nie ma możliwości zamieszczenia wszystkich niezbędnych informacji opisanych w wymaganiu 396. W takich przypadkach na dodatkowej tabliczce zamieszczane są co najmniej ostatnie cztery tiret określone w wymaganiu 396.

Drugą dodatkową tabliczkę mocuje się w stosownych przypadkach obok lub w pobliżu pierwszej podstawowej tabliczki opisanej w wymaganiu 396 i zapewnia się jej taki sam poziom ochrony. Na dodatkowej tabliczce umieszcza się ponadto nazwę, adres lub nazwę handlową zatwierdzonego instalatora lub warsztatu, który dokonał instalacji, oraz datę instalacji.

([1]) Rozporządzenie Komisji (WE) nr 68/2009 z dnia 23 stycznia 2009 r. dostosowujące do postępu technicznego po raz dziewiąty rozporządzenie Rady (EWG) nr 3821/85 w sprawie urządzeń rejestrujących stosowanych w transporcie drogowym (Dz.U. L 21 z 24.1.2009, s. 3).

5.3 **Plombowanie**

398) Następujące części muszą być zaplombowane:

— Wszelkie połączenia, których rozłączenie może powodować niewykrywalne zmiany danych lub niewykrywalne utraty danych (może to dotyczyć np. instalacji czujnika ruchu na skrzyni biegów, adapterów w pojazdach M1/N1, połączenia z urządzeniem zewnętrznym GNSS lub przyrządu rejestrującego);

— Tabliczka instalacyjna, chyba że jest przymocowana w taki sposób, że nie można jej usunąć bez uszkodzenia wykonanych na niej oznaczeń.

399) Plomby, o których mowa powyżej, mogą być usunięte:

— w nagłych przypadkach,

— w celu zainstalowania, wyregulowania lub naprawy urządzenia ograniczenia prędkości lub innego urządzenia istotnego dla bezpieczeństwa drogowego, z zastrzeżeniem że urządzenie rejestrujące nadal pracuje niezawodnie i prawidłowo i zostanie powtórnie zaplombowane przez zatwierdzonego instalatora lub warsztat (zgodnie z rozdziałem 6) niezwłocznie po zainstalowaniu urządzenia ograniczenia prędkości lub innego urządzenia istotnego dla bezpieczeństwa drogowego lub w terminie siedmiu dni w pozostałych przypadkach.

400) Każdy przypadek zdjęcia takiej plomby wymaga sporządzenia pisemnego oświadczenia podającego powody takiego działania, a oświadczenie to udostępniane jest właściwemu organowi.

401) Plomby muszą mieć numer identyfikacyjny przydzielony przez ich producenta. Numer ten jest niepowtarzalny i różny od innych numerów plomb przydzielonych przez innych producentów plomb.

Ten niepowtarzalny numer identyfikacyjny jest określony w następujący sposób: MM NNNNNN w formie niedającego się usunąć oznakowania, gdzie MM to jednoznaczny identyfikator producenta (numer w bazie danych prowadzonej przez KE), a NNNNNN to numer alfanumeryczny plomby, niepowtarzalny dla danego producenta.

402) Na plombie musi być wolne miejsce, na którym zatwierdzeni instalatorzy, warsztaty lub producenci pojazdów mogą dodać specjalny znak zgodnie z art. 22 ust. 3 rozporządzenia (UE) nr 165/2014.

Znak ten nie może zakrywać numeru identyfikacyjnego plomby.

403) Producenci plomb muszą być zarejestrowani w specjalnej bazie danych i muszą udostępniać publicznie numery identyfikacyjne plomb w procedurze, którą ma określić Komisja Europejska.

404) Zatwierdzone warsztaty i producenci pojazdów korzystają, w ramach rozporządzenia (UE) nr 165/2014, wyłącznie z plomb od producentów plomb zapisanych w bazie danych, o której mowa powyżej.

405) Producenci plomb i ich dystrybutorzy zachowują pełną dokumentację umożliwiającą identyfikowalność plomb sprzedawanych do użytku w ramach rozporządzenia (UE) nr 165/2014 i są gotowi do jej przedłużenia właściwym organom krajowym w razie potrzeby.

406) Niepowtarzalne numery identyfikacyjne plomb muszą być widoczne na tabliczce instalacyjnej.

6 KONTROLE, PRZEGLĄDY I NAPRAWY

Wymagania odnośnie do okoliczności, w jakich można usunąć plomby, określone w art. 22 ust. 5 rozporządzenia (UE) nr 165/2014, zostały zdefiniowane w rozdziale 5.3 niniejszego załącznika.

6.1 **Zatwierdzanie instalatorów, warsztatów i producentów pojazdów**

Państwa członkowskie zatwierdzają, regularnie kontrolują i certyfikują instytucje odpowiadające za:

— instalacje,

— kontrole,

— przeglądy,

— naprawy.

Karty warsztatowe wydaje się wyłącznie instalatorom lub warsztatom zatwierdzonym do aktywowania lub kalibrowania urządzeń rejestrujących zgodnie z niniejszym załącznikiem i, chyba że istnieją inne należyte uzasadnienia,

— którzy nie kwalifikują się do posiadania karty firmowej,

— i których inna działalność zawodowa nie stanowi potencjalnego zagrożenia dla ogólnego bezpieczeństwa systemu zgodnie z wymogami w dodatku 10.

6.2 **Kontrola techniczna przyrządów nowych i po naprawie**

407) Każdy przyrząd, tak nowy, jak i po naprawie, jest kontrolowany pod względem prawidłowego funkcjonowania oraz dokładności odczytów i rejestracji, w granicach określonych w rozdziale 3.2.1, 3.2.2, 3.2.3 oraz 3.3 poprzez zaplombowanie zgodnie z rozdziałem 5.3 oraz kalibrację.

6.3 **Przegląd instalacyjny**

408) Po zainstalowaniu w pojeździe cała instalacja (włącznie z urządzeniem rejestrującym) musi być zgodna z przepisami dotyczącymi maksymalnych tolerancji ustanowionymi w rozdziałach 3.2.1, 3.2.2, 3.2.3 i 3.3.

6.4 **Przeglądy okresowe**

409) Przeglądy okresowe urządzeń zainstalowanych w pojazdach przeprowadza się po każdej naprawie urządzenia lub po jakiejkolwiek zmianie współczynnika charakterystycznego pojazdu lub obwodu tocznego opon, lub gdy czas UTC urządzenia różni się od czasu UTC o więcej niż 20 minut, lub przy zmianie numeru VRN i przynajmniej raz w okresie dwóch lat (24 miesięcy) od ostatniej kontroli.

410) Przeglądy te obejmują następujące kontrole:

— czy urządzenie rejestrujące działa prawidłowo, włącznie z funkcją przechowywania danych na kartach do tachografów oraz łącznością z czytnikami na odległość,

— czy jest zachowana zgodność z wymaganiami rozdziału 3.2.1 i 3.2.2 co do maksymalnych tolerancji przy instalacji,

— czy jest zachowana zgodność z przepisami rozdziałów 3.2.3 i 3.3,

— czy urządzenie rejestrujące opatrzone jest znakiem homologacji typu,

— czy tabliczka instalacyjna określona w wymaganiu 396 oraz tabliczka określona w wymaganiu 225 są zamocowane,

— rozmiaru opon i faktycznego obwodu tocznego opon,

— czy do urządzenia nie są podłączone żadne urządzenia służące do manipulacji,

— czy plomby są prawidłowo założone, w dobrym stanie, czy ich numery identyfikacyjne są ważne (producent plomb zatwierdzony w bazie KE) oraz czy ich numery identyfikacyjne odpowiadają oznakowaniom na tabliczce instalacyjnej (zob. wymaganie 401).

411) Jeżeli jedno ze zdarzeń wymienionych w rozdziale 3.9 (Wykrywanie zdarzeń lub usterek) pojawiło się od czasu poprzedniego przeglądu i producenci tachografów lub organy krajowe uważają, że stwarza ono zagrożenie dla bezpieczeństwa urządzenia, warsztat:

a. porównuje dane identyfikacyjne czujnika ruchu podłączonego do skrzyni biegów z danymi sparowanego czujnika ruchu zarejestrowanymi w przyrządzie rejestrującym;

b. sprawdza, czy informacje zapisane na tabliczce instalacyjnej są zgodne z informacjami zawartymi w przyrządzie rejestrującym;

c. sprawdza, czy numer seryjny czujnika ruchu i numer homologacji, jeżeli są nadrukowane na obudowie czujnika ruchu, są zgodne z informacjami przechowywanymi w pamięci danych urządzenia rejestrującego;

d. porównuje dane identyfikacyjne umieszczone na tabliczce znamionowej ewentualnego urządzenia zewnętrznego GNSS z danymi przechowywanymi w pamięci danych przyrządu rejestrującego.

412) Warsztaty odnotowują w swoich sprawozdaniach z przeglądu wszystkie ustalenia dotyczące zniszczonych plomb lub urządzeń służących do manipulacji. Warsztaty przechowują przedmiotowe sprawozdania co najmniej przez 2 lata i udostępniają je każdorazowo na wniosek właściwego organu.

413) W ramach przeglądów wykonuje się kalibrację i zapobiegawczą wymianę plomb, za których montaż odpowiadają warsztaty.

6.5 **Wyznaczanie błędów**

414) Wyznaczanie błędów po zainstalowaniu i podczas użytkowania jest wykonywane w następujących warunkach, które stanowią warunki odniesienia:

— pojazd bez obciążenia w stanie gotowym do jazdy,

— ciśnienie w ogumieniu zgodne z instrukcjami producenta,

— zużycie ogumienia w granicach dopuszczalnych przepisami krajowymi,

— ruch pojazdu:

— pojazd porusza się napędzany własnym silnikiem, po linii prostej i po poziomej powierzchni, z prędkością 50 ± 5 km/h. Odległość pomiarowa wynosi przynajmniej 1 000 m.

— sprawdzenie może być również przeprowadzone inną metodą, np. na odpowiednim stanowisku warsztatowym, pod warunkiem że zapewni ono porównywalną dokładność.

6.6 **Naprawy**

415) Warsztaty mogą pobierać dane z urządzenia rejestrującego w celu przekazania tych danych odpowiedniej firmie przewozowej.

416) Zatwierdzone warsztaty wydają firmom przewozowym zaświadczenie o niemożliwości pobrania danych, w przypadku gdy uszkodzenie urządzenia rejestrującego uniemożliwia pobranie zarejestrowanych danych nawet po naprawie w tym warsztacie. Warsztaty przechowują kopię każdego wydanego zaświadczenia przez okres co najmniej dwóch lat.

7 WYDAWANIE KART

Procedury wydawania kart określone przez państwa członkowskie spełniają następujące wymagania:

417) Pierwsza karta do tachografów wydana wnioskodawcy ma numer karty równy numerowi kolejnemu (jeżeli ma zastosowanie), a numer wymiany i numer odnowienia ustawione na „0”.

418) Numery karty wszystkich nieosobistych kart do tachografów wydanych jednemu organowi kontrolnemu lub jednemu warsztatowi lub jednej firmie przewozowej mają te same pierwsze 13 cyfr i wszystkie mają różny numer kolejny.

419) Karta do tachografów wydana jako duplikat istniejącej karty do tachografów ma ten sam numer karty co karta zastąpiona, z wyjątkiem numeru wymiany, który jest zwiększany o „1” (w kolejności 0, …, 9, A, …, Z).

420) Karta do tachografów wydana jako duplikat istniejącej karty do tachografów ma ten sam termin ważności karty co karta zastąpiona.

421) Karta do tachografów wydana jako odnowienie istniejącej karty do tachografów ma ten sam numer karty co karta odnowiona, z wyjątkiem numeru wymiany, który jest ustawiony na „0" i numeru odnowienia, który jest zwiększany o „1" (w kolejności 0, …, 9, A, …, Z).

422) Przy wymianie istniejącej karty do tachografów w celu zmiany danych administracyjnych stosuje się te same zasady co przy odnawianiu, jeżeli odbywa się w tym samym państwie członkowskim, lub te same zasady co przy pierwszym wydaniu, jeżeli odbywa się w innym państwie członkowskim.

423) W rubryce „nazwisko posiadacza karty" w przypadku nieosobistych kart warsztatowych lub kontrolnych wpisuje się albo nazwę warsztatu lub organu kontrolnego albo nazwisko instalatora lub funkcjonariusza służb kontrolnych, według uznania państw członkowskich.

424) Państwa członkowskie wymieniają dane drogą elektroniczną w celu zapewnienia niepowtarzalności wydawanych kart kierowcy zgodnie z art. 31 rozporządzenia (UE) nr 165/2014.

8 HOMOLOGACJA TYPU URZĄDZEŃ REJESTRUJĄCYCH I KART DO TACHOGRAFÓW

8.1 **Uwagi ogólne**

Do celów niniejszego rozdziału wyrażenie „urządzenie rejestrujące" oznacza „urządzenie rejestrujące lub jego elementy składowe". Homologacji typu nie wymaga się dla przewodu(-ów) łączącego(-ych) czujnik ruchu z przyrządem rejestrującym, urządzenie zewnętrzne GNSS z przyrządem rejestrującym lub urządzenie do łączności na odległość z przyrządem rejestrującym. Papier używany przez urządzenie rejestrujące uważa się za element składowy urządzenia rejestrującego.

Każdy producent może zwrócić się o homologację typu jego elementu składowego z każdym typem czujnika ruchu, urządzenia zewnętrznego GNSS i odwrotnie, pod warunkiem że każdy element jest zgodny z wymaganiami w niniejszym załączniku. Producenci mogą również zwrócić się o homologację typu urządzenia rejestrującego.

425) Urządzenie rejestrujące dostarcza się do homologacji w stanie kompletnym z wszystkimi zintegrowanymi urządzeniami dodatkowymi.

426) Homologacja typu urządzenia rejestrującego i kart do tachografów obejmuje badania związane z bezpieczeństwem, badania funkcjonalności i badania interoperacyjności. Pozytywne wyniki każdego z tych badań potwierdza się odpowiednim świadectwem.

427) Organy homologacji typu w państwach członkowskich nie wydają świadectwa homologacji typu, dopóki nie mają:

— świadectwa bezpieczeństwa,

— świadectwa funkcjonalności,

— i świadectwa interoperacyjności

dla urządzenia rejestrującego lub kart do tachografów, dla których złożono wniosek o homologację typu.

428) O wszelkich modyfikacjach oprogramowania lub sprzętu urządzenia lub rodzaju materiałów użytych do wytworzenia urządzenia należy, przed zastosowaniem, zawiadomić organ, który wydał homologację typu dla urządzenia. Organ ten potwierdza producentowi rozszerzenie homologacji typu lub też może zażądać uaktualnienia lub potwierdzenia stosownych świadectw funkcjonalności, bezpieczeństwa lub interoperacyjności.

429) Procedury aktualizacji oprogramowania w prawidłowo funkcjonującym urządzeniu rejestrującym zatwierdza organ, który wydał homologację typu dla tego urządzenia rejestrującego. Aktualizacja oprogramowania nie może zmienić ani usunąć żadnych danych dotyczących czynności kierowcy przechowywanych w pamięci urządzenia rejestrującego. Oprogramowanie można aktualizować wyłącznie na odpowiedzialność producenta urządzenia.

430) Nie można odmówić homologacji typu zmian w oprogramowaniu, których celem jest aktualizacja wcześniej homologowanego typu urządzenia rejestrującego, jeżeli takie zmiany dotyczą wyłącznie funkcji nieokreślonych w niniejszym załączniku. Aktualizacja oprogramowania urządzenia rejestrującego może nie obejmować wprowadzania nowych zestawów znaków, jeśli nie jest to technicznie wykonalne.

8.2 Świadectwo bezpieczeństwa

431) Świadectwo bezpieczeństwa wydaje się zgodnie z przepisami dodatku 10 do niniejszego załącznika. Elementy składowe urządzenia rejestrującego objęte certyfikacją to przyrząd rejestrujący, czujnik ruchu, urządzenie zewnętrzne GNSS i karty do tachografów.

432) W wyjątkowej sytuacji, gdy organy certyfikacji bezpieczeństwa odmawiają certyfikowania nowego urządzenia z powodu przestarzałych mechanizmów bezpieczeństwa, homologację typu przyznaje się nadal tylko w tych konkretnych i wyjątkowych okolicznościach oraz jeżeli, zgodnie z rozporządzeniem, nie istnieje rozwiązanie alternatywne.

433) W takiej sytuacji dane państwo członkowskie bezzwłocznie informuje Komisję Europejską, która w ciągu dwunastu miesięcy kalendarzowych od przyznania homologacji typu wszczyna procedurę mającą na celu zapewnienie przywrócenia poziomu bezpieczeństwa do stanu początkowego.

8.3 Świadectwo funkcjonalności

434) Każdy ubiegający się o homologację typu dostarcza organowi państwa członkowskiego właściwemu dla homologacji typu wszelkie materiały i dokumentacje, jakie organ ten uzna za niezbędne.

435) W ciągu jednego miesiąca od złożenia wniosku producenci dostarczają odpowiednie próbki produktów posiadających homologację typu i związaną z nimi dokumentację wymaganą przez laboratoria wyznaczone do przeprowadzenia badań funkcjonalności. Wnioskodawca ponosi wszystkie koszty wynikające z przedmiotowego wniosku. Laboratoria zachowują poufność wszystkich informacji wrażliwych pod względem handlowym.

436) Świadectwo funkcjonalności wydaje się producentowi wyłącznie po pozytywnym przejściu przynajmniej przez wszystkie badania funkcjonalności wyszczególnione w dodatku 9.

437) Organ właściwy dla homologacji typu wydaje świadectwo funkcjonalności. W świadectwie tym podaje się, oprócz nazwy (nazwiska) otrzymującego świadectwo i identyfikacji modelu, szczegółowy wykaz wykonanych badań i uzyskanych wyników.

438) W świadectwie funkcjonalności każdego elementu składowego urządzenia rejestrującego wskazuje się także numery homologacji typu wszystkich innych homologowanych kompatybilnych elementów składowych urządzenia rejestrującego przebadanych do celów certyfikacji.

439) W świadectwie funkcjonalności każdego elementu składowego urządzenia rejestrującego wskazuje się także normę CEN lub ISO, na podstawie której certyfikowano interfejs funkcjonalny.

8.4 Świadectwo interoperacyjności

440) Badania interoperacyjności przeprowadza jedno laboratorium w imieniu i na odpowiedzialność Komisji Europejskiej.

441) Laboratorium rejestruje wnioski o badania interoperacyjności złożone przez producentów w kolejności chronologicznej napływu tych wniosków.

442) Wnioski rejestruje się oficjalnie tylko wtedy, gdy w posiadaniu laboratorium znajdują się:

— komplet materiałów i dokumentów niezbędnych do takich badań interoperacyjności,

— odpowiednie świadectwo bezpieczeństwa,

— odpowiednie świadectwo funkcjonalności.

Producenta zawiadamia się o dacie rejestracji wniosku.

443) Laboratorium nie przeprowadza żadnych badań interoperacyjności urządzeń rejestrujących ani kart do tachografów, którym nie przyznano świadectwa bezpieczeństwa i świadectwa funkcjonalności, poza wyjątkowymi sytuacjami opisanymi w wymaganiu 432.

444) Producent wnioskujący o przeprowadzenie badań interoperacyjności zobowiązuje się do pozostawienia w laboratorium, które ma przeprowadzić te badania, kompletu materiałów i dokumentów, które dostarczył do przeprowadzenia tych badań.

445) Badania interoperacyjności przeprowadza się, zgodnie z przepisami dodatku 9 do niniejszego załącznika, dla, odpowiednio, wszystkich typów urządzenia rejestrującego lub kart do tachografów:

— które mają jeszcze ważną homologację typu, lub

— których homologacja typu jest w toku i które mają ważne świadectwo interoperacyjności.

446) Badania interoperacyjności obejmują wszystkie generacje urządzeń rejestrujących lub kart do tachografów będące nadal w użyciu.

447) Laboratorium wydaje producentowi świadectwo interoperacyjności tylko wtedy, gdy objęte nim urządzenia pomyślnie przejdą wszystkie wymagane badania interoperacyjności.

448) Jeżeli co najmniej jedno urządzenie rejestrujące lub karta do tachografów nie przejdą pomyślnie badań interoperacyjności, świadectwa interoperacyjności nie wydaje się, dopóki wnioskujący producent nie wprowadzi niezbędnych poprawek i dopóki nie przejdą one pomyślnie przez badania interoperacyjności. Laboratorium, przy pomocy zainteresowanych producentów, rozpoznaje przyczynę usterki interoperacyjności i dokłada starań, by pomóc wnioskującemu producentowi w znalezieniu rozwiązania technicznego. W przypadku gdy producent modyfikuje swój produkt, odpowiada on za uzyskanie potwierdzenia właściwych organów, że świadectwo bezpieczeństwa i świadectwo funkcjonalności nadal zachowują ważność.

449) Świadectwo interoperacyjności ważne jest przez sześć miesięcy. Zostaje ono odwołane na koniec tego okresu, jeżeli producent nie uzyska odpowiadającego mu świadectwa homologacji typu. Producent przekazuje to świadectwo organowi homologacji typu w państwie członkowskim, który wydał świadectwo funkcjonalności.

450) Żaden element, który może być źródłem usterki interoperacyjności, nie może być użyty do osiągania korzyści z pozycji dominującej ani prowadzić do uzyskania takiej pozycji.

8.5 **Świadectwo homologacji typu**

451) Organ homologacji typu w państwie członkowskim może wydać świadectwo homologacji typu, jeżeli posiada trzy wymagane świadectwa.

452) W świadectwie homologacji typu każdego elementu składowego urządzenia rejestrującego wskazuje się także numery homologacji typu innych homologowanych interoperacyjnych urządzeń rejestrujących.

453) Organ homologacji typu przekazuje kopię świadectwa homologacji typu do laboratorium właściwego do przeprowadzenia badań interoperacyjności równocześnie z dostarczeniem świadectwa producentowi.

454) Laboratorium właściwe do przeprowadzenia badań interoperacyjności prowadzi publiczną stronę internetową, na której znajduje się uaktualniony wykaz modeli urządzeń rejestrujących lub kart do tachografów:

— dla których zarejestrowano wniosek o badania interoperacyjności,

— które uzyskały świadectwo interoperacyjności (nawet czasowe),

— które uzyskały świadectwo homologacji typu.

8.6 **Procedura szczególna: pierwsze świadectwa interoperacyjności dla urządzeń rejestrujących i kart do tachografów 2. generacji**

455) Przez cztery miesiące od czasu, gdy pierwsza para urządzeń rejestrujących 2. generacji i kart do tachografów 2. generacji (karty kierowcy, warsztatowe, kontrolne i firmowe) uzyska świadectwa interoperacyjności, wszelkie wydane świadectwa interoperacyjności (łącznie z pierwszymi), w odniesieniu do wniosków zarejestrowanymi w tym okresie, uważa się za czasowe.

456) Jeżeli na koniec tego okresu wszystkie produkty, których to dotyczy, współdziałają, wszystkie odpowiednie świadectwa interoperacyjności zastępuje się świadectwem ostatecznym.

457) Jeżeli w tym okresie wykryje się usterki interoperacyjności, laboratorium właściwe do przeprowadzenia badań interoperacyjności rozpoznaje przyczyny problemów z pomocą wszystkich zainteresowanych producentów i zachęca ich do wprowadzenia niezbędnych poprawek.

458) Jeżeli na koniec tego okresu nadal występują problemy interoperacyjności, laboratorium właściwe do przeprowadzenia badań interoperacyjności, we współpracy z zainteresowanymi producentami i organami homologacji typu, które wydały odpowiednie świadectwa funkcjonalności, szuka przyczyn usterek interoperacyjności i ustala, jakie poprawki powinien wprowadzić każdy z zainteresowanych producentów. Poszukiwanie rozwiązań technicznych trwa maksymalnie dwa miesiące, po czym, jeśli nie zostanie znalezione wspólne rozwiązanie, Komisja, po konsultacji z laboratorium właściwym do przeprowadzenia badań interoperacyjności, decyduje, które urządzenie(-a) i karty otrzymują ostateczne świadectwa interoperacyjności wraz z uzasadnieniem swojej decyzji.

459) Wszelkie wnioski o przeprowadzenie badań interoperacyjności, zarejestrowane przez laboratorium w okresie między końcem czteromiesięcznego okresu po dostarczeniu pierwszego czasowego świadectwa interoperacyjności a datą decyzji Komisji, o której mowa w wymaganiu 455, są odraczane aż do rozwiązania początkowych problemów interoperacyjności. Następnie wnioski te rozpatruje się w kolejności chronologicznej ich rejestracji.

Dodatek 1

SPIS DANYCH:

SPIS TREŚCI

1. WPROWADZENIE

Niniejszy dodatek określa formaty danych, elementy danych i struktury danych przeznaczone do wykorzystania w urządzeniach rejestrujących i kartach do tachografów.

1.1. **Podejście do definicji typów danych**

W niniejszym dodatku do definiowania typów danych użyto zapisu składni abstrakcyjnej 1 (ASN.1). Pozwala to na definiowanie prostych i strukturalnych danych bez narzucania żadnej swoistej składni przesyłania danych (reguł kodowania), która zależy od aplikacji i środowiska.

Konwencje nazewnictwa typu ASN.1 opracowano zgodnie z normą ISO/IEC 8824-1. Powyższe oznacza, że:

— tam gdzie możliwe wybrane nazwy opisują znaczenie typu,

— tam gdzie typ danych zbudowany jest z innych typów danych nazwa typu danych ma postać pojedynczego ciągu znaków alfanumerycznych zaczynającego się od dużej litery, natomiast duże litery wewnątrz nazwy opisują odpowiednie znaczenia,

— ogólnie nazwy typów danych powiązane są z nazwami typów danych, z których są zbudowane, urządzeniem, w którym są zgromadzone i funkcją z nimi związaną.

Jeżeli typ ASN.1 jest już zdefiniowany jako część innej normy i jeżeli jest to właściwe w celu wykorzystania w urządzeniu rejestrującym, to ten typ ASN.1 jest zdefiniowany w niniejszym dodatku.

Aby umożliwić stosowanie kilku reguł kodowania, niektóre typy ASN.1 w niniejszym dodatku są ograniczone identyfikatorami zakresu wartości. Identyfikatory zakresu wartości zostały zdefiniowane w pkt. 3 i dodatku 2.

1.2. **Odniesienia**

W niniejszym dodatku stosuje się następujące odniesienia:

ISO 639	Kod reprezentacji nazw języków. Wydanie pierwsze: 1988.
ISO 3166	Kody nazw krajów i ich jednostek administracyjnych – Część 1: Kody krajów, 2013.
ISO 3779	Pojazdy drogowe – Numer identyfikacyjny pojazdu (VIN) – zawartość i struktura. 2009
ISO/IEC 7816-5	Karty identyfikacyjne — Elektroniczne karty stykowe — część 5: Rejestracja identyfikatorów aplikacji Wydanie drugie: 2004.
ISO/IEC 7816-6	Karty identyfikacyjne — Elektroniczne karty stykowe — część 6: Elementy danych wymieniane z otoczeniem niezależnie od dziedziny zastosowań, 2004 + Poprawka techniczna 1: 2006
ISO/IEC 8824-1	Informatyka – Zapis składni abstrakcyjnej 1 (ASN.1): Specyfikacja notacji podstawowej. 2008 + sprostowanie techniczne 1: 2012 i sprostowanie techniczne 2: 2014.
ISO/IEC 8825-2	Informatyka – Reguły kodowania ASN.1: Specyfikacja reguł upakowanego kodowania (PER). 2008.
ISO/IEC 8859-1	Informatyka – 8-bitowe jednobajtowe zestawy znaków graficznych – część 1: Zestaw łaciński 1. Wydanie pierwsze: 1998.
ISO/IEC 8859-7	Informatyka – 8-bitowe jednobajtowe zestawy znaków graficznych – część 7: Alfabet łaciński/grecki. 2003.

ISO 16844-3	Pojazdy drogowe – Systemy tachograficzne – interfejs czujnika ruchu. 2004 + Poprawka techniczna 1: 2006.
TR-03110-3	Wytyczne techniczne BSI/ANSSI TR-03110-3, Zaawansowane mechanizmy zabezpieczeń dokumentów podróży odczytywanych maszynowo i token eIDAS – część 3 Wspólne specyfikacje, wersja 2.20, 3. Luty 2015 r.

2. DEFINICJE TYPÓW DANYCH

Dla każdego z następujących typów danych wartość domyślna „nieznane" lub zawartość „nie dotyczy" polega na wypełnieniu elementu danych bajtami „FF".

Wszystkie typy danych są wykorzystywane w aplikacjach generacji 1 i generacji 2, chyba że określono inaczej.

2.1. **ActivityChangeInfo**

Ten typ danych umożliwia kodowanie, w dwubajtowym słowie, stanu szczeliny czytnika o godzinie 00:00 lub statusu kierowcy o godzinie 00:00 lub zmiany czynności, lub zmiany stanu prowadzenia pojazdu, lub zmiany stanu karty dla kierowcy lub współkierowcy. Ten typ danych związany jest z wymaganiami 105, 266, 291, 320, 321, 343 i 344 określonymi w załączniku 1C.

```
ActivityChangeInfo ::= OCTET STRING (SIZE(2))
```

Przypisanie wartości – zapisane oktetami: 'scpaatttttttttt'B (16 bitów)

Zapisy w pamięci danych (lub stan szczeliny czytnika karty):

's'B	Szczelina czytnika karty:
	'0'B: KIEROWCA,
	'1'B: WSPÓŁKIEROWCA,
'c'B	Stan prowadzenia pojazdu:
	'0'B: JEDEN KIEROWCA,
	'1'B: ZAŁOGA,
'p'B	Stan karty kierowcy (lub warsztatowej) w odpowiedniej szczelinie czytnika:
	'0'B: WŁOŻONA, karta jest włożona,
	'1'B: NIEWŁOŻONA, brak karty (lub karta jest wyjęta),
'aa'B	Czynność:
	'00'B: PRZERWA/ODPOCZYNEK,
	'01'B: GOTOWOŚĆ,
	'10'B: PRACA,
	'11'B: PROWADZENIE,
'ttttttttttt'B	Godzina zmiany: liczba minut od godziny 00:00 w danym dniu.

Dla zapisów na kartach kierowcy (lub warsztatowej) (i statusu kierowcy):

's'B	Szczelina czytnika karty (nieistotne, gdy „p" = 1 z wyjątkiem jak w uwadze poniżej):
	'0'B: KIEROWCA,
	'1'B: WSPÓŁKIEROWCA,
'c'B	Stan prowadzenia pojazdu (przypadek „p" = 0); lub
	Następny stan czynności (przypadek „p" = 1):
	'0'B: JEDEN KIEROWCA,
	'0'B: NIEZNANY
	'1'B: ZAŁOGA,
	'1'B: ZNANY (=wprowadzony ręcznie)
'p'B	Stan karty:
	'0'B: WŁOŻONA, karta jest włożona do urządzenia rejestrującego,
	'1'B: NIEWŁOŻONA, brak karty (lub karta jest wyjęta)
'aa'B	Czynność (nieistotne, gdy „p" = 1 i „c" = 0 z wyjątkiem jak w uwadze poniżej):
	'00'B: PRZERWA/ODPOCZYNEK,
	'01'B: GOTOWOŚĆ,
	'10'B: PRACA,
	'11'B: PROWADZENIE,
'ttttttttttt'B	Godzina zmiany: liczba minut od godziny 00:00 w danym dniu.

Uwaga dla przypadku „wyjęcie karty":

Gdy karta jest wyjęta:

— „s" odnosi się do szczeliny czytnika i wskazuje szczelinę czytnika, z której wyjęta jest karta,

— „c" musi być ustawiony na 0,

— „p" musi być ustawiony na 1,

— „aa" musi kodować bieżącą czynność wybraną w tym czasie.

W wyniku ręcznego wprowadzenia danych bity „c" i „aa" słowa (zapisanego na karcie) mogą być nadpisane później w celu odzwierciedlania zapisu.

2.2. Address

Adres.

```
Address ::= SEQUENCE {
   codePage                              INTEGER (0..255),
   address                               OCTET STRING (SIZE(35))
}
```

codePage określa zestaw znaków zdefiniowany w rozdziale 4,

address jest adresem zakodowanym przy użyciu wyszczególnionego zestawu znaków.

2.3. **AESKey**

Generacja 2:

Klucz AES o długości 128, 192 lub 256 bitów.

```
AESKey ::= CHOICE {
   aes128Key                          AES128Key,
   aes192Key                          AES192Key,
   aes256Key                          AES256Key
}
```

Przypisanie wartości: nie określa się.

2.4. **AES128Key**

Generacja 2:

Klucz AES 128.

```
AES128Key ::= SEQUENCE {
   length                             INTEGER(0..255),
   aes128Key                          OCTET STRING (SIZE(16))
}
```

length oznacza długość klucza AES 128 w oktetach.

aes128Key oznacza klucz AES o długości 128 bitów.

Przypisanie wartości:

długość ma wartość 16.

2.5. **AES192Key**

Generacja 2:

Klucz AES 192.

```
AES192Key ::= SEQUENCE {
   length                             INTEGER(0..255),
   aes192Key                          OCTET STRING (SIZE(24))
}
```

length oznacza długość klucza AES 192 w oktetach.

aes192Key oznacza klucz AES o długości 192 bitów.

Przypisanie wartości:

długość ma wartość 24.

2.6. **AES256Key**

Generacja 2:

Klucz AES 256.

```
AES256Key ::= SEQUENCE {
   length                                  INTEGER(0..255),
   aes256Key                               OCTET STRING (SIZE(32))
}
```

długość oznacza długość klucza AES 256 w oktetach.

aes256Key oznacza klucz AES o długości 256 bitów.

Przypisanie wartości:

długość ma wartość 32.

2.7. **BCDString**

BCDString jest stosowany do reprezentacji liczb w zapisie dziesiętnym kodowanym dwójkowo (BCD). Tego typu danych używa się do przedstawiania jednej cyfry dziesiętnej w półoktecie (4 bity). BCDString oparty jest na definicji z normy ISO/IEC 8824-1 „CharacterStringType".

```
BCDString ::= CHARACTER STRING (WITH COMPONENTS {
   identification ( WITH COMPONENTS {
   fixed PRESENT }) })
```

BCDString używa notacji „hstring". Skrajna lewa cyfra heksadecymalna jest najbardziej znaczącym półoktetem pierwszego oktetu. Aby utworzyć wielokrotne oktety, wstawia się, gdy trzeba, zerowe półoktety o lewej skrajnej pozycji półoktetu w pierwszym oktecie.

Dozwolonymi cyframi są: 0, 1, .. 9.

2.8. **CalibrationPurpose**

Kod wyjaśniający, dlaczego zarejestrowano zbiór parametrów kalibracyjnych. Ten typ danych związany jest z wymaganiami 097 i 098 określonymi w załączniku 1B i wymaganiem 119 określonym w załączniku 1C.

```
CalibrationPurpose ::= OCTET STRING (SIZE(1))
```

Przypisanie wartości:

Generacja 1:

'00'H	wartość zastrzeżona,
'01'H	aktywacja: zapis parametrów kalibracyjnych znanych w momencie aktywacji VU,
'02'H	pierwsza instalacja: pierwsza kalibracja VU po aktywacji,
'03'H	instalacja: pierwsza kalibracja VU w bieżącym pojeździe,
'04'H	przegląd okresowy.

Generacja 2:

Oprócz generacji 1 używane są następujące wartości:

'05'H wprowadzenie VRN przez firmę,

'06'H korekta czasu bez kalibracji,

'07'H to '7F'H RFU,

'80'H – 'FF'H swoisty dla producenta.

2.9. **CardActivityDailyRecord**

Informacje, zapisane na karcie, dotyczące czynności kierowcy w danym dniu kalendarzowym. Ten typ danych związany jest z wymaganiami 266, 291, 320 i 343 określonymi w załączniku 1C.

```
CardActivityDailyRecord ::= SEQUENCE {
   activityPreviousRecordLength         INTEGER(0..CardActivityLengthRange),
   activityRecordLength                 INTEGER(0..CardActivityLengthRange),
   activityRecordDate                   TimeReal,
   activityDailyPresenceCounter         DailyPresenceCounter,
   activityDayDistance                  Distance,
   activityChangeInfo                   SET SIZE(1..1440) OF ActivityChangeInfo
}
```

activityPreviousRecordLength jest całkowitą długością w bajtach poprzedniego rekordu dziennego. Maksymalną wartość określa długość OCTET STRING zawierającego te rekordy (zob. pkt 4 CardActivityLengthRange w dodatku 2). Gdy rekord ten jest najstarszym rekordem dziennym, wartość activityPreviousRecordLength musi być ustawiona na 0.

activityRecordLength jest całkowitą długością tego rekordu w bajtach. Maksymalną wartość określa długość OCTET STRING zawierającego te rekordy.

activityRecordDate jest datą rekordu.

activityDailyPresenceCounter jest licznikiem obecności dla karty w tym dniu.

activityDayDistance jest całkowitą drogą przebytą w tym dniu.

activityChangeInfo jest zbiorem danych ActivityChangeInfo dla kierowcy w tym dniu. Może zawierać maksymalnie 1440 wartości (jedna zmiana czynności na minutę). W tym zbiorze danych zawsze znajduje się activityChangeInfo określający status kierowcy o godzinie 00:00.

2.10. **CardActivityLengthRange**

Liczba bajtów na karcie kierowcy lub na karcie warsztatowej, dostępnych do przechowywania rekordów z czynnościami kierowcy.

```
CardActivityLengthRange ::= INTEGER(0..2^16-1)
```

Przypisanie wartości: zob. dodatek 2.

2.11. **CardApprovalNumber**

Numer homologacji typu karty.

```
CardApprovalNumber ::= IA5String(SIZE(8))
```

Przypisanie wartości:

Należy podawać numer homologacji, który został opublikowany na odpowiedniej stronie internetowej Komisji Europejskiej, tj. na przykład z uwzględnieniem myślników, jeżeli występują. Numer homologacji musi być wyrównany do lewej strony.

2.12. **CardCertificate**

Generacja 1:

Certyfikat klucza publicznego karty.

```
CardCertificate ::= Certificate
```

2.13. **CardChipIdentification**

Informacje, zapisane na karcie, dotyczące identyfikacji układu scalonego karty (IC) (wymaganie 249 określone w załączniku 1C). IcSerialNumber wraz z icManufacturingReferences identyfikują w sposób niepowtarzalny chip karty. Sam IcSerialNumber nie identyfikuje chipu karty w sposób niepowtarzalny.

```
CardChipIdentification ::= SEQUENCE {
   icSerialNumber                    OCTET STRING (SIZE(4)),
   icManufacturingReferences         OCTET STRING (SIZE(4))
}
```

icSerialNumber jest numerem seryjnym IC.

icManufacturingReferences jest identyfikatorem swoistym producenta IC.

2.14. **CardConsecutiveIndex**

Numer kolejny karty (definicja h)).

```
CardConsecutiveIndex ::= IA5String(SIZE(1))
```

Przypisanie wartości: (zob. rozdział 7 załącznika 1C)

Kolejność zwiększania: '0, …, 9, A, …, Z, a, …, z'

2.15. **CardControlActivityDataRecord**

Informacje przechowywane na karcie kierowcy lub warsztatowej dotyczące ostatniej kontroli, której poddany był kierowca (wymagania 274, 299, 327 i 350 określone w załączniku 1C).

```
CardControlActivityDataRecord ::= SEQUENCE {
   controlType                       ControlType,
   controlTime                       TimeReal,
   controlCardNumber                 FullCardNumber,
   controlVehicleRegistration        VehicleRegistrationIdentification,
   controlDownloadPeriodBegin        TimeReal,
   controlDownloadPeriodEnd          TimeReal
}
```

controlType jest typem kontroli.

controlTime jest datą i godziną kontroli.

controlCardNumber jest numerem karty FullCardNumber funkcjonariusza służb kontrolnych przeprowadzającego kontrolę.

controlVehicleRegistration jest numerem VRN i państwa członkowskiego rejestracji pojazdu, w którym miała miejsce kontrola.

controlDownloadPeriodBegin i **controlDownloadPeriodEnd** jest okresem, dla którego pobrano dane, w przypadku pobierania danych.

2.16. CardCurrentUse

Informacje o rzeczywistym użyciu karty (wymagania 273, 298, 326 i 349 określone w załączniku 1C).

```
CardCurrentUse ::= SEQUENCE {
   sessionOpenTime                    TimeReal,
   sessionOpenVehicle                 VehicleRegistrationIdentification
}
```

sessionOpenTime jest godziną, o której kartę włożono dla bieżącego użycia. Przy wyjęciu karty element ten jest zerowany.

sessionOpenVehicle jest identyfikacją aktualnie używanego pojazdu ustawianą przy wkładaniu karty. Przy wyjęciu karty element ten jest zerowany.

2.17. CardDriverActivity

Informacje przechowywane na karcie kierowcy lub na karcie warsztatowej dotyczące czynności kierowcy (wymagania 267, 268, 292, 293, 321 i 344 określone w załączniku 1C).

```
CardDriverActivity ::= SEQUENCE {
   activityPointerOldestDayRecord     INTEGER(0.. CardActivityLengthRange-1),
   activityPointerNewestRecord        INTEGER(0.. CardActivityLengthRange-1),
   activityDailyRecords               OCTET STRING
                                      (SIZE(CardActivityLengthRange))
}
```

activityPointerOldestDayRecord jest wskaźnikiem początku miejsca gromadzenia danych (liczba bajtów od początku łańcucha znaków) najstarszego, pełnego rekordu dziennego w łańcuchu activityDailyRecords. Maksymalna wartość jest określona długością łańcucha.

activityPointerNewestRecord jest wskaźnikiem początku miejsca gromadzenia danych (liczba bajtów od początku łańcucha znaków) najświeższego rekordu dziennego w łańcuchu activityDailyRecords. Maksymalna wartość jest określona długością łańcucha.

activityDailyRecords jest przestrzenią dostępną do przechowywania danych dotyczących czynności kierowcy (struktura danych: CardActivityDailyRecord) dla każdego dnia kalendarzowego, w którym karta jest użyta.

Przypisanie wartości: ten OCTET STRING jest cyklicznie wypełniany rekordami CardActivityDailyRecord. Przy pierwszym użyciu gromadzenie rozpoczyna się od pierwszego bajtu łańcucha. Wszystkie nowe rekordy dołącza się do końca poprzedniego rekordu. Gdy łańcuch zostaje zapełniony wypełnianie rozpoczyna się od pierwszego bajtu łańcucha niezależnie od przerwy w elemencie danych. Przed wstawieniem do łańcucha danych o nowej czynności (zwiększenie bieżącego rekordu activityDailyRecord lub wstawienie nowego rekordu activityDailyRecord), który zamienia stare dane o starej czynności, wskaźnik activityPointerOldestDayRecord musi być uaktualniony w celu odzwierciedlenia nowego położenia najstarszego, pełnego rekordu dziennego a długość activityPreviousRecordLength tego (nowego) najstarszego, pełnego rekordu dziennego musi być wyzerowana.

2.18. CardDrivingLicenceInformation

Informacje przechowywane na karcie kierowcy dotyczące prawa jazdy posiadacza karty (wymagania 259 i 284 określone w załączniku 1C).

```
CardDrivingLicenceInformation ::= SEQUENCE {
   drivingLicenceIssuingAuthority       Name,
   drivingLicenceIssuingNation          NationNumeric,
   drivingLicenceNumber                 IA5String(SIZE(16))
}
```

drivingLicenceIssuingAuthority jest organem, który wydał prawo jazdy.

drivingLicenceIssuingNation jest przynależnością państwową organu, który wydał prawo jazdy.

drivingLicenceNumber jest numerem prawa jazdy.

2.19. **CardEventData**

Informacje przechowywane na karcie kierowcy lub na karcie warsztatowej dotyczące zdarzeń związanych z posiadaczem karty (wymagania 260, 285, 318 i 341 określone w załączniku 1C).

```
CardEventData ::= SEQUENCE SIZE(6) OF {
   cardEventRecords                     SET SIZE(NoOfEventsPerType) OF
                                        CardEventRecord
}
```

CardEventData jest sekwencją uporządkowaną w kolejności rosnącej typu EventFaultType, w zapisach cardEventRecords (z wyjątkiem rekordów związanych z próbami naruszenia zabezpieczeń, które gromadzone są w ostatnim zbiorze sekwencji).

cardEventRecords jest zbiorem rekordów ze zdarzeniami dla danego typu zdarzenia (lub kategorii prób naruszeń zabezpieczenia).

2.20. **CardEventRecord**

Informacje przechowywane na karcie kierowcy lub na karcie warsztatowej dotyczące zdarzenia związanego z posiadaczem karty (wymagania 261, 286, 318 i 341 określone w załączniku 1C).

```
CardEventRecord ::= SEQUENCE {
   eventType                            EventFaultType,
   eventBeginTime                       TimeReal,
   eventEndTime                         TimeReal,
   eventVehicleRegistration             VehicleRegistrationIdentification
}
```

eventType jest typem zdarzenia.

eventBeginTime jest datą i godziną rozpoczęcia zdarzenia.

eventEndTime jest datą i godziną zakończenia zdarzenia.

eventVehicleRegistration jest numerem VRN i państwa członkowskiego rejestracji pojazdu, w którym zdarzenie miało miejsce.

2.21. **CardFaultData**

Informacje przechowywane na karcie kierowcy lub na karcie warsztatowej dotyczące usterek związanych z posiadaczem karty (wymagania 263, 288, 318 i 341 określone w załączniku 1C).

```
CardFaultData ::= SEQUENCE SIZE(2) OF {
   cardFaultRecords                     SET SIZE(NoOfFaultsPerType) OF
                                        CardFaultRecord
}
```

CardFaultData jest sekwencją zbioru rekordów dotyczących usterek urządzenia rejestrującego poprzedzającego zbiór rekordów dotyczących usterek kart.

cardFaultRecords jest zbiorem rekordów dotyczących usterek danej kategorii (urządzenia rejestrującego lub karty).

2.22. **CardFaultRecord**

Informacje przechowywane na karcie kierowcy lub na karcie warsztatowej dotyczące usterki związanej z posiadaczem karty (wymagania 264, 289, 318 i 341 określone w załączniku 1C).

```
CardFaultRecord ::= SEQUENCE {
   faultType                        EventFaultType,
   faultBeginTime                   TimeReal,
   faultEndTime                     TimeReal,
   faultVehicleRegistration         VehicleRegistrationIdentification
}
```

faultType jest typem usterki.

faultBeginTime jest datą i godziną początku usterki.

faultEndTime jest datą i godziną zakończenia usterki.

faultVehicleRegistration jest numerem VRN i państwa członkowskiego rejestracji pojazdu, w którym usterka się zdarzyła.

2.23. **CardIccIdentification**

Informacje zapisane na karcie dotyczące identyfikacji karty z układem scalonym (IC) (wymaganie 248 określone w załączniku 1C).

```
CardIccIdentification ::= SEQUENCE {
   clockStop                        OCTET STRING (SIZE(1)),
   cardExtendedSerialNumber         ExtendedSerialNumber,
   cardApprovalNumber               CardApprovalNumber,
   cardPersonaliserID               ManufacturerCode,
   embedderIcAssemblerId            EmbedderIcAssemblerId,
   icIdentifier                     OCTET STRING (SIZE(2))
}
```

clockStop jest trybem Clockstop zdefiniowanym w dodatku 2.

cardExtendedSerialNumber jest niepowtarzalnym numerem seryjnym karty IC, dodatkowo określonym za pomocą typu danych ExtendedSerialNumber.

cardApprovalNumber jest numerem homologacji typu karty.

cardPersonaliserID jest identyfikatorem jednostki personalizującej kartę zakodowanym jako ManufacturerCode.

embedderIcAssemblerId zapewnia informacje o wbudowującym/montującym układ scalony.

icIdentifier jest identyfikatorem układu scalonego na karcie i producenta układu scalonego zdefiniowanym w normie ISO/IEC 7816-6.

2.24. **CardIdentification**

Informacje zapisane na karcie dotyczące identyfikacji karty (wymagania 255, 280, 310, 333, 359, 365, 371 i 377 określone w załączniku 1C).

```
CardIdentification ::= SEQUENCE {
   cardIssuingMemberState              NationNumeric,
   cardNumber                          CardNumber,
   cardIssuingAuthorityName            Name,
   cardIssueDate                       TimeReal,
   cardValidityBegin                   TimeReal,
   cardExpiryDate                      TimeReal
}
```

cardIssuingMemberState jest kodem państwa członkowskiego wydającego kartę.

cardNumber jest numerem karty.

cardIssuingAuthorityName jest nazwą organu wydającego kartę.

cardIssueDate jest datą wydania karty aktualnemu posiadaczowi.

cardValidityBegin jest pierwszą datą ważności karty.

cardExpiryDate jest terminem ważności karty.

2.25. **CardMACertificate**

Generacja 2:

Certyfikat klucza publicznego karty na potrzeby wzajemnego uwierzytelniania z VU. Strukturę tego certyfikatu określono w dodatku 11.

```
CardMACertificate ::= Certificate
```

2.26. **CardNumber**

Numer karty zgodny z definicją g).

```
CardNumber ::= CHOICE {
   SEQUENCE {
      driverIdentification             IA5String(SIZE(14)),
      cardReplacementIndex             CardReplacementIndex,
      cardRenewalIndex                 CardRenewalIndex
   },
   SEQUENCE {
      ownerIdentification              IA5String(SIZE(13)),
      cardConsecutiveIndex             CardConsecutiveIndex,
      cardReplacementIndex             CardReplacementIndex,
      cardRenewalIndex                 CardRenewalIndex
   }
}
```

driverIdentification jest jednoznaczną identyfikacją kierowcy w państwie członkowskim.

ownerIdentification jest jednoznaczną identyfikacją firmy lub warsztatu lub organu kontrolnego w państwie członkowskim.

cardConsecutiveIndex jest numerem kolejnym karty.

cardReplacementIndex jest numerem wymiany karty.

cardRenewalIndex jest numerem odnowienia karty.

Pierwsza wybierana sekwencja umożliwia kodowanie karty kierowcy, a druga wybierana sekwencja umożliwia kodowanie numeru karty warsztatowej, karty kontrolnej i karty firmowej.

2.27. **CardPlaceDailyWorkPeriod**

Informacje przechowywane na karcie kierowcy lub na karcie warsztatowej dotyczące miejsc rozpoczęcia lub zakończenia dziennych okresów pracy (wymagania 272, 297, 325 i 348 określone w załączniku 1C).

```
CardPlaceDailyWorkPeriod ::= SEQUENCE {
   placePointerNewestRecord    INTEGER(0 .. NoOfCardPlaceRecords-1),
   placeRecords                SET SIZE(NoOfCardPlaceRecords) OF PlaceRecord
}
```

placePointerNewestRecord jest indeksem ostatniego, uaktualnionego rekordu miejsca.

Przypisanie wartości: liczba odpowiadająca stanowi licznika rekordów miejsca, zaczynająca się od „0” dla pierwszego wystąpienia rekordów miejsca w strukturze.

placeRecords jest zbiorem rekordów dotyczących wprowadzonych miejsc.

2.28. **CardPrivateKey**

Generacja 1:

Klucz prywatny karty.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.29. **CardPublicKey**

Klucz publiczny karty.

```
CardPublicKey ::= PublicKey
```

2.30. **CardRenewalIndex**

Numer odnowienia karty (definicja i)).

```
CardRenewalIndex ::= IA5String(SIZE(1))
```

Przypisanie wartości: (zob. rozdział VII niniejszego załącznika).

‘0’ Wydanie pierwsze.

Kolejność zwiększania: ‘0, …, 9, A, …, Z’

2.31. **CardReplacementIndex**

Numer wymiany karty (definicja j)).

```
CardReplacementIndex ::= IA5String(SIZE(1))
```

Przypisanie wartości: (zob. rozdział VII niniejszego załącznika).

‘0’ Oryginał karty.

Kolejność zwiększania: ‘0, …, 9, A, …, Z’

2.32. **CardSignCertificate**

Generacja 2:

Certyfikat klucza publicznego karty do podpisu. Strukturę tego certyfikatu określono w dodatku 11.

```
CardSignCertificate ::= Certificate
```

2.33. **CardSlotNumber**

Kod rozróżnienia między dwiema szczelinami kart w przyrządzie rejestrującym.

```
CardSlotNumber ::= INTEGER {
   driverSlot                          (0),
   co-driverSlot                       (1)
}
```

Przypisanie wartości: nie określa się.

2.34. **CardSlotsStatus**

Kod wskazujący typ kart włożonych do dwóch szczelin czytników karty przyrządu rejestrującego.

```
CardSlotsStatus ::= OCTET STRING (SIZE(1))
```

Przypisanie wartości – zapisane oktetami: 'ccccdddd'B

'cccc'B identyfikacja typu karty włożonej do szczeliny karty współkierowcy,

'dddd'B identyfikacja typu karty włożonej do szczeliny karty kierowcy,

z następującymi kodami identyfikującymi:

'0000'B brak karty,

'0001'B karta kierowcy jest włożona,

'0010'B karta warsztatowa jest włożona,

'0011'B karta kontrolna jest włożona,

'0100'B karta firmowa jest włożona.

2.35. **CardSlotsStatusRecordArray**

Generacja 2:

CardSlotsStatus wraz z metadanymi stosowany w protokole pobierania danych.

```
CardSlotsStatusRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CardSlotsStatus
}
```

recordType oznacza typ rekordu (CardSlotsStatus). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość CardSlotsStatus w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem rekordów CardSlotsStatus.

2.36. **CardStructureVersion**

Kod wskazujący wersję struktury na karcie do tachografu.

```
CardStructureVersion ::= OCTET STRING (SIZE(2))
```

Przypsianie wartości: 'aabb'H:

'aa'H indeks zmian struktury,

'00'H dla aplikacji generacji 1

'01'H dla aplikacji generacji 2

'bb'H indeks zmian dotyczących użycia elementów danych zdefiniowanych dla struktury określony wyższym bajtem.

'00'H dla tej wersji aplikacji generacji 1

'00'H la tej wersji aplikacji generacji 2

2.37. **CardVehicleRecord**

Informacje przechowywane na karcie kierowcy lub na karcie warsztatowej dotyczące okresu używania pojazdu w czasie dnia kalendarzowego (wymagania 269, 294, 322 i 345 określone w załączniku 1C).

Generacja 1:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter
}
```

vehicleOdometerBegin jest stanem licznika kilometrów na początku okresu używania pojazdu.

vehicleOdometerEnd jest stanem licznika kilometrów na końcu okresu używania pojazdu.

vehicleFirstUse jest datą i godziną rozpoczęcia okresu używania pojazdu.

vehicleLastUse jest datą i godziną zakończenia okresu używania pojazdu.

vehicleRegistration wskazuje numer VRN i państwo członkowskie rejestracji pojazdu.

vuDataBlockCounter jest wartością licznika VuDataBlockCounter ostatniego wyciągu okresu użycia pojazdu.

Generacja 2:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter,
   vehicleIdentificationNumber             VehicleIdentificationNumber
}
```

Oprócz generacji 1 używany jest następujący element danych:

VehicleIdentificationNumber jest numerem identyfikacyjnym pojazdu odnoszącym się do pojazdu jako całości.

2.38. **CardVehiclesUsed**

Informacje przechowywane na karcie kierowcy lub na karcie warsztatowej dotyczące używanych pojazdów (wymagania 270, 295, 323 i 346 określone w załączniku 1C).

```
CardVehiclesUsed := SEQUENCE {
   vehiclePointerNewestRecord          INTEGER(0..NoOfCardVehicleRecords-1),
   cardVehicleRecords                  SET SIZE(NoOfCardVehicleRecords) OF
                                       CardVehicleRecord
}
```

vehiclePointerNewestRecord jest indeksem ostatniego, uaktualnionego rekordu dotyczącego pojazdu.

Przypisanie wartości: liczba odpowiadająca stanowi licznika rekordów dotyczących pojazdu, rozpoczynając od „0” dla pierwszego wystąpienia w strukturze rekordów dotyczących pojazdu.

cardVehicleRecords jest zbiorem rekordów zawierających informacje o używanych pojazdach.

2.39. **CardVehicleUnitRecord**

Generacja 2:

informacje przechowywane na karcie kierowcy lub na karcie warsztatowej dotyczące używanego przyrządu rejestrującego (wymagania 303 i 351 określone w załączniku 1C).

```
CardVehicleUnitRecord ::= SEQUENCE {
   timeStamp                           TimeReal,
   manufacturerCode                    ManufacturerCode,
   deviceID                            INTEGER(0..255),
   vuSoftwareVersion                   VuSoftwareVersion
}
```

timeStamp jest początkiem okresu używania przyrządu rejestrującego (tj. pierwszym włożeniem karty do przyrządu rejestrującego dla tego okresu).

manufacturerCode identyfikuje producenta przyrządu rejestrującego.

deviceID identyfikuje typ przyrządu rejestrującego producenta. Wartość jest swoista dla producenta.

vuSoftwareVersion jest numerem wersji oprogramowania przyrządu rejestrującego.

2.40. **CardVehicleUnitsUsed**

Generacja 2:

Informacje przechowywane na karcie kierowcy lub na karcie warsztatowej dotyczące przyrządów rejestrujących używanych przez posiadacza karty (wymagania 306 i 352 określone w załączniku 1C).

```
CardVehicleUnitsUsed := SEQUENCE {
   vehicleUnitPointerNewestRecord       INTEGER(0..NoOfCardVehicleUnitRecords-1),
   cardVehicleUnitRecords               SET SIZE(NoOfCardVehicleUnitRecords) OF
                                        CardVehicleUnitRecord
}
```

vehiclePointerNewestRecord jest indeksem ostatniego, uaktualnionego rekordu dotyczącego przyrządu rejestrującego.

Przypisanie wartości: liczba odpowiadająca stanowi licznika rekordów przyrządu rejestrującego, rozpoczynając od „0" dla pierwszego wystąpienia w strukturze rekordów dotyczących przyrządu rejestrującego.

cardVehicleUnitRecords jest zbiorem rekordów zawierających informacje o używanych przyrządach rejestrujących.

2.41. **Certyfikat**

Certyfikat klucza publicznego wydany przez organ certyfikacji.

Generacja 1:

```
Certificate ::= OCTET STRING (SIZE(194))
```

Przypisanie wartości: podpis cyfrowy z częściowym odzyskiwaniem zawartości CertificateContent, zgodnie z dodatkiem 11 „Wspólne mechanizmy bezpieczeństwa": Podpis (128 bajtów) || Reszta klucza publicznego (58 bajtów) || Odnośnik do organu certyfikacji: (8 bajtów)

Generacja 2:

```
Certificate ::= OCTET STRING (SIZE(204..341))
```

Przypisanie wartości: zob. dodatek 11

2.42. **CertificateContent**

Generacja 1:

Treść certyfikatu klucza publicznego zgodnie z dodatkiem 11 – Wspólne mechanizmy bezpieczeństwa.

```
CertificateContent ::= SEQUENCE {
   certificateProfileIdentifier         INTEGER(0..255),
   certificationAuthorityReference      KeyIdentifier,
   certificateHolderAuthorisation       CertificateHolderAuthorisation,
   certificateEndOfValidity             TimeReal,
   certificateHolderReference           KeyIdentifier,
   publicKey                            PublicKey
}
```

certificateProfileIdentifier jest wersją odpowiedniego certyfikatu.

Przypisanie wartości: '01h' dla tej wersji.

certificationAuthorityReference identyfikuje organ certyfikacji wydający certyfikat. Jest tu także odesłanie do klucza publicznego tego organu certyfikacji.

certificateHolderAuthorisation identyfikuje prawa posiadacza certyfikatu.

certificateEndOfValidity jest datą administracyjnego wygaśnięcia certyfikatu.

certificateHolderReference identyfikuje posiadacza certyfikatu. Jest tu także odesłanie do jego klucza publicznego.

publicKey jest kluczem publicznym, który jest poświadczony tym certyfikatem.

2.43. **CertificateHolderAuthorisation**

Identyfikacja praw posiadacza certyfikatu.

```
CertificateHolderAuthorisation ::= SEQUENCE {
   tachographApplicationID              OCTET STRING(SIZE(6))
   equipmentType                        EquipmentType
}
```

Generacja 1:

tachographApplicationID jest identyfikatorem aplikacji dla aplikacji tachograficznej.

Przypisanie wartości: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. Ten AID jest zastrzeżonym, nierejestrowanym identyfikatorem aplikacji zgodnie z normą ISO/IEC 7816-5.

equipmentType jest identyfikacją typu urządzenia, dla którego przeznaczony jest certyfikat.

Przypisanie wartości: zgodnie z typem danych EquipmentType. **0** gdy jest to certyfikat jednego z państw członkowskich.

Generacja 2:

tachographApplicationID oznacza 6 najbardziej znaczących bajtów odpowiedniego identyfikatora aplikacji (AID) karty do tachografu generacji 2. AID dla aplikacji karty do tachografu określono w rozdziale 6.2.

Przypisanie wartości: 'FF 53 4D 52 44 54'.

equipmentType jest identyfikacją typu urządzenia określonego dla generacji 2, dla którego przeznaczony jest certyfikat.

Przypisanie wartości: zgodnie z typem danych EquipmentType.

2.44. **CertificateRequestID**

Jednoznaczna identyfikacja wniosku o certyfikat. Może być także używana jako identyfikator klucza publicznego przyrządu rejestrującego, jeżeli numer seryjny przyrządu rejestrującego, do którego ten klucz jest przeznaczony, nie jest znany w czasie sporządzania certyfikatu.

```
CertificateRequestID ::= SEQUENCE{
   requestSerialNumber                  INTEGER(0..2^32-1),
   requestMonthYear                     BCDString(SIZE(2)),
   crIdentifier                         OCTET STRING(SIZE(1)),
   manufacturerCode                     ManufacturerCode
}
```

requestSerialNumber jest numerem seryjnym wniosku o certyfikat, unikatowym dla producenta i miesiąca określonego poniżej.

requestMonthYear jest identyfikacją miesiąca i roku wniosku o certyfikat.

Przypisanie wartości: miesiąc (dwie cyfry) i rok (dwie ostatnie cyfry) w kodzie BCD.

crIdentifier: jest identyfikatorem umożliwiającym rozróżnienie wniosku o certyfikat od rozszerzonego numeru seryjnego.

Przypisanie wartości: 'FFh'.

manufacturerCode: jest kodem numerycznym producenta wnioskującego o certyfikat.

2.45. **CertificationAuthorityKID**

Identyfikator klucza publicznego organu certyfikacji (organu certyfikacji państwa członkowskiego lub europejskiego organu certyfikacji).

```
CertificationAuthorityKID ::= SEQUENCE{
   nationNumeric                        NationNumeric,
   nationAlpha                          NationAlpha,
   keySerialNumber                      INTEGER(0..255),
   additionalInfo                       OCTET STRING(SIZE(2)),
   caIdentifier                         OCTET STRING(SIZE(1))
}
```

nationNumeric jest numerycznym kodem krajowym organu certyfikacji.

nationAlpha jest alfanumerycznym kodem krajowym organu certyfikacji.

keySerialNumber jest numerem seryjnym umożliwiającym rozróżnienie różnych kluczy organu certyfikacji w przypadku zmiany kluczy.

additionalInfo jest dwubajtowym polem przeznaczonym na dodatkowy kod (swoisty dla organu certyfikacji).

caIdentifier jest identyfikatorem umożliwiającym rozróżnienie identyfikatora klucza organu certyfikacji od innych identyfikatorów kluczy.

Przypisanie wartości: '01h'.

2.46. **CompanyActivityData**

Informacje przechowywane na karcie firmowej dotyczące czynności wykonanych przy użyciu karty (wymagania 373 i 379 określone w załączniku 1C).

```
CompanyActivityData ::= SEQUENCE {
   companyPointerNewestRecord         INTEGER(0..NoOfCompanyActivityRecords-1),
   companyActivityRecords             SET SIZE(NoOfCompanyActivityRecords) OF
    companyActivityRecord              SEQUENCE {
     companyActivityType                CompanyActivityType,
     companyActivityTime                TimeReal,
     cardNumberInformation              FullCardNumber,
     vehicleRegistrationInformation     VehicleRegistrationIdentification,
     downloadPeriodBegin                TimeReal,
     downloadPeriodEnd                  TimeReal
    }
}
```

companyPointerNewestRecord jest indeksem ostatniego, uaktualnionego zapisu companyActivityRecord.

Przypisanie wartości: liczba odpowiadająca stanowi licznika rekordów czynności firmy, rozpoczynając od „0" dla pierwszego wystąpienia rekordu czynności firmy w strukturze.

companyActivityRecords są zbiorem wszystkich rekordów czynności firmy.

companyActivityRecord jest sekwencją informacji dotyczących jednej czynności firmy.

companyActivityType jest typem czynności firmy.

companyActivityTime jest datą i godziną czynności firmy.

cardNumberInformation jest numerem karty i państwa członkowskiego wydającego kartę, z której pobrano dane, gdy dotyczy.

vehicleRegistrationInformation jest numerem VRN i państwem członkowskim rejestracji pojazdu, dla którego pobrano dane lub zablokowano, lub zdjęto blokadę.

downloadPeriodBegin i **downloadPeriodEnd** jest okresem, dla którego pobrano dane z VU, gdy dotyczy.

2.47. **CompanyActivityType**

Kod wskazujący czynność wykonaną przez firmę z wykorzystaniem jej karty firmowej.

```
CompanyActivityType ::= INTEGER {
   card downloading                    (1),
   VU downloading                      (2),
   VU lock-in                          (3),
   VU lock-out                         (4)
}
```

2.48. **CompanyCardApplicationIdentification**

Informacje przechowywane na karcie firmowej dotyczące identyfikacji aplikacji na karcie (wymagania 369 i 375 określone w załączniku 1C).

```
CompanyCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfCompanyActivityRecords          NoOfCompanyActivityRecords
}
```

typeOfTachographCardId określa wdrożony typ karty.

cardStructureVersion określa wersję struktury wdrożonej na karcie.

noOfCompanyActivityRecords jest liczbą rekordów z czynnościami firmy, które można przechowywać na karcie.

2.49. **CompanyCardHolderIdentification**

Informacje przechowywane na karcie firmowej dotyczące identyfikacji posiadacza karty (wymagania 372 i 378 określone w załączniku 1C).

```
CompanyCardHolderIdentification ::= SEQUENCE {
   companyName                         Name,
   companyAddress                      Address,
   cardHolderPreferredLanguage         Language
}
```

companyName jest nazwą firmy posiadającej kartę.

companyAddress jest adresem firmy posiadającej kartę.

cardHolderPreferredLanguage jest preferowanym językiem posiadacza karty.

2.50. **ControlCardApplicationIdentification**

Informacje przechowywane na karcie kontrolnej dotyczące identyfikacji aplikacji na karcie (wymagania 357 i 363 określone w załączniku 1C).

```
ControlCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfControlActivityRecords          NoOfControlActivityRecords
}
```

typeOfTachographCardId określa wdrożony typ karty.

cardStructureVersion określa wersję struktury wdrożoną na karcie.

noOfControlActivityRecords jest liczbą rekordów czynności kontrolnych, które mogą być zapisane na karcie.

2.51. **ControlCardControlActivityData**

Informacje przechowywane na karcie kontrolnej dotyczące czynności wykonanych przy użyciu karty (wymagania 361 i 367 określone w załączniku 1C).

```
ControlCardControlActivityData ::= SEQUENCE {
   controlPointerNewestRecord        INTEGER(0.. NoOfControlActivityRecords-1),
   controlActivityRecords            SET SIZE(NoOfControlActivityRecords) OF
    controlActivityRecord             SEQUENCE {
     controlType                       ControlType,
     controlTime                       TimeReal,
     controlledCardNumber              FullCardNumber,
     controlledVehicleRegistration     VehicleRegistrationIdentification,
     controlDownloadPeriodBegin        TimeReal,
     controlDownloadPeriodEnd          TimeReal
    }
}
```

controlPointerNewestRecord jest indeksem ostatniego, uaktualnionego rekordu czynności kontrolnych.

Przypisanie wartości: liczba odpowiadająca stanowi licznika rekordów czynności kontrolnych, rozpoczynając od „0” dla pierwszego wystąpienia w strukturze rekordu czynności kontroli.

controlActivityRecords jest zbiorem wszystkich rekordów czynności kontrolnych.

controlActivityRecord jest ciągiem informacji dotyczących jednej kontroli.

controlType jest typem kontroli.

controlTime jest datą i godziną kontroli.

controlledCardNumber jest numerem karty i państwa członkowskiego wydającego kartę, która jest kontrolowana.

controlledVehicleRegistration jest numerem VRN i państwa członkowskiego rejestracji pojazdu, w którym miała miejsce kontrola.

controlDownloadPeriodBegin i **controlDownloadPeriodEnd** wyznaczają ostatecznie pobierany okres.

2.52. **ControlCardHolderIdentification**

Informacje przechowywane na karcie kontrolnej dotyczące identyfikacji posiadacza karty (wymagania 360 i 366 określone w załączniku 1C).

```
ControlCardHolderIdentification ::= SEQUENCE {
   controlBodyName                   Name,
   controlBodyAddress                Address,
   cardHolderName                    HolderName,
   cardHolderPreferredLanguage       Language
}
```

controlBodyName jest nazwą organu kontrolnego posiadacza karty.

controlBodyAddress jest adresem organu kontrolnego posiadacza karty.

cardHolderName jest nazwą i imieniem (imionami) posiadacza karty kontrolnej.

cardHolderPreferredLanguage jest preferowanym językiem posiadacza karty.

2.53. **ControlType**

Kod wskazujący czynności wykonane podczas kontroli. Ten typ danych związany jest z wymaganiami 126, 274, 299, 327 i 350 określonymi w załączniku 1C.

```
ControlType ::= OCTET STRING (SIZE(1))
```

Generacja 1:

Przypisanie wartości – zapisane oktetami: 'cvpdxxxx'B (8 bitów)

'c'B	pobieranie danych z karty:
	'0'B: nie pobrano danych z karty w czasie tej kontroli,
	'1'B: pobrano dane z karty w czasie tej kontroli
'v'B	pobieranie danych z VU:
	'0'B: nie pobrano danych z VU w czasie tej kontroli,
	'1'B: pobrano dane z VU w czasie tej kontroli
'p'B	drukowanie:
	'0'B: nie wykonano wydruków w czasie tej kontroli,
	'1'B: wykonano wydruki w czasie tej kontroli
'd'B	wyświetlacz:
	'0'B: nie użyto wyświetlacza w czasie tej kontroli,
	'1'B: użyto wyświetlacza w czasie tej kontroli
'xxxx'B	Nieużywany.

Generacja 2:

Przypisanie wartości – zapisane oktetami: 'cvpdexxx'B (8 bitów)

'c'B	pobieranie danych z karty:
	'0'B: nie pobrano danych z karty w czasie tej kontroli,
	'1'B: pobrano dane z karty w czasie tej kontroli
'v'B	pobieranie danych z VU:
	'0'B: nie pobrano danych z VU w czasie tej kontroli,
	'1'B: pobrano dane z VU w czasie tej kontroli
'p'B	drukowanie:
	'0'B: nie wykonano wydruków w czasie tej kontroli,
	'1'B: wykonano wydruki w czasie tej kontroli
'd'B	wyświetlacz:
	'0'B: nie użyto wyświetlacza w czasie tej kontroli,
	'1'B: użyto wyświetlacza w czasie tej kontroli

'e'B	kontrola drogowa kalibracji
	'0'B: parametry kalibracyjne nie zostały skontrolowane w czasie tej kontroli,
	'1'B: parametry kalibracyjne zostały skontrolowane w czasie tej kontroli,
'xxx'B	RFU.

2.54. **CurrentDateTime**

Bieżąca data i godzina urządzenia rejestrującego.

```
CurrentDateTime ::= TimeReal
```

Przypisanie wartości: nie określa się.

2.55. **CurrentDateTimeRecordArray**

Generacja 2:

Bieżąca data i godzina wraz z metadanymi stosowane w protokole pobierania danych.

```
CurrentDateTimeRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CurrentDateTime
}
```

recordType oznacza typ rekordu (CurrentDateTime). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość CurrentDateTime w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem rekordów z bieżącego dnia i godziny.

2.56. **DailyPresenceCounter**

Licznik znajdujący się na karcie kierowcy lub na karcie warsztatowej zwiększany o jeden dla każdego dnia kalendarzowego, w którym karta jest włożona do VU. Ten typ danych związany jest z wymaganiami 266, 299, 320 i 343 określonymi w załączniku 1C.

```
DailyPresenceCounter ::= BCDString(SIZE(2))
```

Przypisanie wartości: Kolejna liczba do maksymalnej wartości = 9 999, i następnie ponownie zaczyna od 0. Przy pierwszym wydaniu karty licznik jest ustawiany na 0.

2.57. **Datef**

Data wyrażona w czytelnym, przeznaczonym do druku formacie numerycznym.

```
Datef ::= SEQUENCE {
   year        BCDString(SIZE(2)),
   month       BCDString(SIZE(1)),
   day         BCDString(SIZE(1))
}
```

Przypisanie wartości:

yyyy	rok
mm	miesiąc
dd	dzień
'00000000'H	oznacza jednoznacznie brak daty.

2.58. **DateOfDayDownloaded**

Generacja 2:

data i godzina pobrania danych;

```
DateOfDayDownloaded ::= TimeReal
```

Przypisanie wartości: nie określa się.

2.59. **DateOfDayDownloadedRecordArray**

Generacja 2:

Data i godzina pobrania danych wraz z metadanymi stosowane w protokole pobierania danych.

```
DateofDayDownloadedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       DateOfDayDownloaded
}
```

recordType oznacza typ rekordu (DateOfDayDownloaded). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość CurrentDateTime w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem daty i godziny rekordów pobierania danych.

2.60. **Distance**

Przebyta odległość (wynik obliczenia różnicy między dwoma odczytami licznika kilometrów pojazdu wyrażona w kilometrach).

```
Distance ::= INTEGER(0..2^16-1)
```

Przypisanie wartości: liczba binarna bez znaku. Wartość w km w zakresie operacyjnym 0 do 9 999 km.

2.61. **DriverCardApplicationIdentification**

Informacje przechowywane na karcie kierowcy dotyczące identyfikacji aplikacji na karcie (wymagania 253 i 278 określone w załączniku 1C).

Generacja 1:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords
}
```

typeOfTachographCardId określa wdrożony typ karty.

cardStructureVersion określa wersję struktury wdrożonej na karcie.

noOfEventsPerType jest liczbą zdarzeń według typu zdarzenia możliwych do zarejestrowania na karcie.

noOfFaultsPerType jest liczbą usterek według typu usterki możliwych do zarejestrowania na karcie.

activityStructureLength podaje liczbę bajtów dostępnych do przechowywania rekordów czynności.

noOfCardVehicleRecords jest liczbą rekordów dotyczących pojazdów możliwych do zarejestrowania na karcie.

noOfCardPlaceRecords jest liczbą miejsc możliwych do zarejestrowania na karcie.

Generacja 2:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords,
   noOfGNSSCDRecords                   NoOfGNSSCDRecords,
   noOfSpecificConditionRecords        NoOfSpecificConditionRecords
}
```

Oprócz generacji 1 używane są następujące elementy danych:

noOfGNSSCDRecords jest liczbą rekordów nieprzerwanego czasu prowadzenia GNSS, które mogą być zapisane na karcie.

noOfSpecificConditionRecords jest liczbą rekordów warunków szczególnych, które mogą być zapisane na karcie.

2.62. DriverCardHolderIdentification

Informacje przechowywane na karcie kierowcy dotyczące identyfikacji posiadacza karty (wymagania 256 i 281 określone w załączniku 1C).

```
DriverCardHolderIdentification ::= SEQUENCE {
   cardHolderName                      HolderName,
   cardHolderBirthDate                 Datef,
   cardHolderPreferredLanguage         Language
}
```

cardHolderName jest nazwą i imieniem (imionami) posiadacza karty kierowcy.

cardHolderBirthDate jest datą urodzenia posiadacza karty kierowcy.

cardHolderPreferredLanguage jest preferowanym językiem posiadacza karty.

2.63. **DSRCSecurityData**

Generacja 2:

Informacje w formie odkrytego tekstu oraz MAC przekazywane za pośrednictwem DSRC z tachografu do zdalnego interrogatora (RI), szczegółowe informacje – zob. dodatek 11 część B rozdział 13.

```
DSRCSecurityData ::= SEQUENCE {
   tagLenthPlainText                    OCTET STRING(SIZE(2)),
   currentDateTime                      CurrentDateTime,
   counter                              INTEGER(0..2^24-1),
   vuSerialNumber                       VuSerialNumber,
   dSRCMKVersionNumber                  INTEGER(SIZE(1)),
   tagLengthMac                         OCTET STRING(SIZE(2)),
   mac                                  MAC
}
```

tagLength jest częścią kodowania DER-TLV i ma przypisaną wartość „81 10” (zob. dodatek 11 część B rozdział 13).

currentDateTime jest bieżącą datą i godziną przyrządu rejestrującego.

counter nadaje numery komunikatom RTM.

vuSerialNumber jest numerem seryjnym przyrządu rejestrującego.

dSRCMKVersionNumber jest numerem wersji klucza głównego DSRC, z którego zostały wyprowadzone poszczególne klucze DSRC dla VU.

tagLengthMac jest znacznikiem i długością obiektu danych MAC w ramach kodowania DER-TLV. Znacznik musi być ustawiony na wartość „8E”, długość musi kodować długość MAC w oktetach (zob. dodatek 11 część B rozdział 13).

mac jest MAC obliczanym na podstawie komunikatu RTM (zob. dodatek 11 część B rozdział 13).

2.64. **EGFCertificate**

Generacja 2:

Certyfikat klucza publicznego urządzenia zewnętrznego GNSS na potrzeby wzajemnego uwierzytelniania z VU. Strukturę tego certyfikatu określono w dodatku 11.

```
EGFCertificate ::= Certificate
```

2.65. **EmbedderIcAssemblerId**

Dostarcza informacje o wbudowującym układ scalony.

```
EmbedderIcAssemblerId ::= SEQUENCE{
   countryCode                          IA5String(SIZE(2)),
   moduleEmbedder                       BCDString(SIZE(2)),
   manufacturerInformation              OCTET STRING(SIZE(1))
}
```

countryCode jest 2-literowym kodem państwa wbudowującego moduł zgodnie z normą ISO 3166.

moduleEmbedder oznacza wbudowującego moduł.

manufacturerInformation na potrzeby użytku wewnętrznego producenta.

2.66. **EntryTypeDailyWorkPeriod**

Kod umożliwiający rozróżnienie między początkiem a końcem wpisu dotyczącego dziennego okresu pracy oraz miejsca i sposobu wprowadzenia wpisu.

Generacja 1

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5)
}
```

Przypisanie wartości: zgodnie z normą ISO/IEC8824-1.

Generacja 2

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5),
   Begin,  related time based on GNSS data                             (6),
   End     related time based on GNSS data                             (7)
}
```

Przypisanie wartości: zgodnie z normą ISO/IEC8824-1.

2.67. **EquipmentType**

Kod umożliwiający rozróżnienie typów urządzeń dla aplikacji tachograficznej.

```
EquipmentType ::= INTEGER(0..255)
```

Generacja 1:

```
--Reserved                          (0),
--Driver Card                       (1),
--Workshop Card                     (2),
--Control Card                      (3),
--Company Card                      (4),
--Manufacturing Card                (5),
--Vehicle Unit                      (6),
--Motion Sensor                     (7),
--RFU                               (8..255)
```

Przypisanie wartości: zgodnie z normą ISO/IEC8824-1.

Wartość 0 jest zastrzeżona do celów oznaczenia państwa członkowskiego lub Europy w rubryce CHA certyfikatów.

Generacja 2:

Takie same wartości jak w przypadku generacji 1 z następującymi uzupełnieniami:

```
--GNSS Facility                          (8),
--Remote Communication Module            (9),
--ITS interface module                   (10),
--Plaque                                 (11), -- may be used in SealRecord
--M1/N1 Adapter                          (12), -- may be used in SealRecord
--European Root CA (ERCA)                (13),
--Member State CA (MSCA)                 (14),
--External GNSS connection               (15), -- may be used in SealRecord
--Unused                                 (16), -- used in SealDataVu
--RFU                                    (17..255)
```

Uwaga: Wartości generacji 2 dla tabliczki, adaptera, połączenia zewnętrznego GNSS, a także wartości generacji 1 dla przyrządu rejestrującego oraz czujnika ruchu mogą być, w stosownych przypadkach, używane w SealRecord.

2.68. **EuropeanPublicKey**

Generacja 1:

Europejski klucz publiczny.

```
EuropeanPublicKey ::= PublicKey
```

2.69. **EventFaultRecordPurpose**

Kod wyjaśniający, dlaczego zarejestrowano zdarzenie lub usterkę.

```
EventFaultRecordPurpose ::= OCTET STRING (SIZE(1))
```

Przypisanie wartości:

'00'H	jedno/jedna z 10 ostatnich zdarzeń lub usterek (lub ostatnie/ostatnia zdarzenie lub usterka)
'01'H	najdłuższe zdarzenie w jednym z ostatnich 10 dni ich występowania
'02'H	jedno z 5 najdłuższych zdarzeń w ciągu ostatnich 365 dni
'03'H	ostatnie zdarzenie w jednym z ostatnich 10 dni ich występowania
'04'H	najpoważniejsze zdarzenie w jednym z ostatnich 10 dni ich występowania
'05'H	jedno z 5 najpoważniejszych zdarzeń w ciągu ostatnich 365 dni
'06'H	pierwsze zdarzenie lub usterka zaistniałe po ostatniej kalibracji
'07'H	aktywne/trwające zdarzenie lub usterka
'08'H to '7F'H	RFU
'80'H to 'FF'H	swoisty dla producenta.

2.70. **EventFaultType**

Kod kwalifikujący zdarzenie lub usterkę.

```
EventFaultType ::= OCTET STRING (SIZE(1))
```

Przypisanie wartości:

Generacja 1:

'0x'H	zdarzenia ogólne
'00'H	brak dalszych szczegółów,
'01'H	włożenie nieważnej karty,
'02'H	konflikt kart,
'03'H	nakładające się czasy,
'04'H	prowadzenie pojazdu bez prawidłowej karty,
'05'H	włożenie karty podczas prowadzenia pojazdu,
'06'H	sesja ostatniej karty niezamknięta prawidłowo,
'07'H	przekroczenie prędkości,
'08'H	przerwa w zasilaniu,
'09'H	błąd danych dotyczących ruchu,
'0A'H	Konflikt ruchu pojazdu,
'0B' to '0F'H	RFU,

	zdarzenia związane z próbami naruszenia zabezpieczenia przyrządu rejestrującego,
‘1x’H	brak dalszych szczegółów,
‘10’H	błąd uwierzytelnienia czujnika ruchu,
‘11’H	błąd uwierzytelnienia kart do tachografów,
‘12’H	nieupoważniona zmiana w czujniku ruchu,
‘13’H	błąd integralności wprowadzania danych na kartę
‘14’H	błąd integralności przechowywanych danych użytkownika,
‘15’H	błąd wewnętrznego przesyłania danych,
‘16’H	nieupoważnione otwarcie obudowy,
‘17’H	uszkodzenie sprzętu,
‘18’H	RFU,
‘19’H to ‘1F’H	
‘2x’H	zdarzenia związane z próbami naruszenia zabezpieczenia czujnika,
‘20’H	brak dalszych szczegółów,
‘21’H	błąd uwierzytelnienia,
‘22’H	błąd integralności przechowywanych danych,
‘23’H	błąd wewnętrznego przesyłania danych,
‘24’H	nieupoważnione otwarcie obudowy,
‘25’H	uszkodzenie sprzętu,
‘26’H to ‘2F’H	RFU,
‘3x’H	usterki urządzenia rejestrującego,
‘30’H	brak dalszych szczegółów,
‘31’H	usterka wewnętrzna VU,
‘32’H	usterka drukarki,
‘33’H	usterka wyświetlacza,
‘34’H	usterka pobierania danych,
‘35’H	usterka czujnika,
‘36’H to ‘3F’H	RFU,
‘4x’H	usterki karty,
‘40’H	brak dalszych szczegółów,
‘41’H to ‘4F’H	RFU,
‘50’H to ‘7F’H	RFU,
‘80’H to ‘FF’H	swoisty dla producenta.

Generacja 2:

Takie same wartości jak w przypadku generacji 1 z następującymi uzupełnieniami:

‘0B’H	konflikt czasu (GNSS i wewnętrzny zegar VU),
‘0C’ to ‘0F’H	RFU,
‘5x’H	usterki związane z GNSS,
‘50’H	brak dalszych szczegółów,
‘51’H	usterka wewnętrzna odbiornika GNSS,
‘52’H	usterka zewnętrzna odbiornika GNSS,
‘53’H	usterka zewnętrzna komunikacji GNSS,
‘54’H	brak danych GNSS dotyczących położenia
‘55’H	wykrycie ingerencji w GNSS,
‘56’H	wygaśnięcie certyfikatu urządzenia zewnętrznego GNSS,
‘57’H to ‘5F’H	RFU,
‘6x’H	usterki związane z modułem komunikacji na odległość
‘60’H	brak dalszych szczegółów,
‘61’H	usterka modułu komunikacji na odległość,
‘62’H	usterka modułu komunikacji związana z łącznością,
‘63’H to ‘6F’H	RFU,
‘7x’H	usterki związane z interfejsem ITS,
‘70’H	brak dalszych szczegółów,
‘71’H to ‘7F’H	RFU.

2.71. **ExtendedSealIdentifier**

Generacja 2:

Rozszerzony identyfikator plomby jednoznacznie identyfikuje plombę (wymaganie 401 określone w załączniku 1C).

```
ExtendedSealIdentifier ::= SEQUENCE{
   manufacturerCode                    OCTET STRING (SIZE(2)),
   sealIdentifier                      OCTET STRING (SIZE(6))
}
```

manufacturerCode: jest kodem producenta plomby.

sealIdentifier jest identyfikatorem plomby, który jest niepowtarzalny dla producenta.

2.72. **ExtendedSerialNumber**

Unikalna identyfikacja urządzenia. Może być używana także jako identyfikator klucza publicznego urządzenia.

Generacja 1:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                        INTEGER(0..2^32-1),
   monthYear                           BCDString(SIZE(2)),
   type                                OCTET STRING(SIZE(1)),
   manufacturerCode                    ManufacturerCode
}
```

serialNumber jest numerem seryjnym urządzenia, niepowtarzalnym dla producenta, typu urządzenia i miesiąca oraz roku, jak wyjaśniono poniżej.

monthYear jest identyfikacją miesiąca i roku produkcji (lub przypisanym numerem seryjnym).

Przypisanie wartości: miesiąc (dwie cyfry) i rok (dwie ostatnie cyfry) w kodzie BCD.

type jest identyfikatorem typu urządzenia.

Przypisanie wartości: swoisty dla producenta, z wartością zastrzeżoną „FFh".

manufacturerCode: jest kodem numerycznym identyfikującym producenta homologowanego urządzenia.

Generacja 2:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                        INTEGER(0..2^32-1),
   monthYear                           BCDString(SIZE(2)),
   type                                EquipmentType,
   manufacturerCode                    ManufacturerCode
}
```

serialNumber, zob. generacja 1

monthYear, zob. generacja 1

type jest identyfikatorem typu urządzenia

manufacturerCode: zob. generacja 1.

2.73. **FullCardNumber**

Kod całkowicie identyfikujący kartę do tachografu.

```
FullCardNumber ::= SEQUENCE {
   cardType                              EquipmentType,
   cardIssuingMemberState                NationNumeric,
   cardNumber                            CardNumber
}
```

cardType jest typem karty do tachografu.

cardIssuingMemberState jest kodem państwa członkowskiego, które wydało kartę.

cardNumber jest numerem karty.

2.74. **FullCardNumberAndGeneration**

Generacja 2:

Kod całkowicie identyfikujący kartę do tachografu i jej generację.

```
FullCardNumberAndGeneration ::= SEQUENCE {
   fullCardNumber                        FullCardNumber,
   generation                            Generation
}
```

fullcardNumber identyfikuje kartę do tachografu.

generation oznacza generację używanej karty do tachografu.

2.75. **Generation**

Generacja 2:

wskazuje generację używanego tachografu.

```
Generation ::= INTEGER(0..255)
```

Przypisanie wartości:

'00'H	RFU
'01'H	Generacja 1
'02'H	Generacja 2
'03'H .. 'FF'H	RFU

2.76. **GeoCoordinates**

Generacja 2:

Współrzędne geograficzne są zakodowane jako liczby całkowite. Takie liczby są wielokrotnościami kodowania ± DDMM.M dla szerokości geograficznej i ± DDDMM.M dla długości geograficznej. W powyższym przypadku odpowiednio ± DD i ± DDD oznaczają stopnie, a MM.M minuty.

```
GeoCoordinates ::= SEQUENCE {
   latitude                              INTEGER(-90000..90001),
   longitude                             INTEGER(-180000..180001)
}
```

latitude koduje się jako wielokrotność (mnożnik 10) zapisu ± DDMM.M.

longitude koduje się jako wielokrotność (mnożnik 10) zapisu ± DDMM.M.

2.77. **GNSSAccuracy**

Generacja 2:

Dokładność danych GNSS dotyczących położenia (definicja eee)). Taka dokładność jest kodowana jako liczba całkowita i jest wielokrotnością (mnożnik 10) wartości X.Y podanej w zdaniu GSA NMEA.

```
GNSSAccuracy ::= INTEGER(1..100)
```

2.78. **GNSSContinuousDriving**

Generacja 2:

Informacje zapisane na karcie kierowcy lub na karcie warsztatowej dotyczące położenia pojazdu GNSS, jeżeli nieprzerwany czas prowadzenia pojazdu przez kierowcę osiągnie wielokrotność trzech godzin (wymagania 306 i 354 określone w załączniku 1C).

```
GNSSContinuousDriving := SEQUENCE {
   gnssCDPointerNewestRecord            INTEGER(0..NoOfGNSSCDRecords -1),
   gnssContinuousDrivingRecords         SET SIZE(NoOfGNSSCDRecords) OF
                                        GNSSContinuousDrivingRecord
}
```

controlPointerNewestRecord jest indeksem ostatniego uaktualnionego rekordu nieprzerwanego prowadzenia pojazdu GNSS.

Przypisanie wartości: liczba odpowiadająca stanowi licznika rekordu GNSS dotyczącego nieprzerwanego prowadzenia pojazdu, rozpoczynając od „0" dla pierwszego wystąpienia w strukturze rekordu GNSS dotyczącego nieprzerwanego czasu prowadzenia pojazdu.

gnssContinuousDrivingRecords jest zbiorem rekordów zawierających datę i godzinę, kiedy nieprzerwany czas prowadzenia pojazdu osiąga wielokrotność trzech godzin i informacji na temat położenia pojazdu.

2.79. **GNSSContinuousDrivingRecord**

Generacja 2:

Informacje przechowywane na karcie kierowcy lub na karcie warsztatowej dotyczące położenia pojazdu GNSS, jeżeli nieprzerwany czas prowadzenia pojazdu przez kierowcę osiągnie wielokrotność trzech godzin (wymagania 305 i 353 określone w załączniku 1C).

```
GNSSContinuousDrivingRecord ::= SEQUENCE {
   timeStamp                            TimeReal,
   gnssPlaceRecord                      GNSSPlaceRecord
}
```

timeStamp jest datą i godziną, kiedy nieprzerwany czas prowadzenia pojazdu przez posiadacza karty osiągnie wielokrotność trzech godzin.

gnssPlaceRecord zawiera informacje dotyczące położenia pojazdu.

2.80. **GNSSPlaceRecord**

Generacja 2:

Informacje dotyczące położenia GNSS pojazdu (wymagania 108, 109, 110, 296, 305, 347 i 353 określone w załączniku 1C).

```
GNSSPlaceRecord ::= SEQUENCE {
   timeStamp                            TimeReal,
   gnssAccuracy                         GNSSAccuracy,
   geoCoordinates                       GeoCoordinates
}
```

timeStamp jest datą i godziną określenia położenia GNSS pojazdu.

gnssAccuracy jest dokładnością danych dotyczących położenia GNSS.

geoCoordinates jest lokalizacją zapisaną przy użyciu GNSS.

2.81. **HighResOdometer**

Stan licznika kilometrów pojazdu: skumulowana odległość przebyta przez pojazd w czasie jego eksploatacji.

```
HighResOdometer ::= INTEGER(0..2^32-1)
```

Przypisanie wartości: liczba binarna bez znaku. Wartość wyrażona w 1/200 km w zakresie operacyjnym 0 do 21 055 406 km.

2.82. **HighResTripDistance**

Odległość przebyta w czasie całej lub części podróży.

```
HighResTripDistance ::= INTEGER(0..2^32-1)
```

Przypisanie wartości: liczba binarna bez znaku. Wartość wyrażona w 1/200 km w zakresie operacyjnym 0 do 21 055 406 km.

2.83. **HolderName**

Nazwisko i imię (imiona) posiadacza karty.

```
HolderName ::= SEQUENCE {
   holderSurname                    Name,
   holderFirstNames                 Name
}
```

holderSurname jest nazwiskiem posiadacza. Do nazwiska nie dodaje się tytułów.

Przypisanie wartości: w przypadku kart nieosobowych, holderSurname zawiera te same informacje, co companyName lub workshopName, lub controlBodyName.

holderFirstNames oznacza imię (imiona) i inicjały posiadacza.

2.84. **InternalGNSSReceiver**

Generacja 2:

Informacje, czy odbiornik GNSS znajduje się wewnątrz czy na zewnątrz przyrządu rejestrującego. Prawda – oznacza, że odbiornik GNSS znajduje się wewnątrz VU. Fałsz – oznacza, że odbiornik GNSS jest zewnętrzny.

```
InternalGNSSReceiver ::= BOOLEAN
```

2.85. **K-ConstantOfRecordingEquipment**

Stała urządzenia rejestrującego (definicja m)).

```
K-ConstantOfRecordingEquipment ::= INTEGER(0..2^16-1)
```

Przypisanie wartości: liczba impulsów na kilometr w zakresie operacyjnym 0 do 64 255 impulsów/km.

2.86. **KeyIdentifier**

Unikalny identyfikator klucza publicznego używany przy odwoływaniu się do klucza i do wybierania klucza. Identyfikuje także posiadacza klucza.

```
KeyIdentifier ::= CHOICE {
   extendedSerialNumber                ExtendedSerialNumber,
   certificateRequestID                CertificateRequestID,
   certificationAuthorityKID           CertificationAuthorityKID
}
```

Pierwsza pozycja jest odpowiednia przy odesłaniu do klucza publicznego przyrządu rejestrującego lub karty do tachografu.

Druga pozycja jest odpowiednia przy odesłaniu do klucza publicznego przyrządu rejestrującego (w przypadku, gdy numer seryjny przyrządu rejestrującego może nie być znany w czasie sporządzenia certyfikatu).

Trzecia pozycja jest odpowiednia przy odesłaniu do klucza publicznego państwa członkowskiego.

2.87. **KMWCKey**

Generacja 2:

Klucz AES i związana z nim wersja klucza stosowane do sparowania VU z czujnikiem ruchu. Szczegółowe informacje – zob. dodatek 11.

```
KMWCKey ::= SEQUENCE {
   kMWCKey                             AESKey,
   keyVersion                          INTEGER (SIZE(1))
}
```

kMWCKey jest długością klucza AES w szeregu z kluczem stosowanym do sparowania VU z czujnikiem ruchu.

keyVersion oznacza wersję klucza AES.

2.88. **Language**

Kod identyfikujący język.

```
Language ::= IA5String(SIZE(2))
```

Przypisanie wartości: kod składający się z dwóch małych liter zgodny z normą ISO 639.

2.89. **LastCardDownload**

Data i godzina, zapisane na karcie kierowcy, ostatniego pobierania danych z karty (do innych celów niż kontrola) – wymagania 257 i 282 określone w załączniku 1C. Datę tę aktualizuje VU lub dowolny czytnik kart.

```
LastCardDownload ::= TimeReal
```

Przypisanie wartości: nie określa się.

2.90. **LinkCertificate**

Generacja 2:

Certyfikat połączenia par kluczy Głównego Europejskiego Organu Certyfikacji.

```
LinkCertificate ::= Certificate
```

2.91. **L-TyreCircumference**

Obwód toczny opon (definicja u)).

```
L-TyreCircumference ::= INTEGER(0.. 2^16-1)
```

Przypisanie wartości: liczba binarna bez znaku, wyrażona w 1/8 mm w zakresie operacyjnym 0 do 8 031 mm.

2.92. **MAC**

Generacja 2:

Kryptograficzna suma kontrolna o długości 8, 12 lub 16 bajtów odpowiadającej mechanizmom szyfrowania określonym w dodatku 11.

```
MAC ::= CHOICE {
   mac8                                 OCTET STRING (SIZE(8)),
   mac12                                OCTET STRING (SIZE(12)),
   mac16                                OCTET STRING (SIZE(12))
}
```

2.93. **ManualInputFlag**

Kod identyfikujący czy posiadacz karty wprowadza ręcznie czynności kierowcy przy wkładaniu karty (wymaganie 081 określone w załączniku 1B i wymaganie 102 określone w załączniku 1C).

```
ManualInputFlag ::= INTEGER {
   noEntry                              (0)
   manualEntries                        (1)
}
```

Przypisanie wartości: nie określa się.

2.94. **ManufacturerCode**

Kod identyfikujący producenta urządzeń posiadających homologację typu.

```
ManufacturerCode ::= INTEGER(0..255)
```

Laboratorium właściwe dla przeprowadzania badań interoperacyjności prowadzi i publikuje wykaz kodów producenta na swojej stronie internetowej (wymaganie 454 określone w załączniku 1C).

ManufacturerCodes przyznaje się tymczasowo twórcom tachografów po wystąpieniu przez nich z wnioskiem do laboratorium właściwego dla przeprowadzania badań interoperacyjności.

2.95. **ManufacturerSpecificEventFaultData**

Generacja 2:

Swoiste dla producentów kody błędów upraszczają analizę błędów oraz konserwację przyrządów rejestrujących.

```
ManufacturerSpecificEventFaultData ::= SEQUENCE {
   manufacturerCode                     ManufacturerCode,
   manufacturerSpecificErrorCode        OCTET STRING(SIZE(3))
}
```

manufacturerCode identyfikuje producenta przyrządu rejestrującego.

manufacturerSpecificErrorCode jest kodem błędu swoistym dla producenta.

2.96. **MemberStateCertificate**

Certyfikat klucza publicznego państwa członkowskiego wydany przez europejski organ certyfikacji.

```
MemberStateCertificate ::= Certificate
```

2.97. **MemberStateCertificateRecordArray**

Generacja 2:

Certyfikat państwa członkowskiego wraz z metadanymi stosowany w protokole pobierania danych.

```
MemberStateCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       MemberStateCertificate
}
```

recordType oznacza typ rekordu (MemberStateCertificate). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość MemberStateCertificate w bajtach.

noOfRecords jest liczbą rekordów w zbiorze. Wartość tę należy ustawić na 1, ponieważ certyfikaty mogą mieć różne długości.

records jest zbiorem certyfikatów państw członkowskich.

2.98. **MemberStatePublicKey**

Generacja 1:

Klucz publiczny państwa członkowskiego.

```
MemberStatePublicKey ::= PublicKey
```

2.99. **Name**

Nazwa (nazwisko).

```
Name ::= SEQUENCE {
   codePage                            INTEGER (0..255),
   name                                OCTET STRING (SIZE(35))
}
```

codePage określa zestaw znaków zdefiniowany w rozdziale 4,

name jest nazwą zakodowaną przy użyciu wyszczególnionego zestawu znaków.

2.100. **NationAlpha**

Alfabetyczne określenie państwa musi być zgodne ze znakami wyróżniającymi stosowanymi na pojazdach w ruchu międzynarodowym (Konwencja wiedeńska Narodów Zjednoczonych o ruchu drogowym z 1968 r.).

```
NationAlpha ::= IA5String(SIZE(3))
```

Kody Nation Alpha i Numeric znajdują się na wykazie utrzymywanym na stronie internetowej laboratorium wyznaczonego do przeprowadzenia badań interoperacyjności zgodnie z wymaganiem 440 określonym w załączniku 1C.

2.101. **NationNumeric**

Numeryczne odesłanie do państwa.

```
NationNumeric ::= INTEGER(0 .. 255)
```

Przypisanie wartości: zob. typ danych w 2.100 (NationAlpha)

Modyfikacji lub aktualizacji specyfikacji Nation Alpha lub Numeric opisanych w powyższym akapicie dokonuje się dopiero po otrzymaniu przez wyznaczone laboratorium opinii producentów przyrządów rejestrujących tachografów cyfrowych i inteligentnych posiadających homologację typu.

2.102. **NoOfCalibrationRecords**

Liczba rekordów kalibracyjnych, możliwych do przechowywania na karcie.

Generacja 1:

```
NoOfCalibrationRecords ::= INTEGER(0..255)
```

Przypisanie wartości: zob. dodatek 2.

Generacja 2:

```
NoOfCalibrationRecords ::= INTEGER(0..2^16-1)
```

Przypisanie wartości: zob. dodatek 2.

2.103. **NoOfCalibrationsSinceDownload**

Licznik pokazujący liczbę kalibracji wykonanych przy użyciu karty warsztatowej od ostatniego pobrania danych z tej karty (wymaganie 317 i 340 określone w załączniku 1C).

```
NoOfCalibrationsSinceDownload ::= INTEGER(0..2^16-1)
```

Przypisanie wartości: nie określa się.

2.104. **NoOfCardPlaceRecords**

Liczba rekordów dotyczących miejsca, możliwych do przechowywania na karcie kierowcy lub na karcie warsztatowej.

Generacja 1:

```
NoOfCardPlaceRecords ::= INTEGER(0..255)
```

Przypisanie wartości: zob. dodatek 2.

Generacja 2:

```
NoOfCardPlaceRecords ::= INTEGER(0..2^16-1)
```

Przypisanie wartości: zob. dodatek 2.

2.105. **NoOfCardVehicleRecords**

Liczba rekordów dotyczących użytych pojazdów, możliwych do przechowywania na karcie kierowcy lub na karcie warsztatowej.

```
NoOfCardVehicleRecords ::= INTEGER(0.. 2^16-1)
```

Przypisanie wartości: zob. dodatek 2.

2.106. **NoOfCardVehicleUnitRecords**

Generacja 2:

Liczba rekordów dotyczących przyrządów rejestrujących, możliwych do przechowywania na karcie kierowcy lub na karcie warsztatowej.

```
NoOfCardVehicleUnitRecords ::= INTEGER(0.. 2^16-1)
```

Przypisanie wartości: zob. dodatek 2.

2.107. **NoOfCompanyActivityRecords**

Liczba rekordów dotyczących czynności firmy, możliwych do przechowywania na karcie firmowej.

```
NoOfCompanyActivityRecords ::= INTEGER(0.. 2^16-1)
```

Przypisanie wartości: zob. dodatek 2.

2.108. **NoOfControlActivityRecords**

Liczba rekordów dotyczących czynności kontrolnych, możliwych do przechowywania na karcie kontrolnej.

```
NoOfControlActivityRecords ::= INTEGER(0.. 2^16-1)
```

Przypisanie wartości: zob. dodatek 2.

2.109. **NoOfEventsPerType**

Liczba zdarzeń według typu, możliwych do przechowywania na karcie.

```
NoOfEventsPerType ::= INTEGER(0..255)
```

Przypisanie wartości: zob. dodatek 2.

2.110. **NoOfFaultsPerType**

Liczba usterek według typu, możliwych do przechowywania na karcie.

```
NoOfFaultsPerType ::= INTEGER(0..255)
```

Przypisanie wartości: zob. dodatek 2.

2.111. **NoOfGNSSCDRecords**

Generacja 2:

Liczba rekordów nieprzerwanego czasu prowadzenia pojazdu GNSS, które mogą być przechowywane na karcie.

```
NoOfGNSSCDRecords ::= INTEGER(0..2^16-1)
```

Przypisanie wartości: zob. dodatek 2.

2.112. **NoOfSpecificConditionRecords**

Generacja 2:

Liczba rekordów warunków szczególnych, które mogą być przechowywane na karcie.

```
NoOfSpecificConditionRecords ::= INTEGER(0..2^16-1)
```

Przypisanie wartości: zob. dodatek 2.

2.113. **OdometerShort,**

Stan licznika kilometrów pojazdu w skróconej postaci.

```
OdometerShort ::= INTEGER(0..2^24-1)
```

Przypisanie wartości: liczba binarna bez znaku. Wartość w km w zakresie operacyjnym 0 do 9 999 999 km.

2.114. **OdometerValueMidnight**

Stan licznika kilometrów o północy w danym dniu (wymaganie 090 określone w załączniku 1B i wymaganie 113 określone w załączniku 1C).

```
OdometerValueMidnight ::= OdometerShort
```

Przypisanie wartości: nie określa się.

2.115. **OdometerValueMidnightRecordArray**

Generacja 2:

OdometerValueMidnight wraz z metadanymi stosowany w protokole pobierania danych.

```
OdometerValueMidnightRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       OdometerValueMidnight
}
```

recordType oznacza typ rekordu (OdometerValueMidnight). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość OdometerValueMidnight w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem rekordów OdometerValueMidnight.

2.116. **OverspeedNumber**

Liczba zdarzeń przekroczenia prędkości od ostatniej kontroli przekroczenia prędkości.

```
OverspeedNumber ::= INTEGER(0..255)
```

Przypisanie wartości: 0 oznacza, że nie było zdarzenia przekroczenie prędkości od ostatniej kontroli przekroczenia prędkości, 1 oznacza, że było jedno zdarzenie przekroczenia prędkości od ostatniej kontroli przekroczenia prędkości... 255 oznacza, że było 255 lub więcej zdarzeń przekroczenia prędkości od ostatniej kontroli przekroczenia prędkości.

2.117. **PlaceRecord**

Informacje dotyczące miejsca rozpoczęcia lub zakończenia dziennego okresu pracy (wymagania 108, 271, 296, 324 i 347 określone w załączniku 1C).

Generacja 1:

```
PlaceRecord ::= SEQUENCE {
   entryTime                        TimeReal,
   entryTypeDailyWorkPeriod         EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry           NationNumeric,
   dailyWorkPeriodRegion            RegionNumeric,
   vehicleOdometerValue             OdometerShort
}
```

entryTime jest datą i godziną wpisu.

entryTypeDailyWorkPeriod jest typem wpisu.

dailyWorkPeriodCountry jest wprowadzonym państwem.

dailyWorkPeriodRegion jest wprowadzonym regionem.

vehicleOdometerValue jest stanem licznika kilometrów w czasie wprowadzania miejsca.

Generacja 2:

```
PlaceRecord ::= SEQUENCE {
   entryTime                        TimeReal,
   entryTypeDailyWorkPeriod         EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry           NationNumeric,
   dailyWorkPeriodRegion            RegionNumeric,
   vehicleOdometerValue             OdometerShort,
   entryGNSSPlaceRecord             GNSSPlaceRecord
}
```

Oprócz generacji 1 używany jest następujący element składowy:

entryGNSSPlaceRecord jest zapisaną lokalizacją i godziną.

2.118. **PreviousVehicleInfo**

Informacje dotyczące pojazdu poprzednio używanego przez kierowcę w chwili wkładania jego karty do przyrządu rejestrującego (wymaganie 081 określone w załączniku 1B i wymaganie 102 określone w załączniku 1C).

Generacja 1:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal
}
```

vehicleRegistrationIdentification wskazuje numer VRN i państwo członkowskie rejestracji pojazdu.

cardWithdrawalTime jest datą i godziną wyjęcia karty.

Generacja 2:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal,
   vuGeneration                           Generation
}
```

Oprócz generacji 1 używany jest następujący element danych:

vuGeneration identyfikuje generację przyrządu rejestrującego.

2.119. **PublicKey**

Generacja 1:

Klucz publiczny RSA.

```
PublicKey ::= SEQUENCE {
   rsaKeyModulus                    RSAKeyModulus,
   rsaKeyPublicExponent             RSAKeyPublicExponent
}
```

rsaKeyModulus jest modułem pary kluczy.

rsaKeyPublicExponent jest wykładnikiem publicznym pary kluczy.

2.120. **RecordType**

Generacja 2:

Odniesienie do typu rekordu. Ten typ danych stosuje się w RecordArrays.

```
RecordType ::= OCTET STRING(SIZE(1))
```

Przypisanie wartości:

'01'H	ActivityChangeInfo,
'02'H	CardSlotsStatus,
'03'H	CurrentDateTime,
'04'H	MemberStateCertificate,
'05'H	OdometerValueMidnight,
'06'H	DateOfDayDownloaded,
'07'H	SensorPaired,
'08'H	Signature,
'09'H	SpecificConditionRecord,
'0A'H	VehicleIdentificationNumber,
'0B'H	VehicleRegistrationNumber,
'0C'H	VuCalibrationRecord,
'0D'H	VuCardIWRecord,
'0E'H	VuCardRecord,
'0F'H	VuCertificate,
'10'H	VuCompanyLocksRecord,
'11'H	VuControlActivityRecord,
'12'H	VuDetailedSpeedBlock,
'13'H	VuDownloadablePeriod,
'14'H	VuDownloadActivityData,
'15'H	VuEventRecord,
'16'H	VuGNSSCDRecord,
'17'H	VuITSConsentRecord,
'18'H	VuFaultRecord,
'19'H	VuIdentification,
'1A'H	VuOverSpeedingControlData,
'1B'H	VuOverSpeedingEventRecord,
'1C'H	VuPlaceDailyWorkPeriodRecord,
'1D'H	VuTimeAdjustmentGNSSRecord,
'1E'H	VuTimeAdjustmentRecord,
'1F'H	VuPowerSupplyInterruptionRecord,
'20'H	SensorPairedRecord,
'21'H	SensorExternalGNSSCoupledRecord,
'22'H to '7F'H	RFU,
'80'H to 'FF'H	swoisty dla producenta.

2.121. **RegionAlpha**

Alfabetyczne odniesienie do regionu w określonym kraju.

```
RegionAlpha ::= IA5STRING(SIZE(3))
```

Generacja 1:

Przypisanie wartości:

```
‘   ’         No information available,
Spain:
‘AN ’         Andalucía,
‘AR ’         Aragón,
‘AST’         Asturias,
‘C  ’         Cantabria,
‘CAT’         Cataluña,
‘CL ’         Castilla-León,
‘CM ’         Castilla-La-Mancha,
‘CV’          Valencia,
‘EXT’         Extremadura,
‘G  ’         Galicia,
‘IB ’         Baleares,
‘IC ’         Canarias,
‘LR ’         La Rioja,
‘M  ’         Madrid,
‘MU ’         Murcia,
‘NA ’         Navarra,
‘PV ’         País Vasco
```

Generacja 2:

Kody RegionAlpha znajdują się na wykazie utrzymywanym na stronie internetowej laboratorium wyznaczonego do przeprowadzenia badań interoperacyjności.

2.122. **RegionNumeric**

Numeryczne odniesienie do regionu w określonym państwie.

```
RegionNumeric ::= OCTET STRING (SIZE(1))
```

Generacja 1:

Przypisanie wartości:

```
‘00’H         No information available,
Spain:
‘01’H         Andalucía,
‘02’H         Aragón,
‘03’H         Asturias,
‘04’H         Cantabria,
‘05’H         Cataluña,
‘06’H         Castilla-León,
‘07’H         Castilla-La-Mancha,
‘08’H         Valencia,
‘09’H         Extremadura,
‘0A’H         Galicia,
‘0B’H         Baleares,
‘0C’H         Canarias,
‘0D’H         La Rioja,
‘0E’H         Madrid,
‘0F’H         Murcia,
‘10’H         Navarra,
‘11’H         País Vasco
```

Generacja 2:

Kody RegionNumeric znajdują się na wykazie utrzymywanym na stronie internetowej laboratorium wyznaczonego do przeprowadzenia badań interoperacyjności.

2.123. **RemoteCommunicationModuleSerialNumber**

Generacja 2:

Numer seryjny modułu komunikacji na odległość.

```
RemoteCommunicationModuleSerialNumber ::= ExtendedSerialNumber
```

2.124. **RSAKeyModulus**

Generacja 1:

Moduł pary kluczy RSA.

```
RSAKeyModulus ::= OCTET STRING (SIZE(128))
```

Przypisanie wartości: nieokreślona.

2.125. **RSAKeyPrivateExponent**

Generacja 1:

Wykładnik prywatny pary kluczy RSA.

```
RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))
```

Przypisanie wartości: nieokreślona.

2.126. **RSAKeyPublicExponent**

Generacja1:

Wykładnik publiczny pary kluczy RSA.

```
RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))
```

Przypisanie wartości: nieokreślona.

2.127. **RtmData**

Generacja2:

Definicja tego typu danych znajduje się w dodatku 14.

2.128. **SealDataCard**

Generacja 2:

W tym typie danych przechowuje się informacje o plombach przymocowanych do różnych części pojazdu i jest on przeznaczony do przechowywania na karcie. Ten typ danych związany jest z wymaganiem 337 określonym w załączniku 1C.

```
SealDataCard ::= SEQUENCE {
   noOfSealRecords                     INTEGER(1..5),
   sealRecords                         SET SIZE(noOfSealRecords) OF SealRecord
}
```

noOfSealRecords jest liczbą rekordów w zbiorze sealRecords.

sealRecords jest zbiorem rekordów dotyczących plomb.

2.129. **SealDataVu**

Generacja 2:

W tym typie danych przechowuje się informacje o plombach przymocowanych do różnych części pojazdu i jest on przeznaczony do przechowywania w przyrządzie rejestrującym.

```
SealDataVu ::= SEQUENCE SIZE(5) OF {
   sealRecords                         SealRecord
}
```

sealRecords jest zbiorem rekordów dotyczących plomb. W przypadku gdy dostępnych jest mniej niż 5 plomb wartość EquipmentType we wszystkich niewykorzystanych sealRecords należy ustawić na 16, tj. niewykorzystane.

2.130. **SealRecord**

Generacja 2:

W tym typie danych przechowuje się informacje o plombie przymocowanej do danego elementu składowego. Ten typ danych związany jest z wymaganiem 337 określonym w załączniku 1C.

```
SealRecord ::= SEQUENCE {
   equipmentType                       EquipmentType,
   extendedSealIdentifier              ExtendedSealIdentifier
}
```

equipmentType określa typ urządzenia, do którego jest przymocowana plomba.

extendedSealIdentifier jest identyfikatorem plomby przymocowanej do urządzenia.

2.131. **SensorApprovalNumber**

Numer homologacji typu czujnika.

Generacja 1:

```
SensorApprovalNumber ::= IA5String(SIZE(8))
```

Przypisanie wartości: nieokreślona.

Generacja 2:

```
SensorApprovalNumber ::= IA5String(SIZE(16))
```

Przypisanie wartości:

Należy podawać numer homologacji, który został opublikowany na odpowiedniej stronie internetowej Komisji Europejskiej, tj. na przykład z uwzględnieniem myślników, jeżeli występują. Numer homologacji musi być wyrównany do lewej strony.

2.132. **SensorExternalGNSSApprovalNumber**

Generacja 2:

Numer homologacji urządzenia zewnętrznego GNSS.

```
SensorExternalGNSSApprovalNumber ::= IA5String(SIZE(16))
```

Przypisanie wartości:

Należy podawać numer homologacji, który został opublikowany na odpowiedniej stronie internetowej Komisji Europejskiej, tj. na przykład z uwzględnieniem myślników, jeżeli występują. Numer homologacji musi być wyrównany do lewej strony.

2.133. **SensorExternalGNSSCoupledRecord**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące identyfikacji urządzenia zewnętrznego GNSS powiązanego z przyrządem rejestrującym (wymaganie 100 określone w załączniku 1C).

```
SensorExternalGNSSCoupledRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorCouplingDate                  SensorGNSSCouplingDate
}
```

sensorSerialNumber jest numerem seryjnym urządzenia zewnętrznego GNSS powiązanego z przyrządem rejestrującym.

sensorApprovalNumber jest numerem homologacji tego urządzenia zewnętrznego GNSS.

sensorCouplingDate jest datą powiązania tego urządzenia zewnętrznego GNSS z przyrządem rejestrującym.

2.134. **SensorExternalGNSSIdentification**

Generacja 2:

Informacje dotyczące identyfikacji urządzenia zewnętrznego GNSS (wymaganie 98 określone w załączniku 1C).

```
SensorExternalGNSSIdentification ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorSCIdentifier                  SensorExternalGNSSSCIdentifier,
   sensorOSIdentifier                  SensorExternalGNSSOSIdentifier
}
```

sensorSerialNumber jest rozszerzonym numerem seryjnym urządzenia zewnętrznego GNSS.

sensorApprovalNumber jest numerem homologacji urządzenia zewnętrznego GNSS.

sensorSCIdentifier jest identyfikatorem elementu zabezpieczenia urządzenia zewnętrznego GNSS.

sensorOSIdentifier jest identyfikatorem systemu operacyjnego urządzenia zewnętrznego GNSS.

2.135. **SensorExternalGNSSInstallation**

Generacja 2:

Informacje, przechowywane w urządzeniu zewnętrznym GNSS, dotyczące instalacji urządzenia zewnętrznego GNSS (wymaganie 123 określone w załączniku 1C).

```
SensorExternalGNSSInstallation ::= SEQUENCE {
   sensorCouplingDateFirst              SensorGNSSCouplingDate,
   firstVuApprovalNumber                VuApprovalNumber,
   firstVuSerialNumber                  VuSerialNumber,
   sensorCouplingDateCurrent            SensorGNSSCouplingDate,
   currentVuApprovalNumber              VuApprovalNumber,
   currentVUSerialNumber                VuSerialNumber
}
```

sensorCouplingDateFirst jest datą pierwszego powiązania urządzenia zewnętrznego GNSS z przyrządem rejestrującym.

firstVuApprovalNumber jest numerem homologacji pierwszego przyrządu rejestrującego powiązanego z urządzeniem zewnętrznym GNSS.

firstVuSerialNumber jest numerem seryjnym pierwszego przyrządu rejestrującego sparowanego z urządzeniem zewnętrznym GNSS.

sensorCouplingDateCurrent jest datą obecnego powiązania urządzenia zewnętrznego GNSS z przyrządem rejestrującym.

currentVuApprovalNumber jest numerem homologacji przyrządu rejestrującego powiązanego obecnie z urządzeniem zewnętrznym GNSS.

currentVUSerialNumber jest numerem seryjnym przyrządu rejestrującego powiązanego obecnie z urządzeniem zewnętrznym GNSS.

2.136. **SensorExternalGNSSOSIdentifier**

Generacja 2:

Identyfikator systemu operacyjnego urządzenia zewnętrznego GNSS.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Przypisanie wartości: swoisty dla producenta.

2.137. **SensorExternalGNSSSCIdentifier**

Generacja 2:

Ten typ jest stosowany np. w celu zidentyfikowania kryptograficznego modułu urządzenia zewnętrznego GNSS.

Identyfikator elementu zabezpieczenia urządzenia zewnętrznego GNSS.

```
SensorExternalGNSSSCIdentifier ::= IA5String(SIZE(8))
```

Przypisanie wartości: element swoisty dla producenta.

2.138. **SensorGNSSCouplingDate**

Generacja 2:

Data powiązania urządzenia zewnętrznego GNSS z przyrządem rejestrującym.

```
SensorGNSSCouplingDate ::= TimeReal
```

Przypisanie wartości: nieokreślona.

2.139. **SensorGNSSSerialNumber**

Generacja 2:

Ten typ jest wykorzystywany do przechowywania numeru seryjnego odbiornika GNSS, zarówno gdy jest w VU, jak i gdy znajduje się poza VU.

Numer seryjny odbiornika GNSS.

```
SensorGNSSSerialNumber ::= ExtendedSerialNumber
```

2.140. **SensorIdentification**

Informacje przechowywane w czujniku ruchu dotyczące jego identyfikacji (wymaganie 077 określone w załączniku 1B i wymaganie 95 określone w załączniku 1C).

```
SensorIdentification ::= SEQUENCE {
   sensorSerialNumber                  SensorSerialNumber,
   sensorApprovalNumber                SensorApprovalNumber,
   sensorSCIdentifier                  SensorSCIdentifier,
   sensorOSIdentifier                  SensorOSIdentifier
}
```

sensorSerialNumber jest rozszerzonym numerem seryjnym czujnika ruchu (zawiera numer części i kod producenta).

sensorApprovalNumber jest numerem homologacji czujnika ruchu.

sensorSCIdentifier jest identyfikatorem elementu zabezpieczenia czujnika ruchu.

sensorOSIdentifier jest identyfikatorem systemu operacyjnego czujnika ruchu.

2.141. **SensorInstallation**

Informacje przechowywane w czujniku ruchu dotyczące jego instalacji (wymaganie 099 określone w załączniku 1B i wymaganie 122 określone w załączniku 1C).

```
SensorInstallation ::= SEQUENCE {
   sensorPairingDateFirst              SensorPairingDate,
   firstVuApprovalNumber               VuApprovalNumber,
   firstVuSerialNumber                 VuSerialNumber,
   sensorPairingDateCurrent            SensorPairingDate,
   currentVuApprovalNumber             VuApprovalNumber,
   currentVUSerialNumber               VuSerialNumber
}
```

sensorPairingDateFirst jest datą pierwszego sparowania czujnika ruchu z przyrządem rejestrującym.

firstVuApprovalNumber jest numerem homologacji pierwszego przyrządu rejestrującego sparowanego z czujnikiem ruchu.

firstVuSerialNumber jest numerem seryjnym pierwszego przyrządu rejestrującego sparowanego z czujnikiem ruchu.

sensorPairingDateCurrent jest datą obecnego sparowania czujnika ruchu z przyrządem rejestrującym.

currentVuApprovalNumber jest numerem homologacji przyrządu rejestrującego obecnie sparowanego z czujnikiem ruchu.

currentVUSerialNumber jest numerem seryjnym przyrządu rejestrującego obecnie sparowanego z czujnikiem ruchu.

2.142. **SensorInstallationSecData**

Informacje przechowywane na karcie warsztatowej dotyczące zabezpieczenia potrzebne do sparowania czujników ruchu z przyrządami rejestrującymi (wymaganie 308 i 331 określone w załączniku 1C).

Generacja 1:

```
SensorInstallationSecData ::= TdesSessionKey
```

Przypisanie wartości: zgodnie z normą ISO 16844-3.

Generacja 2:

Zgodnie z opisem w dodatku 11 karta warsztatowa musi przechowywać maksymalnie trzy klucze na potrzeby parowania czujnika ruchu z VU. Klucze te mają różne wersje.

```
SensorInstallationSecData ::= SEQUENCE {
   kMWCKey1                          KMWCKey,
   kMWCKey2                          KMWCKey OPTIONAL,
   kMWCKey3                          KMWCKey OPTIONAL
}
```

2.143. **SensorOSIdentifier**

Identyfikator systemu operacyjnego czujnika ruchu.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Przypisanie wartości: swoisty dla producenta.

2.144. **SensorPaired**

Generacja 1:

Informacje przechowywane w przyrządzie rejestrującym dotyczące identyfikacji czujnika ruchu sparowanego z przyrządem rejestrującym (wymaganie 079 określone w załączniku 1B).

```
SensorPaired ::= SEQUENCE {
   sensorSerialNumber                SensorSerialNumber,
   sensorApprovalNumber              SensorApprovalNumber,
   sensorPairingDateFirst            SensorPairingDate
}
```

sensorSerialNumber jest numerem seryjnym czujnika ruchu obecnie sparowanego z przyrządem rejestrującym.

sensorApprovalNumber jest numerem homologacji czujnika ruchu obecnie sparowanego z przyrządem rejestrującym.

sensorPairingDateFirst jest datą pierwszego sparowania z przyrządem rejestrującym czujnika ruchu obecnie sparowanego z przyrządem rejestrującym.

2.145. **SensorPairedRecord**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące identyfikacji czujnika ruchu sparowanego z przyrządem rejestrującym (wymaganie 97 określone w załączniku 1C).

```
SensorPairedRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorSerialNumber,
   sensorApprovalNumber                SensorApprovalNumber,
   sensorPairingDate                   SensorPairingDate
}
```

sensorSerialNumber jest numerem seryjnym czujnika ruchu sparowanego z przyrządem rejestrującym.

sensorApprovalNumber jest numerem homologacji tego czujnika ruchu.

sensorPairingDate jest datą sparowania tego czujnika ruchu z przyrządem rejestrującym.

2.146. **SensorPairingDate**

Data sparowania czujnika ruchu z przyrządem rejestrującym.

```
SensorPairingDate ::= TimeReal
```

Przypisanie wartości: nieokreślona.

2.147. **SensorSCIdentifier**

Identyfikator elementu zabezpieczenia czujnika ruchu.

```
SensorSCIdentifier ::= IA5String(SIZE(8))
```

Przypisanie wartości: element swoisty dla producenta.

2.148. **SensorSerialNumber**

Numer seryjny czujnika ruchu.

```
SensorSerialNumber ::= ExtendedSerialNumber
```

2.149. **Podpis**

Podpis cyfrowy.

Generacja 1:

```
Signature ::= OCTET STRING (SIZE(128))
```

Przypisanie wartości: zgodnie z dodatkiem 11 – Wspólne mechanizmy zabezpieczenia.

Generacja 2:

```
Signature ::= OCTET STRING (SIZE(64..132))
```

Przypisanie wartości: zgodnie z dodatkiem 11 – Wspólne mechanizmy zabezpieczenia.

2.150. **SignatureRecordArray**

Generacja 2:

Zbiór podpisów wraz z metadanymi stosowany w protokole pobierania danych.

```
SignatureRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF Signature
}
```

recordType oznacza typ rekordu (Signature). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość Signature w bajtach.

noOfRecords jest liczbą rekordów w zbiorze. Wartość tę należy ustawić na 1, ponieważ podpisy mogą mieć różne długości.

records jest zbiorem podpisów.

2.151. **SimilarEventsNumber**

Liczba podobnych zdarzeń w danym dniu (wymaganie 094 określone w załączniku 1B i wymaganie 117 określone w załączniku 1C).

```
SimilarEventsNumber ::= INTEGER(0..255)
```

Przypisanie wartości: 0 nie używany, 1 oznacza, że tylko jedno zdarzenie tego typu wystąpiło i jest zapamiętane dla tego dnia, 2 oznacza, że 2 zdarzenia wystąpiły w tym dniu (zapamiętane jest tylko jedno),... 255 oznacza, że 255 lub więcej zdarzeń wystąpiło w tym dniu.

2.152. **SpecificConditionRecord**

Informacje przechowywane na karcie kierowcy, karcie warsztatowej lub w przyrządzie rejestrującym dotyczące warunku szczególnego (wymagania 130, 276, 301, 328 i 355 określone w załączniku 1C).

```
SpecificConditionRecord ::= SEQUENCE {
   entryTime                           TimeReal,
   specificConditionType               SpecificConditionType
}
```

entryTime jest datą i godziną wprowadzenia danych.

specificConditionType jest kodem identyfikującym warunek szczególny.

2.153. **SpecificConditions**

Informacje przechowywane na karcie kierowcy, karcie warsztatowej lub w przyrządzie rejestrującym dotyczące warunku szczególnego (wymagania 131, 277, 302, 329 i 356 określone w załączniku 1C).

Generacja 2:

```
SpecificConditions := SEQUENCE {
   conditionPointerNewestRecord        INTEGER(0..NoOfSpecificConditionRecords-1),
   specificConditionRecords            SET SIZE(NoOfSpecificConditionRecords) OF
                                       SpecificConditionRecord
}
```

conditionPointerNewestRecord jest indeksem ostatniego, uaktualnionego rekordu warunku szczególnego.

Przypisanie wartości: liczba odpowiadająca stanowi licznika rekordu dotyczącego warunku szczególnego, rozpoczynając od „0" dla pierwszego wystąpienia w strukturze rekordu dotyczącego warunku szczególnego.

specificConditionRecords jest zbiorem rekordów zawierających informacje o zarejestrowanych warunkach szczególnych.

2.154. **SpecificConditionType**

Kod identyfikujący warunek szczególny (wymagania 050b, 105a, 212a i 230a określone w załączniku 1B oraz wymaganie 62 określone w załączniku 1C).

```
SpecificConditionType ::= INTEGER(0..255)
```

Generacja 1:

Przypisanie wartości:

'00'H	RFU
'01'H	poza zakresem — początek
'02'H	poza zakresem — koniec
'03'H	Przeprawa promowa/przejazd kolejowy
'04'H .. 'FF'H	RFU

Generacja 2:

Przypisanie wartości:

'00'H	RFU
'01'H	poza zakresem — początek
'02'H	poza zakresem — koniec
'03'H	Przeprawa promowa/przejazd kolejowy – początek
'04'H	Przeprawa promowa/przejazd kolejowy – koniec
'05'H .. 'FF'H	RFU

2.155. **Prędkość**

Prędkość pojazdu (km/h).

```
Speed ::= INTEGER(0..255)
```

Przypisanie wartości: kilometry na godzinę w zakresie operacyjnym 0 do 220 km/h.

2.156. **SpeedAuthorised**

Maksymalne dozwolone prędkości pojazdu (definicja hh)).

```
SpeedAuthorised ::= Speed
```

2.157. **SpeedAverage**

Prędkość średnia w uprzednio zdefiniowanym przedziale czasu (km/h).

```
SpeedAverage ::= Speed
```

2.158. **SpeedMax**

Prędkość maksymalna zmierzona w uprzednio zdefiniowanym przedziale czasu.

```
SpeedMax ::= Speed
```

2.159. **TachographPayload**

Generacja 2:

Definicja tego typu danych znajduje się w dodatku 14.

2.160. **TachographPayloadEncrypted**

Generacja 2:

Ładunek tachografu zaszyfrowany w formacie DER-TLV, tj. dane przesłane w formie zaszyfrowanego komunikatu RTM. Odnośnie do kodowania zob. rozdział 13 dodatek 11 część B.

```
TachographPayloadEncrypted ::= SEQUENCE {
   tag                                  OCTET STRING(SIZE(1)),
   length                               OCTET STRING(SIZE(1..2)),
   paddingContentIndicatorByte          OCTET STRING(SIZE(1)),
   encryptedData                        OCTET STRING(SIZE(16..192))
}
```

tag jest częścią kodowania w formacie DER-TLV ma przypisaną wartość „87” (zob. dodatek 11 część B rozdział 13).

length jest częścią kodowania w formacie DER-TLV i koduje długość następujących paddingContentIndicatorByte i encryptedData.

paddingContentIndicatorByte musi mieć przypisaną wartość „00”.

encryptedData jest zaszyfrowanym tachographPayload, określonym w dodatku 11 część B rozdział 13. Długość tych danych w oktetach musi być zawsze wielokrotnością liczby 16.

2.161. **TDesSessionKey**

Generacja 1:

Klucz sesyjny T-DES.

```
TDesSessionKey ::= SEQUENCE {
   tDesKeyA                             OCTET STRING (SIZE(8)),
   tDesKeyB                             OCTET STRING (SIZE(8))
}
```

Przypisanie wartości: nie określa się.

2.162. **TimeReal**

Kod w polu zawierającym łącznie datę i godzinę, gdzie data i godzina są wyrażone w sekundach liczonych od godziny 00h.00m.00s. w dniu 1 stycznia 1970 r. GMT.

```
TimeReal{INTEGER:TimeRealRange} ::= INTEGER(0..TimeRealRange)
```

Przypisanie wartości – zapisane oktetami: liczba sekund od północy 1 stycznia 1970 r. GMT.

Maksymalna możliwa data/godzina wypada w 2106 r.

2.163. **TyreSize**

Oznaczenie wymiarów opon.

```
TyreSize ::= IA5String(SIZE(15))
```

Przypisanie wartości: zgodnie z dyrektywą 92/23 (EWG) z dnia 31 marca 1992, Dz.U. L 129 s. 95.

2.164. **VehicleIdentificationNumber**

Numer identyfikacyjny pojazdu (VIN) odnoszący się do pojazdu jako całości, normalnie numer seryjny nadwozia lub ramy.

```
VehicleIdentificationNumber ::= IA5String(SIZE(17))
```

Przypisanie wartości: jak określono w normie ISO 3779.

2.165. **VehicleIdentificationNumberRecordArray**

Generacja 2:

Numer identyfikacyjny pojazdu wraz z metadanymi stosowany w protokole pobierania danych.

```
VehicleIdentificationNumberRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VehicleIdentificationNumber
}
```

recordType oznacza typ rekordu (VehicleIdentificationNumber). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość VehicleIdentificationNumber w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem numerów identyfikacyjnych pojazdu.

2.166. **VehicleRegistrationIdentification**

Identyfikacja pojazdu, unikalna dla Europy (VRN i państwo członkowskie).

```
VehicleRegistrationIdentification ::= SEQUENCE {
   vehicleRegistrationNation           NationNumeric,
   vehicleRegistrationNumber           VehicleRegistrationNumber
}
```

vehicleRegistrationNation jest państwem, w którym pojazd jest zarejestrowany.

vehicleRegistrationNumber jest numerem rejestracyjnym pojazdu (VRN).

2.167. **VehicleRegistrationNumber**

Numer rejestracyjny pojazdu (VRN). Numer rejestracyjny przydziela organ rejestracji pojazdów.

```
VehicleRegistrationNumber ::= SEQUENCE {
   codePage                            INTEGER (0..255),
   vehicleRegNumber                    OCTET STRING (SIZE(13))
}
```

codePage określa zestaw znaków zdefiniowany w rozdziale 4,

vehicleRegNumber jest numerem VRN zakodowanym przy użyciu wyszczególnionego zestawu znaków.

Przypisanie wartości: swoisty dla kraju.

2.168. **VehicleRegistrationNumberRecordArray**

Generacja 2:

Numer rejestracyjny pojazdu wraz z metadanymi stosowany w protokole pobierania danych.

```
VehicleRegistrationNumberRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VehicleRegistrationNumber
}
```

recordType oznacza typ rekordu (VehicleRegistrationNumber). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość VehicleRegistrationNumber w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem numerów rejestracyjnych pojazdu.

2.169. **VuAbility**

Generacja 2:

Informacje przechowywane w VU dotyczące możliwości stosowania kart do tachografów generacji 1 (wymaganie 121 określone w załączniku 1C).

```
VuAbility ::= OCTET STRING (SIZE(1))
```

Przypisanie wartości – zapisane oktetami: 'xxxxxxxa'B (8 bitów)

Odnośnie do zdolności do obsługi generacji 1:

'a'B	Zdolność do obsługi kart do tachografów generacji 1:
	'0' B generacja 1 jest obsługiwana,
	'1' B generacja 1 nie jest obsługiwana,
'xxxxxxx'B	RFU

2.170. **VuActivityDailyData**

Generacja 1:

Informacje przechowywane w VU dotyczące zmian czynności lub zmian stanu prowadzenia pojazdu lub zmian stanu karty dla określonego dnia kalendarzowego (wymaganie 084 określone w załączniku 1B i wymagania 105, 106, 107 określone w załączniku 1C) i stanu czytników o godzinie 00:00 tego dnia.

```
VuActivityDailyData ::= SEQUENCE {
   noOfActivityChanges                  INTEGER SIZE(0..1440),
   activityChangeInfos                  SET SIZE(noOfActivityChanges) OF
                                        ActivityChangeInfo
}
```

noOfActivityChanges jest liczbą słów ActivityChangeInfo w zbiorze activityChangeInfos.

activityChangeInfos jest zbiorem słów ActivityChangeInfo przechowywanych w VU dla danego dnia. Zawsze zawiera dwa słowa ActivityChangeInfo opisujące stan dwóch czytników o godzinie 00:00 tego dnia.

2.171. **VuActivityDailyRecordArray**

Generacja 2:

Informacje przechowywane w VU dotyczące zmian czynności lub zmian stanu prowadzenia pojazdu lub zmian stanu karty dla określonego dnia kalendarzowego (wymaganie 105, 106, 107 określone w załączniku 1C) i stanu szczelin o godzinie 00:00 tego dnia.

```
VuActivityDailyRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF ActivityChangeInfo
}
```

recordType oznacza typ rekordu (ActivityChangeInfo). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość ActivityChangeInfo w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem słów ActivityChangeInfo przechowywanych w VU dla danego dnia. Zawsze zawiera dwa słowa ActivityChangeInfo opisujące stan dwóch czytników o godzinie 00:00 tego dnia.

2.172. **VuApprovalNumber**

Numer homologacji typu przyrządu rejestrującego.

Generacja 1:

```
VuApprovalNumber ::= IA5String(SIZE(8))
```

Przypisanie wartości: nieokreślona.

Generacja 2:

```
VuApprovalNumber ::= IA5String(SIZE(16))
```

Przypisanie wartości:

Należy podawać numer homologacji, który został opublikowany na odpowiedniej stronie internetowej Komisji Europejskiej, tj. na przykład z uwzględnieniem myślników, jeżeli występują. Numer homologacji musi być wyrównany do lewej strony.

2.173. **VuCalibrationData**

Generacja 1:

Informacje przechowywane w przyrządzie rejestrującym dotyczące kalibracji urządzenia rejestrującego (wymaganie 098 określone w załączniku 1B).

```
VuCalibrationData ::= SEQUENCE {
   noOfVuCalibrationRecords            INTEGER(0..255),
   vuCalibrationRecords                SET SIZE(noOfVuCalibrationRecords) OF
                                       VuCalibrationRecord
}
```

noOfVuCalibrationRecords jest liczbą rekordów w zbiorze vuCalibrationRecords.

vuCalibrationRecords jest zbiorem rekordów kalibracyjnych.

2.174. **VuCalibrationRecord**

Informacje przechowywane w przyrządzie rejestrującym dotyczące kalibracji urządzenia rejestrującego (wymaganie 098 określone w załączniku 1B i wymaganie 119 i 120 określone w załączniku 1C).

Generacja 1:

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                  CalibrationPurpose,
   workshopName                        Name,
   workshopAddress                     Address,
   workshopCardNumber                  FullCardNumber,
   workshopCardExpiryDate              TimeReal,
   vehicleIdentificationNumber         VehicleIdentificationNumber,
   vehicleRegistrationIdentification   VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant      W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment       K-ConstantOfRecordingEquipment,
   lTyreCircumference                  L-TyreCircumference,
   tyreSize                            TyreSize,
   authorisedSpeed                     SpeedAuthorised,
   oldOdometerValue                    OdometerShort,
   newOdometerValue                    OdometerShort,
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal,
   nextCalibrationDate                 TimeReal
}
```

calibrationPurpose jest celem kalibracji.

workshopName, workshopAddress są nazwą i adresem warsztatu.

workshopCardNumber identyfikuje kartę warsztatową używaną przy kalibracji.

workshopCardExpiryDate jest terminem ważności karty.

vehicleIdentificationNumber jest numerem VIN.

vehicleRegistrationIdentification zawiera numer VRN i państwa członkowskiego rejestracji.

wVehicleCharacteristicConstant jest współczynnikiem charakterystycznym pojazdu.

kConstantOfRecordingEquipment jest stałą urządzenia rejestrującego.

lTyreCircumference jest obwodem tocznym kół.

tyreSize jest oznaczeniem rozmiaru opon zamontowanych w pojeździe.

authorisedSpeed jest dozwoloną prędkością pojazdu.

oldOdometerValue, newOdometerValue są starym i nowym stanem licznika kilometrów.

oldTimeValue, newTimeValue są starą i nową wartością daty i godziny.

nextCalibrationDate jest datą następnej kalibracji typu określonego w CalibrationPurpose, którą powinien przeprowadzić autoryzowany organ kontrolny.

Generacja 2:

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                    CalibrationPurpose,
   workshopName                          Name,
   workshopAddress                       Address,
   workshopCardNumber                    FullCardNumber,
   workshopCardExpiryDate                TimeReal,
   vehicleIdentificationNumber           VehicleIdentificationNumber,
   vehicleRegistrationIdentification     VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant        W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment         K-ConstantOfRecordingEquipment,
   lTyreCircumference                    L-TyreCircumference,
   tyreSize                              TyreSize,
   authorisedSpeed                       SpeedAuthorised,
   oldOdometerValue                      OdometerShort,
   newOdometerValue                      OdometerShort,
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   nextCalibrationDate                   TimeReal,
   sealDataVu                            SealDataVu
}
```

Oprócz generacji 1 używany jest następujący element danych:

sealDataVu podaje informacje o plombach przymocowanych do różnych części pojazdu.

2.175. **VuCalibrationRecordArray**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące kalibracji urządzenia rejestrującego (wymagania 119 i 120 określone w załączniku 1C).

```
VuCalibrationRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuCalibrationRecord
}
```

recordType oznacza typ rekordu (VuCalibrationRecord). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość VuCalibrationRecord w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem rekordów kalibracji.

2.176. **VuCardIWData**

Generacja 1:

Informacje przechowywane w przyrządzie rejestrującym dotyczące cykli wkładania i wyjmowania kart dla kart kierowcy lub kart warsztatowych w przyrządzie rejestrującym (wymaganie 081 określone w załączniku 1B i wymaganie 103 określone w załączniku 1C).

```
VuCardIWData ::= SEQUENCE {
   noOfIWRecords                       INTEGER(0..2^16-1),
   vuCardIWRecords                     SET SIZE(noOfIWRecords) OF VuCardIWRecord
}
```

noOfIWRecords jest liczbą rekordów w zbiorze vuCardIWRecords.

vuCardIWRecords jest zbiorem rekordów dotyczących cykli wkładania i wyjmowania kart.

2.177. **VuCardIWRecord**

Informacje przechowywane w przyrządzie rejestrującym dotyczące cyklu wkładania i wyjmowania karty kierowcy lub karty warsztatowej w przyrządzie rejestrującym (wymaganie 081 określone w załączniku 1B i wymaganie 102 określone w załączniku 1C).

Generacja 1:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                      HolderName,
   fullCardNumber                      FullCardNumber,
   cardExpiryDate                      TimeReal,
   cardInsertionTime                   TimeReal,
   vehicleOdometerValueAtInsertion     OdometerShort,
   cardSlotNumber                      CardSlotNumber,
   cardWithdrawalTime                  TimeReal,
   vehicleOdometerValueAtWithdrawal    OdometerShort,
   previousVehicleInfo                 PreviousVehicleInfo,
   manualInputFlag                     ManualInputFlag
}
```

cardHolderName jest nazwiskiem i imionami posiadacza karty kierowcy lub karty warsztatowej zapisanymi na karcie.

fullCardNumber jest typem karty, państwem członkowskim wydającym kartę i numerem karty zapisanymi na karcie.

cardExpiryDate jest terminem ważności karty zapisanym na karcie.

cardInsertionTime jest datą i godziną włożenia karty.

vehicleOdometerValueAtInsertion jest stanem licznika kilometrów przy wkładaniu karty.

cardSlotNumber jest szczeliną czytnika, do której karta jest włożona.

cardWithdrawalTime jest datą i godziną wyjęcia karty.

vehicleOdometerValueAtWithdrawal jest stanem licznika kilometrów przy wyjęciu karty.

previousVehicleInfo zawiera informacje o pojeździe poprzednio używanym przez kierowcę, zapisane na karcie.

manualInputFlag jest flagą pokazującą, czy posiadacz karty przy wkładaniu karty wprowadził ręcznie czynności kierowcy.

Generacja 2:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                       HolderName,
   fullCardNumberAndGeneration          FullCardNumberAndGeneration,
   cardExpiryDate                       TimeReal,
   cardInsertionTime                    TimeReal,
   vehicleOdometerValueAtInsertion      OdometerShort,
   cardSlotNumber                       CardSlotNumber,
   cardWithdrawalTime                   TimeReal,
   vehicleOdometerValueAtWithdrawal     OdometerShort,
   previousVehicleInfo                  PreviousVehicleInfo,
   manualInputFlag                      ManualInputFlag
}
```

Zamiast fullCardNumber w strukturze danych generacji 2 wykorzystuje się następujący element danych.

fullCardNumberAndGeneration jest typem karty, państwem członkowskim wydającym kartę, numerem karty i generacją zapisanymi na karcie.

2.178. **VuCardIWRecordArray**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące cykli wkładania i wyjmowania kart kierowcy lub kart warsztatowych w przyrządzie rejestrującym (wymaganie 103 określone w załączniku 1C).

```
VuCardIWRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF VuCardIWRecord
}
```

recordType oznacza typ rekordu (VuCardIWRecord). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość VuCardIWRecord w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem rekordów dotyczących cykli wkładania i wyjmowania kart.

2.179. **VuCardRecord**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące używanej karty do tachografu (wymaganie 132 określone w załączniku 1C).

```
VuCardRecord ::= SEQUENCE {
   cardExtendedSerialNumber            ExtendedSerialNumber,
   cardPersonaliserID                  OCTET STRING(SIZE(1)),
   typeofTachographCardID              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   cardNumber                          CardNumber
}
```

cardExtendedSerialNumber odczytany z pliku EF_ICC w ramach pliku głównego karty.

cardPersonaliserIDodczytane z pliku EF_ICC w ramach pliku głównego karty.

typeOfTachographCardId odczytane z pliku EF_Application_Identification w ramach pliku DF_Tachograph_G2

cardStructureVersion odczytane z pliku EF_Application_Identification w ramach pliku DF_Tachograph_G2

cardNumber odczytane z pliku EF_Identification w ramach pliku DF_Tachograph_G2

2.180. **VuCardRecordArray**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące kart do tachografów używanych w tym VU. Informacje te są przeznaczone do analizy przez VU problemów dotyczących kart (wymaganie 132 określone w załączniku 1C).

```
VuCardRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCardRecord
}
```

recordType oznacza typ rekordu (VuCardRecord). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość VuCardRecord w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem rekordów dotyczących kart do tachografów używanych w VU.

2.181. **VuCertificate**

Certyfikat klucza publicznego przyrządu rejestrującego.

```
VuCertificate ::= Certificate
```

2.182. **VuCertificateRecordArray**

Generacja 2:

Certyfikat VU wraz z metadanymi stosowany w protokole pobierania danych.

```
VuCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCertificate
}
```

recordType oznacza typ rekordu (VuCertificate). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość VuCertificate w bajtach.

noOfRecords jest liczbą rekordów w zbiorze. Wartość tę należy ustawić na 1, ponieważ certyfikaty mogą mieć różne długości.

records jest zbiorem certyfikatów VU.

2.183. **VuCompanyLocksData**

Generacja 1:

Informacje przechowywane w przyrządzie rejestrującym dotyczące blokad firmowych (wymaganie 104 określone w załączniku 1B).

```
VuCompanyLocksData ::= SEQUENCE {
   noOfLocks                          INTEGER(0..255),
   vuCompanyLocksRecords              SET SIZE(noOfLocks) OF VuCompanyLocksRecord
}
```

noOfLocks jest liczbą blokad wyszczególnionych w vuCompanyLocksRecords.

vuCompanyLocksRecords jest zbiorem rekordów blokad firmowych.

2.184. **VuCompanyLocksRecord**

Informacje przechowywane w przyrządzie rejestrującym dotyczące jednej blokady (wymaganie 104 określone w załączniku 1B i wymaganie 128 określone w załączniku 1C).

Generacja 1:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                         TimeReal,
   lockOutTime                        TimeReal,
   companyName                        Name,
   companyAddress                     Address,
   companyCardNumber                  FullCardNumber
}
```

lockInTime, lockOutTime są datą i godziną założenia i zdjęcia blokady.

companyName, companyAddress są nazwą i adresem firmy związanej z założeniem blokady.

companyCardNumber identyfikuje kartę użytą przy założeniu blokady.

Generacja 2:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                         TimeReal,
   lockOutTime                        TimeReal,
   companyName                        Name,
   companyAddress                     Address,
   companyCardNumberAndGeneration     FullCardNumberAndGeneration
}
```

Zamiast companyCardNumber w strukturze danych generacji 2 wykorzystuje się następujący element danych.

companyCardNumberAndGeneration identyfikuje kartę, w tym jej generację, użytą przy założeniu blokady.

2.185. **VuCompanyLocksRecordArray**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące blokad firmowych (wymaganie 128 określone w załączniku 1C).

```
VuCompanyLocksRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuCompanyLocksRecord
}
```

recordType oznacza typ rekordu (VuCompanyLocksRecord). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość VuCompanyLocksRecord w bajtach.

noOfRecords jest liczbą rekordów w zbiorze. Wartość 0..255.

records jest zbiorem rekordów blokad firmowych.

2.186. **VuControlActivityData**

Generacja 1:

Informacje przechowywane w przyrządzie rejestrującym, dotyczące kontroli przeprowadzonych przy użyciu tego VU (wymaganie 102 określone w załączniku 1B).

```
VuControlActivityData ::= SEQUENCE {
   noOfControls                        INTEGER(0..20),
   vuControlActivityRecords            SET SIZE(noOfControls) OF
                                       VuControlActivityRecord
}
```

noOfControls jest liczbą kontroli wyszczególnionych w vuControlActivityRecords.

vuControlActivityRecords jest zbiorem rekordów czynności kontrolnych.

2.187. **VuControlActivityRecord**

Informacje przechowywane w przyrządzie rejestrującym dotyczące kontroli wykonanej przy użycie tego VU (wymaganie 102 określone w załączniku 1B i wymaganie 126 określone w załączniku 1C).

Generacja 1:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                         ControlType,
   controlTime                         TimeReal,
   controlCardNumber                   FullCardNumber,
   downloadPeriodBeginTime             TimeReal,
   downloadPeriodEndTime               TimeReal
}
```

controlType jest typem kontroli.

controlTime jest datą i godziną kontroli.

controlCardNumber identyfikuje kartę kontrolną użytą przy kontroli.

downloadPeriodBeginTime jest czasem rozpoczęcia okresu, dla którego pobrano dane, w przypadku pobierania danych.

downloadPeriodEndTime jest czasem zakończenia okresu, dla którego pobrano dane, w przypadku pobierania danych.

Generacja 2:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumberAndGeneration       FullCardNumberAndGeneration,
   downloadPeriodBeginTime              TimeReal,
   downloadPeriodEndTime                TimeReal
}
```

Zamiast controlCardNumber w strukturze danych generacji 2 wykorzystuje się następujący element danych.

controlCardNumberAndGeneration identyfikuje kartę kontrolną, w tym jej generację, użytą przy kontroli.

2.188. **VuControlActivityRecordArray**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym, dotyczące kontroli przeprowadzonych przy użyciu tego VU (wymaganie 126 określone w załączniku 1C).

```
VuControlActivityRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuControlActivityRecord
}
```

recordType oznacza typ rekordu (VuControlActivityRecord). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość VuControlActivityRecord w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem rekordów czynności kontrolnych VU.

2.189. **VuDataBlockCounter**

Licznik przechowywany na karcie pokazujący kolejno cykle wkładania/wyjmowania karty dla przyrządów rejestrujących.

```
VuDataBlockCounter ::= BCDString(SIZE(2))
```

Przypisanie wartości: kolejna liczba, po osiągnięciu wartości maksymalnej 9 999 liczenie rozpoczyna się ponownie od 0.

2.190. **VuDetailedSpeedBlock**

Informacje przechowywane w przyrządzie rejestrującym dotyczące szczegółowej prędkości pojazdu dla minuty, przez którą pojazd był w ruchu (wymaganie 093 określone w załączniku 1B i wymaganie 116 określone w załączniku 1C).

```
VuDetailedSpeedBlock ::= SEQUENCE {
   speedBlockBeginDate    TimeReal,
   speedsPerSecond        SEQUENCE SIZE(60) OF Speed
}
```

speedBlockBeginDate jest datą i godziną pierwszego odczytu prędkości w bloku.

speedsPerSecond jest chronologicznym ciągiem prędkości mierzonych co sekundę w ciągu minuty rozpoczynającej się od godziny określonej w speedBlockBeginDate (włącznie).

2.191. **VuDetailedSpeedBlockRecordArray**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące szczegółowej prędkości pojazdu.

```
VuDetailedSpeedBlockRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuDetailedSpeedBlock
}
```

recordType oznacza typ rekordu (VuDetailedSpeedBlock). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość VuDetailedSpeedBlock w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem bloków szczegółowej prędkości.

2.192. **VuDetailedSpeedData**

Generacja 1:

Informacje przechowywane w przyrządzie rejestrującym dotyczące szczegółowej prędkości pojazdu.

```
VuDetailedSpeedData ::= SEQUENCE {
   noOfSpeedBlocks                     INTEGER(0..2^16-1),
   vuDetailedSpeedBlocks               SET SIZE(noOfSpeedBlocks) OF
                                       VuDetailedSpeedBlock
}
```

noOfSpeedBlocks jest liczbą bloków zarejestrowanych prędkości w zbiorze vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks jest zbiorem bloków szczegółowej prędkości.

2.193. **VuDownloadablePeriod**

Najstarsza i najświeższa data i godzina, wyznaczające okres, dla którego przyrząd rejestrujący przechowuje dane dotyczące czynności kierowców (wymagania 081, 084 lub 087 określone w załączniku 1B i wymagania 102, 105, 108 określone w załączniku 1C).

```
VuDownloadablePeriod ::= SEQUENCE {
   minDownloadableTime                 TimeReal
   maxDownloadableTime                 TimeReal
}
```

minDownloadableTime jest przechowywaną w VU datą i godziną dawniejszego włożenia karty lub zmiany czynności lub miejsca wprowadzania danych.

maxDownloadableTime jest przechowywaną w VU datą i godziną ostatniego wyjęcia karty lub zmiany czynności, lub miejsca wprowadzania danych.

2.194. **VuDownloadablePeriodRecordArray**

Generacja 2:

VUDownloadablePeriod wraz z metadanymi stosowany w protokole pobierania danych.

```
VuDownloadablePeriodRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuDownloadablePeriod
}
```

recordType oznacza typ rekordu (VuDownloadablePeriod). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość VuDownloadablePeriod w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem rekordów VuDownloadablePeriod.

2.195. **VuDownloadActivityData**

Informacje przechowywane w przyrządzie rejestrującym dotyczące ostatniego pobrania danych (wymaganie 105 określone w załączniku 1B i wymaganie 129 określone w załączniku 1C).

Generacja 1:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                     TimeReal,
   fullCardNumber                      FullCardNumber,
   companyOrWorkshopName               Name
}
```

downloadingTime jest datą i godziną pobierania danych.

fullCardNumber identyfikuje kartę użytą do autoryzowania pobierania danych.

companyOrWorkshopName jest nazwą firmy lub warsztatu.

Generacja 2:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                     TimeReal,
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   companyOrWorkshopName               Name
}
```

Zamiast fullCardNumber w strukturze danych generacji 2 wykorzystuje się następujący element danych.

fullCardNumberAndGeneration identyfikuje kartę kontrolną, w tym jej generację, użytą do autoryzacji pobierania danych.

2.196. **VuDownloadActivityDataRecordArray**

Generacja 2:

Informacje dotyczące ostatniego pobrania danych z VU (wymaganie 129 określone w załączniku 1C).

```
VuDownloadActivityDataRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuDownloadActivityData
}
```

recordType oznacza typ rekordu (VuDownloadActivityData). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość VuDownloadActivityData w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem rekordów czynności pobierania danych.

2.197. **VuEventData**

Generacja 1:

Informacje przechowywane w przyrządzie rejestrującym, dotyczące zdarzeń (wymaganie 094 określone w załączniku 1B z wyłączeniem przekroczenia prędkości).

```
VuEventData ::= SEQUENCE {
   noOfVuEvents                          INTEGER(0..255),
   vuEventRecords                        SET SIZE(noOfVuEvents) OF VuEventRecord
}
```

noOfVuEvents jest liczbą zdarzeń wyszczególnionych w zbiorze vuEventRecords.

vuEventRecords jest zbiorem rekordów dotyczących zdarzeń.

2.198. **VuEventRecord**

Informacje przechowywane w przyrządzie rejestrującym, dotyczące zdarzenia (wymaganie 094 określone w załączniku 1B i wymaganie 117 określone w załączniku 1C z wyłączeniem przekroczenia prędkości).

Generacja 1:

```
VuEventRecord ::= SEQUENCE {
   eventType                             EventFaultType,
   eventRecordPurpose                    EventFaultRecordPurpose,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   cardNumberDriverSlotBegin             FullCardNumber,
   cardNumberCodriverSlotBegin           FullCardNumber,
   cardNumberDriverSlotEnd               FullCardNumber,
   cardNumberCodriverSlotEnd             FullCardNumber,
   similarEventsNumber                   SimilarEventsNumber
}
```

eventType jest typem zdarzenia.

eventRecordPurpose jest celem, dla którego zarejestrowano to zdarzenie.

eventBeginTime jest datą i godziną rozpoczęcia zdarzenia.

eventEndTime jest datą i godziną zakończenia zdarzenia.

cardNumberDriverSlotBegin identyfikuje kartę włożoną do szczeliny karty kierowcy na początku zdarzenia.

cardNumberCodriverSlotBegin identyfikuje kartę włożoną do szczeliny karty współkierowcy na początku zdarzenia.

cardNumberDriverSlotEnd identyfikuje kartę włożoną do szczeliny karty kierowcy na końcu zdarzenia.

cardNumberCodriverSlotEnd identyfikuje kartę włożoną do szczeliny karty współkierowcy na końcu zdarzenia.

similarEventsNumber jest liczbą podobnych zdarzeń w tym dniu.

Sekwencji tej można używać dla wszystkich zdarzeń innych niż przekroczenie prędkości.

Generacja 2:

```
VuEventRecord ::= SEQUENCE {
   eventType                              EventFaultType,
   eventRecordPurpose                     EventFaultRecordPurpose,
   eventBeginTime                         TimeReal,
   eventEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   similarEventsNumber                    SimilarEventsNumber,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Oprócz generacji 1 używane są następujące elementy danych:

manufacturerSpecificEventFaultData zawiera dodatkowe, szczegółowe informacje o zdarzeniu odnoszące się do danego producenta.

Zamiast cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd i cardNumber-CodriverSlotEnd w strukturze danych generacji 2 wykorzystuje się następujący element danych.

cardNumberAndGenDriverSlotBegin identyfikuje kartę, w tym jej generację, włożoną do szczeliny karty kierowcy na początku zdarzenia.

cardNumberAndGenCodriverSlotBegin identyfikuje kartę, w tym jej generację, włożoną do szczeliny karty współkierowcy na początku zdarzenia.

cardNumberAndGenDriverSlotEnd identyfikuje kartę, w tym jej generację, włożoną do szczeliny karty kierowcy na końcu zdarzenia.

cardNumberAndGenCodriverSlotEnd identyfikuje kartę, w tym jej generację, włożoną do szczeliny karty współkierowcy na końcu zdarzenia.

Jeżeli w zdarzeniu zachodzi konflikt czasu eventBeginTime i eventEndTime należy interpretować w następujący sposób:

eventBeginTime jest datą i godziną urządzenia rejestrującego.

eventEndTime jest datą i godziną GNSS.

2.199. **VuEventRecordArray**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym, dotyczące zdarzeń (wymaganie 117 określone w załączniku 1C z wyłączeniem przekroczenia prędkości).

```
VuEventRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuEventRecord
}
```

recordType oznacza typ rekordu (VuEventRecord). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość VuEventRecord w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem rekordów dotyczących zdarzeń.

2.200. **VuFaultData**

Generacja 1:

Informacje przechowywane w przyrządzie rejestrującym dotyczące usterek (wymaganie 096 określone w załączniku 1B).

```
VuFaultData ::= SEQUENCE {
   noOfVuFaults                          INTEGER(0..255),
   vuFaultRecords                        SET SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults jest liczbą usterek wyszczególnionych w zbiorze vuFaultRecords.

vuFaultRecords jest zbiorem rekordów dotyczących usterek.

2.201. **VuFaultRecord**

Informacje przechowywane w przyrządzie rejestrującym dotyczące jednej usterki (wymaganie 096 określone w załączniku 1B i wymaganie 118 określone w załączniku 1C).

Generacja 1:

```
VuFaultRecord ::= SEQUENCE {
   faultType                             EventFaultType,
   faultRecordPurpose                    EventFaultRecordPurpose,
   faultBeginTime                        TimeReal,
   faultEndTime                          TimeReal,
   cardNumberDriverSlotBegin             FullCardNumber,
   cardNumberCodriverSlotBegin           FullCardNumber,
   cardNumberDriverSlotEnd               FullCardNumber,
   cardNumberCodriverSlotEnd             FullCardNumber
}
```

faultType jest typem usterki urządzenia rejestrującego.

faultRecordPurpose jest celem, dla którego ta usterka jest zarejestrowana.

faultBeginTime jest datą i godziną początku usterki.

faultEndTime jest datą i godziną zakończenia usterki.

cardNumberDriverSlotBegin identyfikuje kartę włożoną do szczeliny karty kierowcy na początku usterki.

cardNumberCodriverSlotBegin identyfikuje kartę włożoną do szczeliny karty współkierowcy na początku usterki.

cardNumberDriverSlotEnd identyfikuje kartę włożoną do szczeliny karty kierowcy na końcu usterki.

cardNumberCodriverSlotEnd identyfikuje kartę włożoną do szczeliny karty współkierowcy na końcu usterki.

Generacja 2:

```
VuFaultRecord ::= SEQUENCE {
   faultType                              EventFaultType,
   faultRecordPurpose                     EventFaultRecordPurpose,
   faultBeginTime                         TimeReal,
   faultEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Oprócz generacji 1 używany jest następujący element danych:

manufacturerSpecificEventFaultData zawiera dodatkowe, szczegółowe informacje o usterce odnoszące się do danego producenta.

Zamiast cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd i cardNumber-CodriverSlotEnd w strukturze danych generacji 2 wykorzystuje się następujący element danych.

cardNumberAndGenDriverSlotBegin identyfikuje kartę, w tym jej generację, włożoną do szczeliny karty kierowcy na początku usterki.

cardNumberAndGenCodriverSlotBegin identyfikuje kartę, w tym jej generację, włożoną do szczeliny karty współkierowcy na początku usterki.

cardNumberAndGenDriverSlotEnd identyfikuje kartę, w tym jej generację, włożoną do szczeliny karty kierowcy na końcu usterki.

cardNumberAndGenCodriverSlotEnd identyfikuje kartę, w tym jej generację, włożoną do szczeliny karty współkierowcy na końcu usterki.

2.202. **VuFaultRecordArray**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące usterek (wymaganie 118 określone w załączniku 1C).

```
VuFaultRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuFaultRecord
}
```

recordType oznacza typ rekordu (VuFaultRecord). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość VuFaultRecord w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem rekordów dotyczących usterek.

2.203. **VuGNSSCDRecord**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące położenia pojazdu GNSS, jeżeli nieprzerwany czas prowadzenia pojazdu przez kierowcę osiągnie wielokrotność trzech godzin (wymagania 108 i 110 określone w załączniku 1C).

```
VuGNSSCDRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   cardNumberAndGenDriverSlot             FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlot           FullCardNumberAndGeneration,
   gnssPlaceRecord                        GNSSPlaceRecord
}
```

timeStamp jest datą i godziną, kiedy nieprzerwany czas prowadzenia pojazdu przez posiadacza karty osiągnie wielokrotność trzech godzin.

cardNumberAndGenDriverSlot identyfikuje kartę, w tym jej generację, włożoną do szczeliny karty kierowcy.

cardNumberAndGenCodriverSlot identyfikuje kartę, w tym jej generację, włożoną do szczeliny karty współkierowcy.

gnssPlaceRecord zawiera informacje dotyczące położenia pojazdu.

2.204. **VuGNSSCDRecordArray**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące położenia pojazdu GNSS, jeżeli nieprzerwany czas prowadzenia pojazdu przez kierowcę osiągnie wielokrotność trzech godzin (wymagania 108 i 110 określone w załączniku 1C).

```
VuGNSSCDRecordArray  ::= SEQUENCE {
   recordType                             RecordType,
   recordSize                             INTEGER(1..65535),
   noOfRecords                            INTEGER(0..65535),
   records                                SET SIZE(noOfRecords) OF VuGNSSCDRecord
}
```

recordType oznacza typ rekordu (VuGNSSCDRecord). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość VuGNSSCDRecord w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem rekordów nieprzerwanego czasu prowadzenia pojazdu GNSS.

2.205. **VuIdentification**

Informacje przechowywane w przyrządzie rejestrującym dotyczące jego identyfikacji (wymaganie 075 określone w załączniku 1B oraz wymagania 93 i 121 określone w załączniku 1C).

Generacja 1:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                     VuManufacturerName,
   vuManufacturerAddress                  VuManufacturerAddress,
   vuPartNumber                           VuPartNumber,
   vuSerialNumber                         VuSerialNumber,
   vuSoftwareIdentification               VuSoftwareIdentification,
   vuManufacturingDate                    VuManufacturingDate,
   vuApprovalNumber                       VuApprovalNumber
}
```

vuManufacturerName jest nazwą producenta przyrządu rejestrującego.

vuManufacturerAddress jest adresem producenta przyrządu rejestrującego.

vuPartNumber jest numerem części przyrządu rejestrującego.

vuSerialNumber jest numerem seryjnym przyrządu rejestrującego.

vuSoftwareIdentification identyfikuje oprogramowanie zainstalowane w przyrządzie rejestrującym.

vuManufacturingDate jest datą produkcji przyrządu rejestrującego.

vuApprovalNumber jest numerem homologacji typu przyrządu rejestrującego.

Generacja 2:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                  VuManufacturerName,
   vuManufacturerAddress               VuManufacturerAddress,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   vuSoftwareIdentification            VuSoftwareIdentification,
   vuManufacturingDate                 VuManufacturingDate,
   vuApprovalNumber                    VuApprovalNumber,
   vuGeneration                        Generation,
   vuAbility                           VuAbility
}
```

Oprócz generacji 1 używane są następujące elementy danych:

vuGeneration identyfikuje generację przyrządu rejestrującego.

vuAbility zapewnia informacje, czy VU obsługuje karty do tachografu generacji 1.

2.206. **VuIdentificationRecordArray**

Generacja 2:

VuIdentification wraz z metadanymi stosowany w protokole pobierania danych.

```
VuIdentificationRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuIdentification
}
```

recordType oznacza typ rekordu (VuIdentification). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość VuIdentification w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem rekordów VuIdentification.

2.207. **VuITSConsentRecord**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące zgody kierowcy na stosowanie inteligentnych systemów transportowych.

```
VuITSConsentRecord ::= SEQUENCE {
   cardNumberAndGen                    FullCardNumberAndGeneration,
   consent                             BOOLEAN
}
```

companyCardNumberAndGen identyfikuje kartę, w tym jej generację. Musi to być karta kierowcy lub karta warsztatowa.

consent jest flagą wskazującą, czy kierowca wyraził zgodę na stosowanie inteligentnych systemów transportowych w danym pojeździe / przyrządzie rejestrującym.

Przypisanie wartości:

TRUE wskazuje zgodę kierowcy na stosowanie inteligentnych systemów transportowych

FALSE wskazuje odmowę kierowcy dotyczącą stosowania inteligentnych systemów transportowych

2.208. **VuITSConsentRecordArray**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące zgody kierowcy na stosowanie inteligentnych systemów transportowych (wymaganie 200 określone w załączniku 1C).

```
VuITSConsentRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuITSConsentRecord
}
```

recordType oznacza typ rekordu (VuITSConsentRecord). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość VuITSConsentRecord w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem rekordów ITS.

2.209. **VuManufacturerAddress**

Adres producenta przyrządu rejestrującego.

```
VuManufacturerAddress ::= Address
```

Przypisanie wartości: nieokreślona.

2.210. **VuManufacturerName**

Nazwa producenta przyrządu rejestrującego.

```
VuManufacturerName ::= Name
```

Przypisanie wartości: nieokreślona.

2.211. **VuManufacturingDate**

Data produkcji przyrządu rejestrującego.

```
VuManufacturingDate ::= TimeReal
```

Przypisanie wartości: nieokreślona.

2.212. **VuOverSpeedingControlData**

Informacje przechowywane w przyrządzie rejestrującym dotyczące przekroczeń prędkości od ostatniej kontroli przekroczenia prędkości (wymaganie 095 określone w załączniku 1B i wymaganie 117 określone w załączniku 1C).

```
VuOverSpeedingControlData ::= SEQUENCE {
   lastOverspeedControlTime            TimeReal,
   firstOverspeedSince                 TimeReal,
   numberOfOverspeedSince              OverspeedNumber
}
```

lastOverspeedControlTime jest datą i godziną ostatniej kontroli przekroczenia prędkości.

firstOverspeedSince jest datą i godziną pierwszego przekroczenia prędkości po tej ostatniej kontroli przekroczenia prędkości.

numberOfOverspeedSince jest liczbą zdarzeń przekroczenia prędkości od ostatniej kontroli przekroczenia prędkości.

2.213. **VuOverSpeedingControlDataRecordArray**

Generacja 2:

VuOverSpeedingControlData wraz z metadanymi stosowany w protokole pobierania danych.

```
VuOverSpeedingControlDataRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuOverSpeedingControlData
}
```

recordType oznacza typ rekordu (VuOverSpeedingControlData). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość VuOverSpeedingControlData w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem rekordów danych kontroli przekroczenia prędkości.

2.214. **VuOverSpeedingEventData**

Generacja 1:

Informacje przechowywane w przyrządzie rejestrującym dotyczące zdarzeń przekroczenia prędkości (wymaganie 094 określone w załączniku 1B).

```
VuOverSpeedingEventData ::= SEQUENCE {
   noOfVuOverSpeedingEvents            INTEGER(0..255),
   vuOverSpeedingEventRecords          SET SIZE(noOfVuOverSpeedingEvents) OF
                                       VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents jest liczbą zdarzeń wyszczególnionych w zbiorze vuOverSpeedingEventRecords.

vuOverSpeedingEventRecords jest zbiorem rekordów zdarzeń przekroczenia prędkości.

2.215. **VuOverSpeedingEventRecord**

Generacja 1:

Informacje przechowywane w przyrządzie rejestrującym dotyczące zdarzeń przekroczenia prędkości (wymaganie 094 określone w załączniku 1B i wymaganie 117 określone w załączniku 1C).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   maxSpeedValue                      SpeedMax,
   averageSpeedValue                  SpeedAverage,
   cardNumberDriverSlotBegin          FullCardNumber,
   similarEventsNumber                SimilarEventsNumber
}
```

eventType jest typem zdarzenia.

eventRecordPurpose jest celem, dla którego zarejestrowano to zdarzenie.

eventBeginTime jest datą i godziną rozpoczęcia zdarzenia.

eventEndTime jest datą i godziną zakończenia zdarzenia.

maxSpeedValue jest maksymalną prędkością zmierzoną w czasie zdarzenia.

averageSpeedValue jest średnią arytmetyczną prędkości zmierzonych w czasie zdarzenia.

cardNumberDriverSlotBegin identyfikuje kartę włożoną do szczeliny karty kierowcy na początku zdarzenia.

similarEventsNumber jest liczbą podobnych zdarzeń w tym dniu.

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące zdarzeń przekroczenia prędkości (wymaganie 094 określone w załączniku 1B i wymaganie 117 określone w załączniku 1C).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   maxSpeedValue                      SpeedMax,
   averageSpeedValue                  SpeedAverage,
   cardNumberAndGenDriverSlotBegin    FullCardNumberAndGeneration,
   similarEventsNumber                SimilarEventsNumber
}
```

Zamiast cardNumberDriverSlotBegin w strukturze danych generacji 2 wykorzystuje się następujący element danych.

cardNumberAndGenDriverSlotBegin identyfikuje kartę, w tym jej generację, włożoną do szczeliny karty kierowcy na początku zdarzenia.

2.216. **VuOverSpeedingEventRecordArray**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące zdarzeń przekroczenia prędkości (wymaganie 117 określone w załączniku 1C).

```
VuOverSpeedingEventRecordArray ::= SEQUENCE {
   recordType                         RecordType,
   recordSize                         INTEGER(1..65535),
   noOfRecords                        INTEGER(0..65535),
   records                            SET SIZE(noOfRecords) OF
                                      VuOverSpeedingEventRecord
}
```

recordType oznacza typ rekordu (VuOverSpeedingEventRecord). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość VuOverSpeedingEventRecord w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem rekordów zdarzeń przekroczenia prędkości.

2.217. **VuPartNumber**

Numer części przyrządu rejestrującego.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Przypisanie wartości: swoista dla producenta VU.

2.218. **VuPlaceDailyWorkPeriodData**

Generacja 1:

Informacje przechowywane w przyrządzie rejestrującym dotyczące miejsc rozpoczęcia lub zakończenia dziennego okresu pracy kierowców (wymaganie 087 określone w załączniku 1B oraz wymagania 108 i 110 określone w załączniku 1C).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {
   noOfPlaceRecords                    INTEGER(0..255),
   vuPlaceDailyWorkPeriodRecords       SET SIZE(noOfPlaceRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords jest liczbą rekordów wyszczególnionych w zbiorze vuPlaceDailyWorkPeriodRecords.

vuPlaceDailyWorkPeriodRecords jest zbiorem rekordów dotyczących miejsca.

2.219. **VuPlaceDailyWorkPeriodRecord**

Generacja 1:

Informacje przechowywane w przyrządzie rejestrującym dotyczące miejsca rozpoczęcia lub zakończenia dziennego okresu pracy kierowcy (wymaganie 087 określone w załączniku 1B oraz wymagania 108 i 110 określone w załączniku 1C).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumber                      FullCardNumber,
   placeRecord                         PlaceRecord
}
```

fullCardNumber zawiera typ karty kierowcy, państwo członkowskie wydające kartę i numer karty.

placeRecord zawiera informacje dotyczące wprowadzonego miejsca.

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące miejsca rozpoczęcia lub zakończenia dziennego okresu pracy kierowcy (wymaganie 087 określone w załączniku 1B oraz wymagania 108 i 110 określone w załączniku 1C).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   placeRecord                         PlaceRecord
}
```

Zamiast fullCardNumber w strukturze danych generacji 2 wykorzystuje się następujący element danych:

fullCardNumberAndGeneration jest typem karty, państwem członkowskim wydającym kartę, numerem karty i generacją przechowywanymi na karcie.

2.220. **VuPlaceDailyWorkPeriodRecordArray**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące miejsc rozpoczęcia lub zakończenia dziennego okresu pracy kierowców (wymagania 108 i 110 określone w załączniku 1C).

```
VuPlaceDailyWorkPeriodRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

recordType oznacza typ rekordu (VuPlaceDailyWorkPeriodRecord). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość VuPlaceDailyWorkPeriodRecord w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem rekordów dotyczących miejsca.

2.221. **VuPrivateKey**

Generacja 1:

Klucz prywatny przyrządu rejestrującego.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.222. **VuPublicKey**

Generacja 1:

Klucz publiczny przyrządu rejestrującego.

```
VuPublicKey ::= PublicKey
```

2.223. **VuSerialNumber**

Numer seryjny przyrządu rejestrującego (wymaganie 075 określone w załączniku 1B i wymaganie 93 określone w załączniku 1C).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.224. **VuSoftInstallationDate**

Data instalacji wersji oprogramowania przyrządu rejestrującego.

```
VuSoftInstallationDate ::= TimeReal
```

Przypisanie wartości: nieokreślona.

2.225. **VuSoftwareIdentification**

Informacje przechowywane w przyrządzie rejestrującym dotyczące zainstalowanego oprogramowania.

```
VuSoftwareIdentification ::= SEQUENCE {
   vuSoftwareVersion                    VuSoftwareVersion,
   vuSoftInstallationDate               VuSoftInstallationDate
}
```

vuSoftwareVersion jest numerem wersji oprogramowania przyrządu rejestrującego.

vuSoftInstallationDate jest datą zainstalowania wersji oprogramowania.

2.226. **VuSoftwareVersion**

Numer wersji oprogramowania przyrządu rejestrującego.

```
VuSoftwareVersion ::= IA5String(SIZE(4))
```

Przypisanie wartości: nieokreślona.

2.227. **VuSpecificConditionData**

Generacja 1:

Informacje przechowywane w przyrządzie rejestrującym dotyczące warunków szczególnych.

```
VuSpecificConditionData ::= SEQUENCE {
   noOfSpecificConditionRecords         INTEGER(0..2^16-1)
   specificConditionRecords             SET SIZE (noOfSpecificConditionRecords) OF
                                        SpecificConditionRecord
}
```

noOfSpecificConditionRecords jest liczbą rekordów wyszczególnionych w zbiorze specificConditionRecords.

specificConditionRecords jest zbiorem rekordów dotyczących warunków szczególnych.

2.228. **VuSpecificConditionRecordArray**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące warunków szczególnych (wymaganie 130 określone w załączniku 1C).

```
VuSpecificConditionRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        SpecificConditionRecord
}
```

recordType oznacza typ rekordu (SpecificConditionRecord). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość SpecificConditionRecord w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem rekordów dotyczących warunków szczególnych.

2.229. **VuTimeAdjustmentData**

Generacja 1:

Informacje przechowywane w przyrządzie rejestrującym dotyczące korekt czasu dokonanych poza regularną kalibracją (wymaganie 101 określone w załączniku 1C).

```
VuTimeAdjustmentData ::= SEQUENCE {
   noOfVuTimeAdjRecords                INTEGER(0..6),
   vuTimeAdjustmentRecords             SET SIZE(noOfVuTimeAdjRecords) OF
                                       VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords jest liczbą rekordów w zbiorze vuTimeAdjustmentRecords.

vuTimeAdjustmentRecords jest zbiorem rekordów dotyczących korekty czasu.

2.230. **VuTimeAdjustmentGNSSRecord**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące korekty czasu w oparciu o dane dotyczące czasu z GNSS (wymagania 124 i 125 określone w załączniku 1C).

```
VuTimeAdjustmentGNSSRecord ::= SEQUENCE {
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal
}
```

oldTimeValue, newTimeValue są starą i nową wartością daty i godziny.

2.231. **VuTimeAdjustmentGNSSRecordArray**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące korekty czasu dokonywanej w oparciu o dane dotyczące czasu z GNSS (wymagania 124 i 125 określone w załączniku 1C).

```
VuTimeAdjustmentGNSSRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuTimeAdjustmentGNSSRecord
}
```

recordType oznacza typ rekordu (VuTimeAdjustmentGNSSRecord). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość VuTimeAdjustmentGNSSRecord w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem rekordów korekty czasu GNSS.

2.232. **VuTimeAdjustmentRecord**

Informacje przechowywane w przyrządzie rejestrującym dotyczące korekty czasu dokonanej poza regularną kalibracją (wymaganie 101 określone w załączniku 1B oraz wymagania 124 i 125 określone w załączniku 1C).

Generacja 1:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumber                   FullCardNumber
}
```

oldTimeValue, newTimeValue są starą i nową wartością daty i godziny.

workshopName, workshopAddress są nazwą i adresem warsztatu.

workshopCardNumber identyfikuje kartę warsztatowa użytą do dokonania korekty czasu.

Generacja 2:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumberAndGeneration      FullCardNumberAndGeneration
}
```

Zamiast workshopCardNumber w strukturze danych generacji 2 wykorzystuje się następujący element danych.

workshopCardNumberAndGeneration identyfikuje kartę warsztatowa, w tym jej generację, użytą do dokonania korekty czasu.

2.233. **VuTimeAdjustmentRecordArray**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące korekt czasu dokonanych poza regularną kalibracją (wymagania 124 i 125 określone w załączniku 1C).

```
VuTimeAdjustmentRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuTimeAdjustmentRecord
}
```

recordType oznacza typ rekordu (VuTimeAdjustmentRecord). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość VuTimeAdjustmentRecord w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem rekordów korekty czasu.

2.234. **WorkshopCardApplicationIdentification**

Informacje przechowywane na karcie warsztatowej dotyczące identyfikacji aplikacji na karcie (wymagania 307 i 330 określone w załączniku 1C).

Generacja 1:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfEventsPerType                    NoOfEventsPerType,
   noOfFaultsPerType                    NoOfFaultsPerType,
   activityStructureLength              CardActivityLengthRange,
   noOfCardVehicleRecords               NoOfCardVehicleRecords,
   noOfCardPlaceRecords                 NoOfCardPlaceRecords,
   noOfCalibrationRecords               NoOfCalibrationRecords
}
```

typeOfTachographCardId określa wdrożony typ karty.

cardStructureVersion określa wersję struktury wdrożonej na karcie.

noOfEventsPerType jest liczbą zdarzeń według typu zdarzenia możliwych do zarejestrowania na karcie.

noOfFaultsPerType jest liczbą usterek według typu usterki możliwych do zarejestrowania na karcie.

activityStructureLength podaje liczbę bajtów dostępnych do przechowywania rekordów czynności.

noOfCardVehicleRecords jest liczbą rekordów dotyczących pojazdów możliwych do zarejestrowania na karcie.

noOfCardPlaceRecords jest liczbą miejsc możliwych do zarejestrowania na karcie.

noOfCalibrationRecords jest liczbą rekordów kalibracyjnych możliwych do zarejestrowania na karcie.

Generacja 2:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfEventsPerType                    NoOfEventsPerType,
   noOfFaultsPerType                    NoOfFaultsPerType,
   activityStructureLength              CardActivityLengthRange,
   noOfCardVehicleRecords               NoOfCardVehicleRecords,
   noOfCardPlaceRecords                 NoOfCardPlaceRecords,
   noOfCalibrationRecords               NoOfCalibrationRecords,
   noOfGNSSCDRecords                    NoOfGNSSCDRecords,
   noOfSpecificConditionRecords         NoOfSpecificConditionRecords
}
```

Oprócz generacji 1 używane są następujące elementy danych:

noOfGNSSCDRecords jest liczbą rekordów nieprzerwanego czasu prowadzenia pojazdu GNSS, które mogą być przechowywane na karcie.

noOfSpecificConditionRecords jest liczbą rekordów warunków szczególnych, które mogą być zapisane na karcie.

2.235. **WorkshopCardCalibrationData**

Informacje przechowywane na karcie warsztatowej dotyczące czynności warsztatowych wykonanych przy użyciu karty (wymagania 314, 316, 337 i 339 określone w załączniku 1C).

```
WorkshopCardCalibrationData ::= SEQUENCE {
   calibrationTotalNumber              INTEGER(0 .. 2^16-1),
   calibrationPointerNewestRecord      INTEGER(0 .. NoOfCalibrationRecords-1),
   calibrationRecords                  SET SIZE(NoOfCalibrationRecords) OF
                                       WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber jest całkowitą liczbą kalibracji wykonanych przy użyciu karty.

calibrationPointerNewestRecord jest indeksem ostatniego, uaktualnionego rekordu kalibracyjnego.

Przypisanie wartości: liczba odpowiadającą licznikowi rekordów kalibracyjnych, rozpoczynając od „0” dla pierwszego wystąpienia rekordu kalibracyjnego w strukturze.

calibrationRecords jest zbiorem rekordów zawierających informacje o kalibracji lub korekcie czasu.

2.236. **WorkshopCardCalibrationRecord**

Informacje przechowywane na karcie warsztatowej dotyczące czynności wykonanych przy użyciu karty (wymagania 314 i 337 określone w załączniku 1C).

Generacja 1:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                  CalibrationPurpose,
   vehicleIdentificationNumber         VehicleIdentificationNumber,
   vehicleRegistration                 VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant      W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment       K-ConstantOfRecordingEquipment,
   lTyreCircumference                  L-TyreCircumference,
   tyreSize                            TyreSize,
   authorisedSpeed                     SpeedAuthorised,
   oldOdometerValue                    OdometerShort,
   newOdometerValue                    OdometerShort,
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal,
   nextCalibrationDate                 TimeReal,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   sensorSerialNumber                  SensorSerialNumber
}
```

calibrationPurpose jest celem kalibracji.

vehicleIdentificationNumber jest numerem VIN.

vehicleRegistration zawiera numer VRN i państwa członkowskiego rejestracji.

wVehicleCharacteristicConstant jest współczynnikiem charakterystycznym pojazdu.

kConstantOfRecordingEquipment jest stałą urządzenia rejestrującego.

lTyreCircumference jest obwodem tocznym kół.

tyreSize jest oznaczeniem rozmiarów opon zamontowanych w pojeździe.

authorisedSpeed jest maksymalną, dozwoloną prędkością pojazdu.

oldOdometerValue, newOdometerValue są starym i nowym stanem licznika kilometrów.

oldTimeValue, newTimeValue są starą i nową wartością daty i godziny.

nextCalibrationDate jest datą następnej kalibracji typu określonego w CalibrationPurpose, którą powinien przeprowadzić autoryzowany organ kontrolny.

vuPartNumber, **vuSerialNumber** and **sensorSerialNumber** są elementami danych do identyfikacji urządzenia rejestrującego.

Generacja 2:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                  CalibrationPurpose,
   vehicleIdentificationNumber         VehicleIdentificationNumber,
   vehicleRegistration                 VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant      W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment       K-ConstantOfRecordingEquipment,
   lTyreCircumference                  L-TyreCircumference,
   tyreSize                            TyreSize,
   authorisedSpeed                     SpeedAuthorised,
   oldOdometerValue                    OdometerShort,
   newOdometerValue                    OdometerShort,
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal,
   nextCalibrationDate                 TimeReal,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   sensorSerialNumber                  SensorSerialNumber,
   sensorGNSSSerialNumber              SensorGNSSSerialNumber,
   rcmSerialNumber                     RemoteCommunicationModuleSerialNumber,
   sealDataCard                        SealDataCard
}
```

Oprócz generacji 1 używane są następujące elementy danych:

sensorGNSSSerialNumber, który identyfikuje urządzenie zewnętrzne GNSS.

rcmSerialNumber, który identyfikuje moduł komunikacji na odległość.

sealDataCard podaje informacje o plombach przymocowanych do różnych części pojazdu.

2.237. **WorkshopCardHolderIdentification**

Informacje przechowywane na karcie warsztatowej dotyczące identyfikacji posiadacza karty (wymagania 311 i 334 określone w załączniku 1C).

```
WorkshopCardHolderIdentification ::= SEQUENCE {
   workshopName                        Name,
   workshopAddress                     Address,
   cardHolderName                      HolderName,
   cardHolderPreferredLanguage         Language
}
```

workshopName jest nazwą warsztatu posiadacza karty.

workshopAddressjest adresem warsztatu posiadacza karty.

cardHolderName jest nazwiskiem i imieniem (imionami) posiadacza karty (np. nazwiskiem mechanika).

cardHolderPreferredLanguage jest preferowanym językiem posiadacza karty.

2.238. **WorkshopCardPIN**

Osobisty numer identyfikacyjny (PIN) karty warsztatowej (wymaganie 309 i 332 określone w załączniku 1C).

```
WorkshopCardPIN ::= IA5String(SIZE(8))
```

Przypisanie wartości: PIN znany posiadaczowi karty, z prawej strony wypełniony bajtami o wartości „FF" aż do 8 bajtów.

2.239. **W-VehicleCharacteristicConstant**

Współczynnik charakterystyczny pojazdu (definicja k)).

```
W-VehicleCharacteristicConstant ::= INTEGER(0..2^16-1))
```

Przypisanie wartości: liczba impulsów na kilometr w zakresie operacyjnym 0 do 64 255 impulsów/km.

2.240. **VuPowerSupplyInterruptionRecord**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące zdarzeń przerwy w zasilaniu (wymaganie 117 określone w załączniku 1C).

```
VuPowerSupplyInterruptionRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   cardNumberAndGenDriverSlotBegin    FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd      FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin  FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd    FullCardNumberAndGeneration,
   similarEventsNumber                SimilarEventsNumber
}
```

eventType jest typem zdarzenia.

eventRecordPurpose jest celem, dla którego zarejestrowano to zdarzenie.

eventBeginTime jest datą i godziną rozpoczęcia zdarzenia.

eventEndTime jest datą i godziną zakończenia zdarzenia.

cardNumberAndGenDriverSlotBegin identyfikuje kartę, w tym jej generację, włożoną do szczeliny karty kierowcy na początku zdarzenia.

cardNumberAndGenDriverSlotEnd identyfikuje kartę, w tym jej generację, włożoną do szczeliny karty kierowcy na końcu zdarzenia.

cardNumberAndGenCodriverSlotBegin identyfikuje kartę, w tym jej generację, włożoną do szczeliny karty współkierowcy na początku zdarzenia.

cardNumberAndGenCodriverSlotEnd identyfikuje kartę, w tym jej generację, włożoną do szczeliny karty współkierowcy na końcu zdarzenia.

similarEventsNumber jest liczbą podobnych zdarzeń w tym dniu.

2.241. **VuPowerSupplyInterruptionRecordArray**

Generacja 2:

Informacje przechowywane w przyrządzie rejestrującym dotyczące zdarzeń przerwy w zasilaniu (wymaganie 117 określone w załączniku 1C).

```
VuPowerSupplyInterruptionRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuPowerSupplyInterruptionRecord
}
```

recordType oznacza typ rekordu (VuPowerSupplyInterruptionRecord). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość VuPowerSupplyInterruptionRecord w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem rekordów zdarzeń przerwy w zasilaniu.

2.242. **VuSensorExternalGNSSCoupledRecordArray**

Generacja 2:

Zbiór zapisów SensorExternalGNSSCoupledRecord wraz z metadanymi stosowany w protokole pobierania danych.

```
VuSensorExternalGNSSCoupledRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       SensorExternalGNSSCoupledRecord
}
```

recordType oznacza typ rekordu (SensorExternalGNSSCoupledRecord). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość SensorExternalGNSSCoupledRecord w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem rekordów SensorExternalGNSSCoupled.

2.243. **VuSensorPairedRecordArray**

Generacja 2:

Zbiór zapisów SensorPairedRecord wraz z metadanymi stosowany w protokole pobierania danych.

```
VuSensorPairedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF SensorPairedRecord
}
```

recordType oznacza typ rekordu (SensorPairedRecord). **Przypisanie wartości:** zob. RecordType

recordSize to wielkość SensorPairedRecord w bajtach.

noOfRecords jest liczbą rekordów w zbiorze.

records jest zbiorem rekordów sparowanego czujnika.

3. DEFINICJE WARTOŚCI I ZAKRESU WIELKOŚCI

Definicja wartości zmiennych używana w definicjach w ust. 2.

```
TimeRealRange ::= 2^32-1
```

4. ZESTAW ZNAKÓW:

W łańcuchach IA5Strings używa się znaków ASCII zdefiniowanych w normie ISO/IEC 8824-1. Na potrzeby czytelności i łatwego odwoływania się poniżej podano przypisanie wartości. W przypadku rozbieżności między tą uwagą a normą obowiązują przepisy normy ISO/IEC 8824-1.

```
  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ?
@ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ \ ] ^ _
` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
```

W innych łańcuchach znaków (Address, Name, VehicleRegistrationNumber) używa się dodatkowo znaków zdefiniowanych kodami od 161 do 255 następujących 8-bitowych standardowych zestawów znaków, określonych numerem Code Page: Standardowy zestaw znaków	Code Page (dziesiętny)
ISO/IEC 8859-1 Latin-1 – dla Europy Zachodniej	1
ISO/IEC 8859-2 Latin-2 – dla Europy Środkowej i Wschodniej	2
ISO/IEC 8859-3 Latin-3 – dla Europy Południowej	3
ISO/IEC 8859-5 Latin – dla cyrylicy	5
ISO/IEC 8859-7 Latin – dla alfabetu greckiego	7
ISO/IEC 8859-9 Latin-5 – dla alfabetu tureckiego	9
ISO/IEC 8859-13 Latin-7 – dla krajów bałtyckich	13
ISO/IEC 8859-15 Latin-9	15
ISO/IEC 8859-16 Latin-10 – dla Europy Południowo-Wschodniej	16
KOI8-R Latin – dla cyrylicy	80
KOI8-U Latin – dla cyrylicy	85

5. KODOWANIE

Przy kodowaniu zgodnie z zasadami ASN.1, wszystkie zdefiniowane typy danych koduje się zgodnie z wariantem unormowanym w ISO/IEC 8825-2.

6. IDENTYFIKATORY OBIEKTU I IDENTYFIKATORY APLIKACJI

6.1. **Identyfikatory obiektu**

Identyfikatory obiektu (OID) wymienione w niniejszym rozdziale mają zastosowanie wyłącznie do generacji 2. Takie OID wyszczególniono w TR-03110-3 i powtórzono dla kompletności wywodu. Takie OID zawarto w poddrzewie bsi-de:

```
bsi-de OBJECT IDENTIFIER ::= {
   itu-t(0) identified-organization(4) etsi(0)
   reserved(127) etsi-identified-organization(0) 7
}
```

Identyfikatory protokołu uwierzytelnienia VU

```
id-TA         OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 2}
id-TA-ECDSA                 OBJECT IDENTIFIER ::= {id-TA 2}
id-TA-ECDSA-SHA-256 OBJECT IDENTIFIER ::= {id-TA-ECDSA 3}
id-TA-ECDSA-SHA-384 OBJECT IDENTIFIER ::= {id-TA-ECDSA 4}
id-TA-ECDSA-SHA-512 OBJECT IDENTIFIER ::= {id-TA-ECDSA 5}
```

Przykład: Załóżmy, że należy dokonać uwierzytelnienia VU za pomocą SHA-384, wtedy identyfikatorem obiektu, który należy użyć jest (w składni ASN.1) `bsi-de protocols(2) smartcard(2) 2 2 4`. Wartość tego identyfikatora obiektu w zapisie kropkowym wynosi `0.4.0.127.0.7.2.2.2.2.4`.

	Zapis kropkowy	Zapis bajtowy
id-TA-ECDSA-SHA-256	0.4.0.127.0.7.2.2.2.2.3	'04 00 7F 00 07 02 02 02 02 03'
id-TA-ECDSA-SHA-384	0.4.0.127.0.7.2.2.2.2.4	'04 00 7F 00 07 02 02 02 02 04'
id-TA-ECDSA-SHA-512	0.4.0.127.0.7.2.2.2.2.5	'04 00 7F 00 07 02 02 02 02 05'

Identyfikatory protokołu uwierzytelnienia z chipem

```
id-CA         OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 3}
id-CA-ECDH                          OBJECT IDENTIFIER ::= {id-CA 2}
id-CA-ECDH-AES-CBC-CMAC-128         OBJECT IDENTIFIER ::= {id-CA-ECDH 2}
id-CA-ECDH-AES-CBC-CMAC-192         OBJECT IDENTIFIER ::= {id-CA-ECDH 3}
id-CA-ECDH-AES-CBC-CMAC-256         OBJECT IDENTIFIER ::= {id-CA-ECDH 4}
```

Przykład: Przypuśćmy, że uwierzytelnienie chipu ma zostać dokonane za pomocą algorytmu ECDH, co daje długość klucza sesji AES 128 bitów. Ten klucz sesji zostanie następnie wykorzystany w trybie pracy CBC w celu zapewnienia poufności danych i z algorytmem CMAC w celu zapewnienia autentyczności danych. Zatem identyfikatorem obiektu, który należy użyć jest (w składni ASN.1) `bsi-de protocols(2) smartcard(2) 3 2 2`. Wartość tego identyfikatora obiektu w zapisie kropkowym wynosi `0.4.0.127.0.7.2.2.3.2.2`.

	Zapis kropkowy	Zapis bajtowy
id-CA-ECDH-AES-CBC-CMAC-128	0.4.0.127.0.7.2.2.3.2.2	'04 00 7F 00 07 02 02 03 02 02'
id-CA-ECDH-AES-CBC-CMAC-192	0.4.0.127.0.7.2.2.3.2.3	'04 00 7F 00 07 02 02 03 02 03'
id-CA-ECDH-AES-CBC-CMAC-256	0.4.0.127.0.7.2.2.3.2.4	'04 00 7F 00 07 02 02 03 02 04'

6.2. Identyfikatory aplikacji

Generacja 2:

Identyfikator aplikacji (AID) dla urządzenia zewnętrznego GNSS (generacja 2) jest określony za pomocą „FF 44 54 45 47 4D". Jest to zastrzeżony AID zgodny z normą ISO/IEC 7816-4.

Uwaga: 5 ostatnich bajtów koduje DTEGM dla urządzenia zewnętrznego GNSS tachografu inteligentnego.

Identyfikator aplikacji dla aplikacji kart do tachografów generacji 2 jest określony za pomocą „FF 53 4D 52 44 54". Jest to zastrzeżony AID zgodny z normą ISO/IEC 7816-4.

Dodatek 2

SPECYFIKACJA KART DO TACHOGRAFÓW

SPIS TREŚCI

1. WPROWADZENIE

1.1. **Skróty**

Do celów niniejszego dodatku stosuje się poniższe skróty.

AC	[Access conditions] warunki dostępu
AES	[Advanced Encryption Standard] zaawansowany standard szyfrowania
AID	[Application Identifier] identyfikator aplikacji
ALW	[Always] zawsze
APDU	[Application Protocol Data Unit] jednostka danych protokołu aplikacji (struktura polecenia)
ATR	[Answer To Reset] reakcja na sprowadzenie do stanu wyjściowego
AUT	[Authenticated] uwierzytelniony
C6, C7	styki 6 i 7 karty opisane w normie ISO/IEC 7816-2
cc	[clock cycles] cykle zegarowe
CHV	[Card holder Verification Information] informacje weryfikacyjne posiadacza karty
CLA	bajt klasy w poleceniu APDU
DSRC	[Dedicated Short Range Communication] wydzielona łączność krótkiego zasięgu
DF	[Dedicated File] plik dedykowany. DF może zawierać inne pliki (EF lub DF)
ECC	[Elliptic Curve Cryptography] kryptografia krzywych eliptycznych
EF	[Elementary File] plik elementarny
etu	[elementary time unit] elementarna jednostka czasu
G1	[Generation 1] 1. generacja
G2	[Generation 2] 2. generacja
IC	[Integrated Circuit] układ scalony
ICC	[Integrated Circuit Card] karta z układem scalonym
ID	[Identifier] identyfikator
IFD	[Interface Device] urządzenie interfejsu
IFS	[Information Field Size] wielkość pola informacyjnego
IFSC	[Information Field Size for the card] wielkość pola informacyjnego dla karty

IFSD	[Information Field Size Device] wielkość pola informacyjnego urządzenia (dla terminala)
INS	bajt instrukcji w poleceniu APDU
Lc	długość danych wejściowych dla polecenia APDU
Le	długość danych oczekiwanych (dane wyjściowe dla polecenia)
MF	[Master File] plik główny (root DF)
NAD	[Node Address] adres węzła używany w protokole T=1
NEV	[Never] nigdy
P1-P2	bajty parametryczne
PIN	[Personal Identification Number] osobisty numer identyfikacyjny
PRO SM	[Protected with secure messaging] chroniony z bezpieczną wymianą komunikatów
PTS	[Protocol Transmission Selection] wybór protokołu komunikacyjnego
RFU	[Reserved for Future Use] zastrzeżone do wykorzystania w przyszłości
RST	[Reset] sprowadzenie do stanu wyjściowego (karty)
SFID	[Short EF Identifier] krótki identyfikator EF
SM	[Secure Messaging] bezpieczna wymiana komunikatów
SW1-SW2	bajty stanu
TS	początkowy znak ATR
VPP	napięcie programowania
VU	[Vehicle Unit] przyrząd rejestrujący
XXh	wartość XX w zapisie heksadecymalnym
'XXh'	wartość XX w zapisie heksadecymalnym
||	symbol konkatenacji 03||04=0304

1.2. **Odniesienia**

W niniejszym dodatku stosuje się następujące odniesienia:

ISO/IEC 7816-2 Karty identyfikacyjne – Karty z układami scalonymi – część 2: Wymiary i rozmieszczenie styków. ISO/IEC 7816-2:2007.

ISO/IEC 7816-3 Karty identyfikacyjne – Karty z układami scalonymi – część 3: Złącze elektryczne i protokoły komunikacyjne. ISO/IEC 7816-3:2006.

ISO/IEC 7816-4 Karty identyfikacyjne – Karty z układami scalonymi – część 4: Organizacja, zabezpieczenia i polecenia wymiany. ISO/IEC 7816-4:2013 + Cor 1: 2014.

ISO/IEC 7816-6 Karty identyfikacyjne – Karty z układami scalonymi – część 6: Międzybranżowe elementy danych do wymiany. ISO/IEC 7816-6:2004 + Cor 1: 2006.

ISO/IEC 7816-8 Karty identyfikacyjne – Karty z układami scalonymi – część 8: Polecenia operacji zabezpieczających. ISO/IEC 7816-8:2004.

ISO/IEC 9797-2 Technologia informatyczna – Techniki zabezpieczeń – Kody uwierzytelniania wiadomości (MAC) – część 2: Mechanizmy wykorzystujące funkcję haszującą. ISO/IEC 9797-2:2011

2. CHARAKTERYSTYKI ELEKTRYCZNE I FIZYCZNE

TCS_01 Wszystkie sygnały elektryczne muszą być zgodne z normą ISO/IEC 7816-3, chyba że określono inaczej.

TCS_02 Rozmieszczenie i wymiary styków kart muszą być zgodne z normą ISO/IEC 7816-2.

2.1. **Napięcie zasilające i pobór prądu**

TCS_03 Karta pracuje zgodnie ze specyfikacją przy poborze w granicach określonych w normie ISO/IEC 7816-3.

TCS_04 Karta pracuje z Vcc = 3V (± 0,3V) bądź z Vcc = 5V (± 0,5V).

Wybór napięcia odbywa się zgodnie z normą ISO/IEC 7816-3.

2.2. **Napięcie programowania V_{pp}**

TCS_05 Karta nie wymaga napięcia programowania na pinie C6. Oczekuje się, że pin C6 nie jest przyłączony w IFD. Styk C6 może być przyłączony do V_{cc} na karcie, ale nie może być przyłączony do masy. W żadnym przypadku napięcie to nie może być interpretowane.

2.3. **Generowanie i częstotliwość zegara**

TCS_06 Karta pracuje w zakresie częstotliwości 1–5 MHz i może obsługiwać wyższe częstotliwości. W czasie jednej sesji karty częstotliwość zegara może zmieniać się w granicach ± 2 %. Częstotliwość zegara generowana jest przez przyrząd rejestrujący, a nie przez kartę. Cykl pracy może zmieniać się w granicach 40–60 %.

TCS_07 W warunkach określonych na karcie w pliku EF ICC zewnętrzny zegar może zostać zatrzymany. Pierwszy bajt treści pliku EF ICC koduje warunki trybu pracy Clockstop:

Niski	Wysoki		
Bit 3	Bit 2	Bit 1	
0	0	1	Clockstop dozwolony, brak preferowanego poziomu
0	1	1	Clockstop dozwolony, preferowany poziom wysoki
1	0	1	Clockstop dozwolony, preferowany poziom niski
0	0	0	Clockstop niedozwolony
0	1	0	Clockstop dozwolony tylko przy wysokim poziomie
1	0	0	Clockstop dozwolony tylko przy niskim poziomie

Bitów od 4 do 8 nie używa się.

2.4. **Styk we/wy**

TCS_08 Styk we/wy C7 służy do odbierania i wysyłania danych do IFD. W czasie pracy tylko karta albo tylko IFD jest w trybie nadawania. Gdyby jednak obie jednostki jednocześnie znalazły się w trybie nadawania, nie może to spowodować uszkodzenia karty. Karta wchodzi do trybu odbioru, chyba że nadaje dane.

2.5. **Stany karty**

TCS_09 Gdy podawane jest napięcie zasilające, karta pracuje w dwóch stanach:

stan operacyjny, w którym karta wykonuje polecenia lub jest połączona z jednostką cyfrową;

stan jałowy we wszystkich pozostałych sytuacjach (w tym stanie karta zachowuje wszystkie dane).

3. SPRZĘT I KOMUNIKACJA

3.1. **Wprowadzenie**

W punkcie tym opisano minimalną funkcjonalność wymaganą od kart do tachografów i VU w celu zagwarantowania prawidłowego funkcjonowania i interoperacyjności.

Karty do tachografów muszą być zgodne, w największym możliwym stopniu, z obowiązującymi normami ISO/IEC (w szczególności z normą ISO/IEC 7816). Niemniej jednak szczegółowo opisano polecenia i protokoły w celu określenia niektórych ograniczonych zastosowań lub różnic, o ile takie występują. Opisane polecenia są w pełni zgodne z przywołanymi normami, jeżeli nie wskazano inaczej.

3.2. **Protokół komunikacyjny**

TCS_10 Protokół komunikacyjny musi być zgodny z normą ISO/IEC 7816-3 dla T = 0 oraz T = 1. W szczególności VU musi rozpoznawać wysyłane przez kartę przedłużenia czasu oczekiwania.

3.2.1 *Protokoły*

TCS_11 Karta obsługuje zarówno protokół **T = 0**, jak i protokół **T=1**. Karta może ponadto obsługiwać dodatkowe protokoły zorientowane kontaktowo.

TCS_12 **T = 0** jest protokołem domyślnym, dlatego też polecenie **PTS** jest niezbędne do zmiany protokołu na **T = 1**.

TCS_13 Urządzenia wykorzystują **konwencję bezpośrednią** w obu protokołach: w związku z tym konwencja bezpośrednia jest obowiązkowa dla karty.

TCS_14 Bajt **karty informacyjnej wielkości pola** przedstawiony jest na ATR pod oznaczeniem TA3. Wartość ta jest nie mniejsza niż 'F0h' (= 240 bajtów).

Do protokołów stosuje się następujące ograniczenia:

TCS_15 **T=0**

— Urządzenie interfejsu wspiera odpowiedź na we/wy po wzroście krawędzi narastającego sygnału na RST z 400 cc.

— Urządzenie interfejsu potrafi odczytać znaki rozdzielone 12 etu.

— Urządzenie interfejsu odczytuje błędny znak i jego powtórzenie, jeżeli rozdzielone 13 etu. W przypadku wykrycia błędnego znaku na we/wy może pojawić się sygnał błędu między 1 etu a 2 etu. Urządzenie obsługuje opóźnienie 1 etu.

— Urządzenie interfejsu akceptuje 33-bajtowe ATR (TS + 32)

— Jeżeli TC1 znajduje się w ATR, to dla znaków wysyłanych przez urządzenie interfejsu jest dodatkowy czas ochronny (Extra Guard Time), chociaż znaki wysyłane przez kartę mogą być jeszcze przedzielone odstępami 12 etu. Odnosi się to także do znaku ACK wysyłanego przez kartę po wysłaniu znaku P3 przez urządzenie interfejsu.

— Urządzenie interfejsu bierze pod uwagę znak NUL wysyłany przez kartę.

— Urządzenie interfejsu akceptuje tryb uzupełniający dla ACK.

— Polecenia odbierz-odpowiedź (get-response) nie można używać w trybie łańcuchowym do otrzymywania danych, których długość może być większa niż 255 bajtów.

TCS_16 **T=1**

— Bajt NAD: nieużywany (NAD ustawia się na '00').

— S-block ABORT: nieużywany.

— Błąd stanu S-block VPP: nieużywany.

— Całkowita długość łańcucha dla pola danych nie może przekraczać 255 bajtów (IFD musi to zapewniać).

— IFD bezpośrednio po ATR podaje wielkość pola informacyjnego dla urządzenia (IFSD): IFD wysyła żądanie S-Block IFS po ATR, a karta odpowiada S-Block IFS. Zalecaną wartością dla IFSD są 254 bajty.

— Karta nie pyta o skorygowane IFS.

3.2.2 *ATR*

TCS_17 Urządzenie sprawdza bajty ATR, zgodnie z normą ISO/IEC 7816-3. Nie wykonuje się weryfikacji znaków historycznych ATR.

Przykład podstawowego Biprotocol ATR zgodnego z normą ISO/IEC 7816-3

Znak	Wartość	Uwagi
TS	'3Bh'	wskazuje konwencję bezpośrednią
T0	'85h'	TD1 obecny; jest 5 bajtów historycznych
TD1	'80h'	TD2 obecny; będzie użyty T=0
TD2	'11h'	TA3 obecny; będzie użyty T=1
TA3	'XXh' (min. 'F0h')	wielkość pola informacyjnego dla karty (IFSC)
TH1–TH5	'XXh'	znaki historyczne
TCK	'XXh'	znak kontrolny (exclusive OR)

TCS_18 Po ATR wybierany jest domyślnie plik główny (MF) i staje się katalogiem bieżącym.

3.2.3 *PTS*

TCS_19 Domyślnym protokołem jest T=0. Aby wybrać protokół T=1, urządzenie musi wysłać do karty PTS (znane też jako PPS).

TCS_20 Ponieważ oba protokoły T=0 i T=1 są wymagane dla karty, podstawowy PTS do przełączania między protokołami jest obowiązkowy dla karty.

PTS można używać, jak wskazano w normie ISO/IEC 7816-3, do przełączania na szybkości transmisji większe niż standardowa, proponowane przez kartę w ATR, jeżeli dotyczy (bajt TA(1)).

Większe szybkości transmisji są opcjonalne dla karty.

TCS_21 Jeżeli karta nie obsługuje innej szybkości transmisji niż standardowa (lub jeżeli nie obsługuje wybranej szybkości transmisji), karta musi prawidłowo odpowiadać na PTS, zgodnie z normą ISO/IEC 7816-3, opuszczając bajt PPS1.

Poniżej pokazano przykłady podstawowego PTS do wyboru protokołu:

Znak	Wartość	Uwagi
PPSS	'FFh'	znak inicjujący
PPS0	'00h' lub '01h'	nie ma PPS1 do PPS3; '00h', aby wybrać T0, '01h', aby wybrać T1
PK	'XXh'	znak kontrolny: 'XXh' = 'FFh', jeżeli PPS0 = '00h', 'XXh' = 'FEh', jeżeli PPS0 = '01h'.

3.3. **Zasady dostępu**

TCS_22 Zasada dostępu określa odpowiednie warunki zabezpieczenia dla danego trybu dostępu, tj. polecenia. Jeżeli przedmiotowe warunki zabezpieczenia są spełnione, odpowiednie polecenie jest przetwarzane.

TCS_23 Następujące warunki zabezpieczenia są stosowane na potrzeby karty do tachografu:

Skrót	Znaczenie
ALW	Operacja jest zawsze możliwa i może być wykonywana bez ograniczeń. Polecenie i odpowiedź APDU są wysyłane w postaci zwykłego tekstu, tzn. bez bezpiecznej wymiany komunikatów.
NEV	Operacja nie jest nigdy możliwa.
PLAIN-C	Polecenie APDU jest wysyłane w postaci zwykłego tekstu, tzn. bez bezpiecznej wymiany komunikatów.
PWD	Działanie może zostać zrealizowane, wyłącznie jeżeli PIN karty warsztatowej został pomyślnie zweryfikowany, tzn. jeżeli stan zabezpieczenia wewnętrznego karty ma status „PIN_Verified". Polecenie musi być przesłane bez bezpiecznej wymiany komunikatów.
EXT-AUT-G1	Działanie może zostać zrealizowane, wyłącznie jeżeli polecenie External Authenticate dla uwierzytelnienia 1. generacji (zob. także dodatek 11 część A) zostało pomyślnie wykonane.
SM-MAC-G1	Polecenie i odpowiedź APDU muszą być stosowane z bezpieczną wymianą komunikatów 1. generacji w trybie tylko uwierzytelnienia (zob. dodatek 11 część A).
SM-C-MAC-G1	Polecenie APDU musi być stosowane z bezpieczną wymianą komunikatów 1. generacji w trybie tylko uwierzytelnienia (zob. dodatek 11 część A).
SM-R-ENC-G1	Odpowiedź APDU musi być stosowana z bezpieczną wymianą komunikatów 1. generacji w trybie szyfrowania (zob. dodatek 11 część A), tzn. bez zwracania kodu uwierzytelnienia wiadomości.
SM-R-ENC-MAC-G1	Odpowiedź APDU musi być stosowana z bezpieczną wymianą komunikatów 1. generacji w trybie szyfrowania i uwierzytelnienia (zob. dodatek 11 część A).
SM-MAC-G2	Polecenie i odpowiedź APDU muszą być stosowane z bezpieczną wymianą komunikatów 2. generacji w trybie tylko uwierzytelnienia (zob. dodatek 11 część A).
SM-C-MAC-G2	Polecenie APDU musi być stosowane z bezpieczną wymianą komunikatów 2. generacji w trybie tylko uwierzytelnienia (zob. dodatek 11 część A).
SM-R-ENC-MAC-G2	Odpowiedź APDU musi być stosowana z bezpieczną wymianą komunikatów 2. generacji w trybie szyfrowania i uwierzytelnienia (zob. dodatek 11 część A).

TCS_24 Przedmiotowe warunki zabezpieczenia mogą być powiązane ze sobą w następujący sposób:

AND: muszą zostać spełnione wszystkie warunki zabezpieczenia

OR: musi zostać spełniony przynajmniej jeden warunek zabezpieczenia

Zasady dostępu dla systemu plików, tzn. polecenia SELECT, READ BINARY oraz UPDATE BINARY, zostały określone w rozdziale 4. Zasady dostępu dla pozostałych poleceń zostały określone w poniższych tabelach.

TCS_25 W przypadku aplikacji DF Tachograph G1 zastosowanie mają następujące zasady dostępu:

Polecenie	Karta kierowcy	Karta warsztatowa	Karta kontrolna	Karta firmowa
External Authenticate				
— dla uwierzytelnienia 1. generacji	ALW	ALW	ALW	ALW
— dla uwierzytelnienia 2. generacji	ALW	PWD	ALW	ALW
Internal Authenticate	ALW	PWD	ALW	ALW
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	nie dotyczy	nie dotyczy	nie dotyczy	nie dotyczy
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	nie dotyczy	nie dotyczy
PSO: Hash	nie dotyczy	nie dotyczy	ALW	nie dotyczy
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	nie dotyczy	nie dotyczy
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	nie dotyczy	nie dotyczy	ALW	nie dotyczy
Verify	nie dotyczy	ALW	nie dotyczy	nie dotyczy

TCS_26 W przypadku aplikacji DF Tachograph_G2 zastosowanie mają następujące zasady dostępu:

Polecenie	Karta kierowcy	Karta warsztatowa	Karta kontrolna	Karta firmowa
External Authenticate				
— dla uwierzytelnienia 1. generacji	nie dotyczy	nie dotyczy	nie dotyczy	nie dotyczy
— dla uwierzytelnienia 2. generacji	ALW	PWD	ALW	ALW
Internal Authenticate	nie dotyczy	nie dotyczy	nie dotyczy	nie dotyczy

Polecenie	Karta kierowcy	Karta warsztatowa	Karta kontrolna	Karta firmowa
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	nie dotyczy	ALW	ALW	nie dotyczy
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	nie dotyczy	nie dotyczy
PSO: Hash	nie dotyczy	nie dotyczy	ALW	nie dotyczy
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	nie dotyczy	nie dotyczy
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	nie dotyczy	nie dotyczy	ALW	nie dotyczy
Verify	nie dotyczy	ALW	nie dotyczy	nie dotyczy

TCS_27 W przypadku MF zastosowanie mają następujące zasady dostępu:

Polecenie	Karta kierowcy	Karta warsztatowa	Karta kontrolna	Karta firmowa
External Authenticate				
— dla uwierzytelnienia 1. generacji	nie dotyczy	nie dotyczy	nie dotyczy	nie dotyczy
— dla uwierzytelnienia 2. generacji	ALW	PWD	ALW	ALW
Internal Authenticate	nie dotyczy	nie dotyczy	nie dotyczy	nie dotyczy
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	nie dotyczy	nie dotyczy	nie dotyczy	nie dotyczy

Polecenie	Karta kierowcy	Karta warsztatowa	Karta kontrolna	Karta firmowa
PSO: Compute Digital Signature	nie dotyczy	nie dotyczy	nie dotyczy	nie dotyczy
PSO: Hash	nie dotyczy	nie dotyczy	nie dotyczy	nie dotyczy
PSO: Hash of File	nie dotyczy	nie dotyczy	nie dotyczy	nie dotyczy
PSO: Verify Certificate	ALW	ALW	ALW	ALW
Verify	nie dotyczy	ALW	nie dotyczy	nie dotyczy

TCS_28 Karta do tachografu może, ale nie musi przyjmować poleceń z wyższego poziomu zabezpieczenia niż poziom określony w warunkach zabezpieczenia. Tzn. jeżeli warunkiem zabezpieczenia jest ALW (lub PLAIN-C), karta może przyjąć polecenie z bezpieczną wymianą komunikatów (w trybie szyfrowania lub uwierzytelnienia). Jeżeli warunek zabezpieczenia wymaga bezpiecznej wymiany komunikatów w trybie uwierzytelnienia, karta do tachografu może przyjąć polecenie z bezpieczną wymianą komunikatów tej samej generacji w trybie uwierzytelnienia i szyfrowania.

Uwaga: Opisy poleceń dostarczają więcej informacji na temat obsługi poleceń dla poszczególnych typów kart do tachografów oraz poszczególnych DF.

3.4. **Przegląd poleceń i kodów błędów**

Polecenia i organizacja pliku wynikają z normy ISO/IEC 7816-4 i spełniają jej wymagania.

W tej sekcji opisano poniższe pary polecenie-odpowiedź dla APDU. Warianty poleceń, które są obsługiwane przez aplikacje 1. i 2. generacji, zostały określone w odpowiednich opisach poleceń.

Polecenie	INS
SELECT	‘A4h’
READ BINARY	‘B0h’, ‘B1h’
UPDATE BINARY	‘D6h’, ‘D7h’
GET CHALLENGE	‘84h’
VERIFY	‘20h’
GET RESPONSE	‘C0h’
PERFORM SECURITY OPERATION	‘2Ah’
— VERIFY CERTIFICATE	
— COMPUTE DIGITAL SIGNATURE	
— VERIFY DIGITAL SIGNATURE	
— HASH	
— PERFORM HASH OF FILE	
— PROCESS DSRC MESSAGE	

Polecenie	INS
INTERNAL AUTHENTICATE	'88h'
EXTERNAL AUTHENTICATE	'82h'
MANAGE SECURITY ENVIRONMENT	'22h'
— SET DIGITAL SIGNATURE TEMPLATE	
— SET AUTHENTICATION TEMPLATE	
GENERAL AUTHENTICATE	'86h'

TCS_29 Słowa stanu SW1 i SW2 są zwracane w komunikacie odpowiedzi i oznaczają stan przetwarzania polecenia.

SW1	SW2	Znaczenie
90	00	Normalne przetwarzanie.
61	XX	Normalne przetwarzanie. XX = liczba dostępnych bajtów odpowiedzi.
62	81	Przetwarzanie ostrzeżenia. Część zwracanych danych może być uszkodzona
63	00	Nieudane uwierzytelnienie (ostrzeżenie)
63	CX	Nieprawidłowe CHV (PIN). 'X' oznacza licznik pozostałych prób
64	00	Błąd wykonania – Stan pamięci nieulotnej bez zmian. Błąd integralności.
65	00	Błąd wykonania – Stan pamięci nieulotnej zmieniony
65	81	Błąd wykonania – Stan pamięci nieulotnej zmieniony – Uszkodzona pamięć
66	88	Błąd zabezpieczenia: nieprawidłowa kryptograficzna suma kontrolna (w czasie bezpiecznej wymiany komunikatów) lub nieprawidłowy certyfikat (w czasie weryfikacji certyfikatu) lub nieprawidłowy kryptogram (w czasie zewnętrznego uwierzytelnienia) lub nieprawidłowy podpis (w czasie weryfikacji podpisu)
67	00	Nieprawidłowa długość (nieprawidłowe Lc lub Le)
68	82	Bezpieczna wymiana komunikatów nieobsługiwana
68	83	Oczekiwane ostatnie polecenie łańcucha
69	00	Niedozwolone polecenie (brak dostępnej odpowiedzi w T=0)
69	82	Niespełniony stan zabezpieczenia.
69	83	Metoda uwierzytelnienia zablokowana.
69	85	Warunki użycia niespełnione.
69	86	Polecenie niedozwolone (brak bieżącego EF).

SW1	SW2	Znaczenie
69	87	Brak oczekiwanych obiektów danych w bezpiecznej wymianie komunikatów
69	88	Nieprawidłowe obiekty danych w bezpiecznej wymianie komunikatów
6A	80	Nieprawidłowe parametry w polu danych
6A	82	Nie znaleziono pliku.
6A	86	Nieprawidłowe parametry P1-P2.
6A	88	Nie znaleziono powołanych danych.
6 B	00	Nieprawidłowe parametry (przesunięcie poza EF).
6C	XX	Nieprawidłowa długość, SW2 wskazuje dokładną długość. Pole danych nie jest zwracane.
6D	00	Kod instrukcji nieobsługiwany lub nieważny.
6E	00	Klasa nieobsługiwana.
6F	00	Inne błędy kontroli

TCS_30 W przypadku gdy w jednym poleceniu APDU spełniony jest więcej niż jeden warunek wystąpienia błędu, karta może odesłać dowolny z odpowiednich słów stanu.

3.5. **Opisy poleceń**

W tym rozdziale opisano obowiązkowe polecenia dla kart do tachografów.

Dodatkowe szczegółowe informacje dotyczące stosowanych czynności kryptograficznych zamieszczono w dodatku 11 Wspólne mechanizmy zabezpieczenia dla tachografów 1. generacji i 2. generacji.

Wszystkie polecenia opisane są niezależnie od używanego protokołu (T=0 lub T=1). Bajty CLA, INS, P1, P2, Lc i Le w APDU są zawsze wskazywane. Jeżeli Lc lub Le nie jest potrzebny dla opisywanego polecenia, związane z nimi długość, wartość i opis są puste.

TCS_31 Jeżeli żądane są oba bajty długości (Lc i Le), opisywane polecenie musi być podzielone na dwie części, jeśli IFD używa protokołu T=0: IFD wysyła to polecenie z P3=Lc + dane, a następnie wysyła polecenie GET RESPONSE (zob. pkt 3.5.6) z P3=Le.

TCS_32 Jeżeli żądane są oba bajty długości i Le=0 (bezpieczna wymiana komunikatów):

— gdy używany jest protokół T=1, karta odpowiada na Le=0, wysyłając wszystkie dostępne dane wyjściowe;

— gdy używany jest protokół T=0, IFD wysyła pierwsze polecenie z P3=Lc + dane, karta odpowiada (na to niejawne Le=0) bajtami stanu '**61La**', gdzie La jest liczbą dostępnych bajtów odpowiedzi. Następnie IFD generuje polecenie GET RESPONSE z P3=La w celu odczytania danych.

TCS_33 Karta do tachografu może opcjonalnie obsługiwać pola o rozszerzonej długości zgodnie z normą ISO/IEC 7816-4. Karta do tachografu, która obsługuje pola o rozszerzonej długości, musi:

— wskazywać możliwość obsługi pól o rozszerzonej długości w ATR;

— zapewniać obsługiwane pojemności bufora za pomocą informacji o rozszerzonej długości w EF ATR/INFO, zob. TCS_146;

— wskazywać, czy obsługuje pola o rozszerzonej długości dla T = 1 lub T = 0 w EF Extended Length, zob. TCS_147.

— obsługiwać pola o rozszerzonej długości dla aplikacji tachograficznej 1. i 2. generacji.

Uwagi:

Wszystkie polecenia zostały określone dla pól o krótkiej długości. Stosowanie APDU o rozszerzonej długości wynika z ISO/IEC 7816-4.

Polecenia są zasadniczo określone dla trybu zwykłego, tj. bez bezpiecznej wymiany komunikatów, ponieważ warstwa bezpiecznej wymiany komunikatów została określona w dodatku 11. Z zasad dostępu dla polecenia wynika, czy polecenie wspiera bezpieczną wymianę komunikatów, a także – czy polecenie wspiera bezpieczną wymianę komunikatów 1. generacji lub 2. generacji. Niektóre warianty poleceń opisano z bezpieczną wymianą komunikatów, aby zilustrować stosowanie bezpiecznej wymiany komunikatów.

TCS_34 VU wykonuje pełny protokół 2. generacji wzajemnego uwierzytelnienia VU – karta dla sesji, łącznie z weryfikacją certyfikatu (jeżeli jest to wymagane), w DF Tachograph, w DF Tachograph_G2 lub w MF.

3.5.1 *SELECT*

Polecenie to jest zgodne z normą ISO/IEC 7816-4, ale jego zastosowanie jest ograniczone w porównaniu z poleceniem zdefiniowanym w tej normie.

Polecenia SELECT używa się:

— do wybierania aplikacji DF (musi być używany wybór przez nazwę);

— do wybierania pliku elementarnego odpowiadającego przekazanemu ID pliku.

3.5.1.1 Wybór przez nazwę (AID)

Polecenie to pozwala wybrać aplikację DF na karcie.

TCS_35 Polecenie to można wykonywać z dowolnego miejsca w strukturze pliku (po ATR lub w dowolnym momencie).

TCS_36 Wybór aplikacji powoduje przywrócenie bieżącego stanu środowiska zabezpieczeń do stanu wyjściowego. Po wybraniu aplikacji żaden bieżący klucz publiczny nie jest już wybierany. Warunek dostępu EXT-AUT-G1 także zostaje utracony. Jeżeli polecenie zostało wykonane bez bezpiecznej wymiany komunikatów, wcześniejsze klucze sesji bezpiecznej wymiany komunikatów nie są już dostępne.

TCS_37 **Komunikat polecenia**

Bajt	Długość	Wartość	Opis
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	Wybór przez nazwę (AID)
P2	1	'0Ch'	brak oczekiwanej odpowiedzi
Lc	1	'NNh'	liczba bajtów wysłanych do karty (długość AID): '06h' dla aplikacji tachograficznej
#6-#(5+NN)	NN	'XX..XXh'	AID: 'FF 54 41 43 48 4F' dla aplikacji tachograficznej 1. generacji AID: 'FF 53 4D 52 44 54' dla aplikacji tachograficznej 2. generacji

Dla polecenia SELECT nie jest potrzebna żadna odpowiedź (brak Le w T=1, bądź nie ma żądania odpowiedzi w T=0).

TCS_38 **Komunikat odpowiedzi (brak żądania odpowiedzi)**

Bajt	Długość	Wartość	Opis
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

— Jeżeli polecenie zostało pomyślnie wykonane, karta zwraca '**9000**'.

— Jeżeli nie znaleziono aplikacji wyszczególnionej przez AID, zwróconym stanem przetwarzania jest '**6A82**'.

— W T=1, jeżeli jest bajt Le, zwróconym stanem jest **'6700'**.

— W T=0, jeżeli po poleceniu SELECT wymaga się odpowiedzi, zwróconym stanem jest **'6900'**.

— Jeżeli wybrana aplikacja uznana jest za uszkodzoną (znaleziony błąd integralności w atrybutach pliku), zwróconym stanem przetwarzania jest '**6400**' lub '**6581**'.

3.5.1.2 Wybór pliku elementarnego przy pomocy identyfikatora pliku

TCS_39 **Komunikat polecenia**

TCS_40 Karta do tachografu musi obsługiwać bezpieczną wymianę komunikatów 2. generacji, jak określono w dodatku 11 część B dla tego wariantu polecenia.

Bajt	Długość	Wartość	Opis
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	wybór EF pod bieżącym DF
P2	1	'0Ch'	brak oczekiwanej odpowiedzi
Lc	1	'02h'	liczba bajtów wysłanych do karty
#6-#7	2	'XXXXh'	identyfikator pliku

Dla polecenia SELECT nie jest potrzebna żadna odpowiedź (brak Le w T=1, bądź nie ma żądania odpowiedzi w T=0).

TCS_41 **Komunikat odpowiedzi (brak żądania odpowiedzi)**

Bajt	Długość	Wartość	Opis
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

— Jeżeli polecenie zostało pomyślnie wykonane, karta zwraca '**9000**'.

— Jeżeli nie znaleziono pliku odpowiadającego identyfikatorowi pliku, zwróconym stanem przetwarzania jest '**6A82**'.

— W T=1, jeżeli jest bajt Le, zwróconym stanem jest **'6700'**.

— W T=0, jeżeli po poleceniu SELECT wymaga się odpowiedzi, zwróconym stanem jest **'6900'**.

— Jeżeli wybrany plik uznany jest za uszkodzony (znaleziony błąd integralności w atrybutach pliku), zwróconym stanem przetwarzania jest '**6400**' lub '**6581**'.

3.5.2 *READ BINARY*

Polecenie to jest zgodne z normą ISO/IEC 7816-4, ale jego zastosowanie jest ograniczone w porównaniu z poleceniem zdefiniowanym w tej normie.

Polecenie READ BINARY służy do odczytu danych z przezroczystego pliku.

Odpowiedź karty obejmuje zwrot odczytanych danych, opcjonalnie obudowane w strukturę bezpiecznej wymiany komunikatów.

3.5.2.1 Polecenie z przesunięciem w P1-P2

Polecenie to umożliwia IFD odczyt danych z aktualnie wybranego EF bez bezpiecznej wymiany komunikatów.

Uwaga: Tego polecenia bez bezpiecznej wymiany komunikatów można używać tylko do odczytu pliku, który wspiera warunek zabezpieczenia ALW dla trybu dostępu do odczytu.

TCS_42 **Komunikat polecenia**

Bajt	Długość	Wartość	Opis
CLA	1	'00h'	
INS	1	'B0h'	Odczyt binarny
P1	1	'XXh'	Przesunięcie w bajtach od początku pliku: bajt najbardziej znaczący
P2	1	'XXh'	Przesunięcie w bajtach od początku pliku: bajt najmniej znaczący
Le	1	'XXh'	Długość oczekiwanych danych. Liczba bajtów do odczytu.

Uwaga: bit 8 w P1 musi być ustawiony na 0.

TCS_43 **Komunikat odpowiedzi**

Bajt	Długość	Wartość	Opis
#1-#X	X	'XX..XXh'	Odczyt danych
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

— Jeżeli polecenie zostało pomyślnie wykonane, karta zwraca '**9000**'.

— Jeżeli nie wybrano EF, zwróconym stanem przetwarzania jest **'6986'**.

— Jeżeli warunki zabezpieczenia wybranego pliku nie są spełnione, polecenie zostaje przerwane z '**6982**'.

— Jeżeli przesunięcie nie jest zgodne z wielkością EF (przesunięcie > wielkość EF), zwróconym stanem przetwarzania jest **'6B00'**.

— Jeżeli wielkość danych do odczytu nie jest zgodna z wielkością EF (przesunięcie + Le > wielkość EF), zwróconym stanem przetwarzania jest **'6700'** lub **'6Cxx'**, gdzie „xx" wskazuje dokładną długość.

— Jeżeli błąd integralności zostaje wykryty w atrybutach pliku, karta uznaje, że plik jest uszkodzony i nienaprawialny, a zwróconym stanem przetwarzania jest **'6400'** lub **'6581'**.

— Jeżeli błąd integralności zostaje wykryty w zgromadzonych danych, karta zwraca żądane dane, a zwróconym stanem przetwarzania jest **'6281'**.

3.5.2.1.1 Polecenie z bezpieczną wymianą komunikatów (przykłady)

Polecenie to umożliwia IFD odczyt danych z bieżąco wybranego EF z bezpieczną wymianą komunikatów w celu zweryfikowania integralności odebranych danych oraz ochrony poufności danych, jeżeli zastosowanie ma warunek zabezpieczenia SM-R-ENC-MAC-G1 (1. generacja) lub SM-R-ENC-MAC-G2 (2. generacja).

TCS_44 **Komunikat polecenia**

Bajt	Długość	Wartość	Opis
CLA	1	'0Ch'	Żądana bezpieczna wymiana komunikatów
INS	1	'B0h'	Odczyt binarny
P1	1	'XXh'	P1 (przesunięcie w bajtach od początku pliku): bajt najbardziej znaczący
P2	1	'XXh'	P2 (przesunięcie w bajtach od początku pliku): bajt najmniej znaczący
Lc	1	'XXh'	Długość danych wejściowych dla bezpiecznej wymiany komunikatów
#6	1	'97h'	T_{LE}: znacznik specyfikacji oczekiwanej długości
#7	1	'01h'	L_{LE}: długość oczekiwanej długości
#8	1	'NNh'	Specyfikacja oczekiwanej długości (początkowy Le): liczba bajtów do odczytu
#9	1	'8Eh'	T_{CC}: znacznik kryptograficznej sumy kontrolnej
#10	1	'XXh'	L_{CC}: długość znajdującej się dalej kryptograficznej sumy kontrolnej '04h' dla bezpiecznej wymiany komunikatów 1. generacji (zob. dodatek 11 część A) '08h', '0Ch' lub '10h', w zależności od długości klucza AES, dla bezpiecznej wymiany komunikatów 2. generacji (zob. dodatek 11 część B)
#11-#(10+L)	L	'XX..XXh'	Kryptograficzna suma kontrolna
Le	1	'00h'	zgodnie ze specyfikacją w normie ISO/IEC 7816-4

TCS_45 **Komunikat odpowiedzi, jeżeli SM-R-ENC-MAC-G1 (1. generacja) / SM-R-ENC-MAC-G2 (2. generacja) nie są wymagane oraz jeżeli format wejściowy bezpiecznej wymiany komunikatów jest prawidłowy:**

Bajt	Długość	Wartość	Opis
#1	1	'99h'	Znacznik stanu przetwarzania (SW1-SW2) – opcjonalny dla bezpiecznej wymiany komunikatów 1. generacji
#2	1	'02h'	Długość stanu przetwarzania
#3 – #4	2	'XX XXh'	Stan przetwarzania niechronionej odpowiedzi APDU
#5	1	'81h'	T_{PV}: znacznik wartości danych odkrytych
#6	L	'NNh' lub '81 NNh'	L_{PV}: długość zwracanych danych (= początkowemu Le). L ma 2 bajty, jeżeli L_{PV}>127 bajtów

Bajt	Długość	Wartość	Opis
#(6+L)-#(5+L+NN)	NN	'XX..XXh'	Wartość danych odkrytych
#(6+L+NN)	1	'8Eh'	T_{CC}: znacznik kryptograficznej sumy kontrolnej
#(7+L+NN)	1	'XXh'	L_{CC}: długość znajdującej się dalej kryptograficznej sumy kontrolnej '04h' dla bezpiecznej wymiany komunikatów 1. generacji (zob. dodatek 11 część A) '08h', '0Ch' lub '10h', w zależności od długości klucza AES, dla bezpiecznej wymiany komunikatów 2. generacji (zob. dodatek 11 część B)
#(8+L+NN)-#(7+M+L+NN)	M	'XX..XXh'	Kryptograficzna suma kontrolna
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

TCS_46 **Komunikat odpowiedzi, jeżeli SM-R-ENC-MAC-G1 (1. generacja) / SM-R-ENC-MAC-G2 (2. generacja) są wymagane oraz jeżeli format wejściowy bezpiecznej wymiany komunikatów jest prawidłowy:**

Bajt	Długość	Wartość	Opis
#1	1	'87h'	$T_{PI\ CG}$: znacznik zaszyfrowanych danych (kryptogram)
#2	L	'MMh' lub '81 MMh'	$L_{PI\ CG}$: długość zwracanych zaszyfrowanych danych (różna od początkowego Le z polecenia, ze względu na wypełnienie) L ma 2 bajty, jeżeli $L_{PI\ CG}$ > 127 bajtów
#(2+L)-#(1+L+MM)	MM	'01XX..XXh'	dane szyfrowane: wskaźnik wypełnienia i kryptogram
#(2+L+MM)	1	'99h'	Znacznik stanu przetwarzania (SW1-SW2) – opcjonalny dla bezpiecznej wymiany komunikatów 1. generacji
#(3+L+MM)	1	'02h'	Długość stanu przetwarzania
#(4+L+MM) – #(5+L+MM)	2	'XX XXh'	Stan przetwarzania niechronionej odpowiedzi APDU
#(6+L+MM)	1	'8Eh'	T_{CC}: znacznik kryptograficznej sumy kontrolnej
#(7+L+MM)	1	'XXh'	L_{CC}: długość znajdującej się dalej kryptograficznej sumy kontrolnej '04h' dla bezpiecznej wymiany komunikatów 1. generacji (zob. dodatek 11 część A) '08h', '0Ch' lub '10h', w zależności od długości klucza AES, dla bezpiecznej wymiany komunikatów 2. generacji (zob. dodatek 11 część B)
#(8+L+MM)-#(7+N+L+MM)	N	'XX..XXh'	Kryptograficzna suma kontrolna
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

Polecenie READ BINARY może zwracać stany regularnego przetwarzania, wymienione w TCS_43 pod znacznikiem '99h', opisane w TCS_59, przy użyciu struktury odpowiedzi bezpiecznej wymiany komunikatów.

Ponadto mogą wystąpić niektóre błędy, swoiście dotyczące bezpiecznej wymiany komunikatów. W takim przypadku zwracany jest po prostu stan przetwarzania bez struktury bezpiecznej wymiany komunikatów:

TCS_47 **Komunikat odpowiedzi przy nieprawidłowym formacie wejściowym bezpiecznej wymiany komunikatów**

Bajt	Długość	Wartość	Opis
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

— Jeżeli klucz bieżącej sesji nie jest dostępny, zwracany jest stan przetwarzania **'6A88'**. Zdarza się to w sytuacji, gdy klucz sesyjny nie jest już generowany, albo w sytuacji, gdy wygaśnie już ważność kluczy sesyjnych (w tym przypadku IFD musi powtórnie uruchomić proces wzajemnego uwierzytelnienia w celu utworzenia nowego klucza sesyjnego).

— Jeżeli w formacie bezpiecznej wymiany komunikatów brakuje pewnych oczekiwanych obiektów (określonych powyżej), zwracany jest stan przetwarzania **'6987'**: ten błąd ma miejsce, jeżeli brakuje oczekiwanego znacznika lub jeżeli treść polecenia nie jest prawidłowo skonstruowana.

— Jeżeli pewne obiekty danych są nieprawidłowe, zwróconym stanem przetwarzania jest **'6988'**: ten błąd ma miejsce, jeżeli obecne są wszystkie wymagane znaczniki, ale niektóre długości różnią się od oczekiwanych.

— Jeżeli weryfikacja kryptograficznej sumy kontrolnej wykaże niezgodność, zwróconym stanem przetwarzania jest **'6688'**.

3.5.2.2 Polecenie z krótkimi identyfikatorem EF (Elementary File)

Ten wariant polecenia umożliwia IFD wybór EF przy pomocy krótkiego identyfikatora EF oraz odczyt danych z tego EF.

TCS_48 Karta do tachografu obsługuje ten wariant polecenia dla wszystkich plików elementarnych z określonym krótkim identyfikatorem EF. Przedmiotowe krótkie identyfikatory EF zostały określone w rozdziale 4.

TCS_49 **Komunikat polecenia**

Bajt	Długość	Wartość	Opis
CLA	1	'00h'	
INS	1	'B0h'	Odczyt binarny
P1	1	'XXh'	Bit 8 ustawiany jest na 1. Bity 7 i 6 ustawiane są na 00. Bity 5 – 1 kodują krótki identyfikator EF odpowiedniego EF.
P2	1	'XXh'	Koduje przesunięcie od 0 do 255 bajtów w EF przywołanym przez P1.
Le	1	'XXh'	Długość oczekiwanych danych. Liczba bajtów do odczytu.

Uwaga: Krótkie identyfikatory EF używane na potrzeby aplikacji tachograficznej 2. generacji zostały określone w rozdziale 4.

Jeżeli P1 koduje krótki identyfikator EF, a polecenie zostało pomyślnie wykonane, ustalone EF staje się bieżąco wybranym EF (bieżący EF).

TCS_50 **Komunikat odpowiedzi**

Bajt	Długość	Wartość	Opis
#1-#L	L	'XX..XXh'	Odczyt danych
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

— Jeżeli polecenie zostało pomyślnie wykonane, karta zwraca '**9000**'.

— Jeżeli nie znaleziono pliku odpowiadającego krótkiemu identyfikatorowi EF, zwróconym stanem przetwarzania jest **'6A82'**.

— Jeżeli warunki zabezpieczenia wybranego pliku nie są spełnione, polecenie zostaje przerwane z '**6982**'.

— Jeżeli przesunięcie nie jest zgodne z wielkością EF (przesunięcie > wielkość EF), zwróconym stanem przetwarzania jest **'6B00'**.

— Jeżeli wielkość danych do odczytu nie jest zgodna z wielkością EF (przesunięcie + Le > wielkość EF), zwróconym stanem przetwarzania jest **'6700'** lub **'6Cxx'**, gdzie „xx" wskazuje dokładną długość.

— Jeżeli błąd integralności zostaje wykryty w atrybutach pliku, karta uznaje, że plik jest uszkodzony i nienaprawialny, a zwróconym stanem przetwarzania jest **'6400'** lub **'6581'**.

— Jeżeli błąd integralności zostaje wykryty w zgromadzonych danych, karta zwraca żądane dane, a zwróconym stanem przetwarzania jest **'6281'**.

3.5.2.3 Polecenie z nieparzystym bajtem instrukcji

Ten wariant polecenia umożliwia IFD odczyt danych z EF, który ma 32 768 bajtów lub więcej.

TCS_51 Karta do tachografu obsługująca EF, który ma 32 768 bajtów lub więcej, musi obsługiwać ten wariant polecenia dla takich EF. Karta do tachografu może, ale nie musi obsługiwać tego wariantu polecenia dla innych EF, z wyjątkiem EF Sensor_Installation_Data (zob. TCS_156 i TCS_160).

TCS_52 **Komunikat polecenia**

Bajt	Długość	Wartość	Opis
CLA	1	'00h'	
INS	1	'B1h'	Odczyt binarny
P1	1	'00h'	bieżący EF
P2	1	'00h'	
Lc	1	'NNh'	Lc długość przesuniętego obiektu danych.
#6-#(5+NN)	NN	'XX..XXh'	przesunięty obiekt danych: znacznik '54h' długość '01h' lub '02h' wartość przesunięcie
Le	1	'XXh'	Liczba bajtów do odczytu.

IFD koduje długość przesuniętego obiektu danych z możliwie najmniejszą liczbą oktetów, tzn. przy pomocy bajtu długości '01h' IFD koduje przesunięcie od 0 do 255 bajtów, a przy pomocy bajtu długości '02h' koduje przesunięcie od '256' do '65 535' bajtów.

TCS_53 **Komunikat odpowiedzi**

Bajt	Długość	Wartość	Opis
#1-#L	L	'XX..XXh'	Odczytane dane zapakowane do nieokreślonego obiektu danych ze znacznikiem '53h'.
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

— Jeżeli polecenie zostało pomyślnie wykonane, karta zwraca '**9000**'.

— Jeżeli nie wybrano EF, zwróconym stanem przetwarzania jest **'6986'**.

— Jeżeli warunki zabezpieczenia wybranego pliku nie są spełnione, polecenie zostaje przerwane z **'6982'**.

— Jeżeli przesunięcie nie jest zgodne z wielkością EF (przesunięcie > wielkość EF), zwróconym stanem przetwarzania jest **'6B00'**.

— Jeżeli wielkość danych do odczytu nie jest zgodna z wielkością EF (przesunięcie + Le > wielkość EF), zwróconym stanem przetwarzania jest **'6700'** lub '**6Cxx**', gdzie „xx" wskazuje dokładną długość.

— Jeżeli błąd integralności zostaje wykryty w atrybutach pliku, karta uznaje, że plik jest uszkodzony i nienaprawialny, a zwróconym stanem przetwarzania jest '**6400**' lub '**6581**'.

— Jeżeli błąd integralności zostaje wykryty w zgromadzonych danych, karta zwraca żądane dane, a zwróconym stanem przetwarzania jest '**6281**'.

3.5.2.3.1 Polecenie z bezpieczną wymianą komunikatów (przykład)

Poniższy przykład ilustruje stosowanie bezpiecznej wymiany komunikatów, jeżeli zastosowanie ma warunek zabezpieczenia SM-MAC-G2.

TCS_54 Komunikat polecenia

Bajt	Długość	Wartość	Opis
CLA	1	'0Ch'	Żądana bezpieczna wymiana komunikatów
INS	1	'B1h'	Odczyt binarny
P1	1	'00h'	bieżący EF
P2	1	'00h'	
Lc	1	'XXh'	długość chronionego pola danych
#6	1	'B3h'	znacznik wartości danych odkrytych kodowanych w BER-TLV
#7	1	'NNh'	L_{PV}: długość przesyłanych danych
#(8)-#(7+NN)	NN	'XX..XXh'	dane odkryte kodowane w BER-TLV, tj. przesunięty obiekt danych ze znacznikiem '54'
#(8+NN)	1	'97h'	T_{LE}: znacznik specyfikacji oczekiwanej długości
#(9+NN)	1	'01h'	L_{LE}: długość oczekiwanej długości
#(10+NN)	1	'XXh'	specyfikacja oczekiwanej długości (początkowy Le): liczba bajtów do odczytu
#(11+NN)	1	'8Eh'	T_{CC}: znacznik kryptograficznej sumy kontrolnej
#(12+NN)	1	'XXh'	L_{CC}: długość znajdującej się dalej kryptograficznej sumy kontrolnej '08h', '0Ch' lub '10h', w zależności od długości klucza AES, dla bezpiecznej wymiany komunikatów 2. generacji (zob. dodatek 11 część B)
#(13+NN)-#(12+M+NN)	M	'XX..XXh'	Kryptograficzna suma kontrolna
Le	1	'00h'	zgodnie ze specyfikacją w normie ISO/IEC 7816-4

TCS_55 komunikat odpowiedzi, jeżeli polecenie zostało pomyślnie wykonane

Bajt	Długość	Wartość	Opis
#1	1	'B3h'	odkryte dane kodowane w BER-TLV
#2	L	'NNh' lub '81 NNh'	L_{PV}: długość zwracanych danych (= początkowemu Le). L ma 2 bajty, jeżeli L_{PV}>127 bajtów
#(2+L)-#(1+L+NN)	NN	'XX..XXh'	Wartość odkrytych danych kodowanych w BER-TLV, tj. odczytane dane zapakowane do nieokreślonego obiektu danych ze znacznikiem '53h'.
#(2+L+NN)	1	'99h'	Stan przetwarzania niechronionej odpowiedzi APDU
#(3+L+NN)	1	'02h'	Długość stanu przetwarzania
#(4+L+NN) – #(5+L+NN)	2	'XX XXh'	Stan przetwarzania niechronionej odpowiedzi APDU
#(6+L+NN)	1	'8Eh'	T_{CC}: znacznik kryptograficznej sumy kontrolnej
#(7+L+NN)	1	'XXh'	L_{CC}: długość znajdującej się dalej kryptograficznej sumy kontrolnej '08h', '0Ch' lub '10h', w zależności od długości klucza AES, dla bezpiecznej wymiany komunikatów 2. generacji (zob. dodatek 11 część B)
#(8+L+NN)-#(7+M+L+NN)	M	'XX..XXh'	Kryptograficzna suma kontrolna
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

3.5.3 *UPDATE BINARY*

Polecenie to jest zgodne z normą ISO/IEC 7816-4, ale jego zastosowanie jest ograniczone w porównaniu z poleceniem zdefiniowanym w tej normie.

Komunikat polecenia UPDATE BINARY inicjuje aktualizację (kasowanie + zapis) bitów już znajdujących się w binarnym EF, zastępując je bitami podanymi w poleceniu APDU.

3.5.3.1 Polecenie z przesunięciem w P1-P2

Polecenie to umożliwia IFD zapis danych do bieżąco wybranego EF, bez sprawdzenia przez kartę integralności otrzymanych danych.

Uwaga: Tego polecenia bez bezpiecznej wymiany komunikatów można używać tylko do aktualizacji pliku, który wspiera warunek zabezpieczenia ALW dla trybu dostępu do aktualizacji.

TCS_56 **Komunikat polecenia**

Bajt	Długość	Wartość	Opis
CLA	1	'00h'	
INS	1	'D6h'	Aktualizacja binarna licznika

Bajt	Długość	Wartość	Opis
P1	1	'XXh'	Przesunięcie w bajtach od początku pliku: bajt najbardziej znaczący
P2	1	'XXh'	Przesunięcie w bajtach od początku pliku: bajt najmniej znaczący
Lc	1	'NNh'	Lc długość aktualizowanych danych. Liczba zapisywanych bajtów.
#6-#(5+NN)	NN	'XX..XXh'	zapisywane dane

Uwaga: bit 8 w P1 musi być ustawiony na 0.

TCS_57 **Komunikat odpowiedzi**

Bajt	Długość	Wartość	Opis
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

— Jeżeli polecenie zostało pomyślnie wykonane, karta zwraca '**9000**'.

— Jeżeli nie wybrano EF, zwróconym stanem przetwarzania jest **'6986'**.

— Jeżeli warunki zabezpieczenia wybranego pliku nie są spełnione, polecenie zostaje przerwane z '**6982**'.

— Jeżeli przesunięcie nie jest zgodne z wielkością EF (przesunięcie > wielkość EF), zwróconym stanem przetwarzania jest **'6B00'**.

— Jeżeli wielkość danych, które mają być zapisane, nie jest zgodna z wielkością EF (przesunięcie + Lc > wielkość EF), zwróconym stanem przetwarzania jest **'6700'**.

— Jeżeli błąd integralności zostaje wykryty w atrybutach pliku, karta uznaje, że plik jest uszkodzony i nienaprawialny, a zwróconym stanem przetwarzania jest **'6400'** lub **'6500'**.

— Jeżeli zapis nie jest wykonany pomyślnie, zwróconym stanem przetwarzania jest **'6581'**.

3.5.3.1.1 Polecenie z bezpieczną wymianą komunikatów (przykłady)

Polecenie to umożliwia IFD zapis danych do bieżąco wybranego EF, ze sprawdzeniem przez kartę integralności otrzymanych danych. Gdy nie jest wymagana poufność, dane nie są szyfrowane.

TCS_58 **Komunikat polecenia**

Bajt	Długość	Wartość	Opis
CLA	1	'0Ch'	Żądana bezpieczna wymiana komunikatów
INS	1	'D6h'	Aktualizacja binarna licznika
P1	1	'XXh'	Przesunięcie w bajtach od początku pliku: bajt najbardziej znaczący
P2	1	'XXh'	Przesunięcie w bajtach od początku pliku: bajt najmniej znaczący
Lc	1	'XXh'	długość chronionego pola danych

Bajt	Długość	Wartość	Opis
#6	1	'81h'	T_{PV}: znacznik wartości danych odkrytych
#7	L	'NNh' lub '81 NNh'	L_{PV}: długość transmitowanych danych. L ma 2 bajty, jeżeli L_{PV} >127 bajtów.
#(7 + L)-#(6 + L + NN)	NN	'XX..XXh'	wartość odkrytych danych (dane, które mają być zapisane)
#(7 + L + NN)	1	'8Eh'	T_{CC}: znacznik kryptograficznej sumy kontrolnej
#(8 + L + NN)	1	'XXh'	L_{CC}: długość znajdującej się dalej kryptograficznej sumy kontrolnej '04h' dla bezpiecznej wymiany komunikatów 1. generacji (zob. dodatek 11 część A) '08h', '0Ch' lub '10h', w zależności od długości klucza AES, dla bezpiecznej wymiany komunikatów 2. generacji (zob. dodatek 11 część B)
#(9 + L + NN)-#(8 + M + L + NN)	M	'XX..XXh'	Kryptograficzna suma kontrolna
Le	1	'00h'	zgodnie ze specyfikacją w normie ISO/IEC 7816-4

TCS_59 **Komunikat odpowiedzi przy prawidłowym formacie wejściowym bezpiecznej wymiany komunikatów**

Bajt	Długość	Wartość	Opis
#1	1	'99h'	T_{SW}: znacznik słów stanu (chroniony przez CC)
#2	1	'02h'	L_{SW}: długość zwracanego słowa stanu
#3-#4	2	'XXXXh'	Stan przetwarzania niechronionej odpowiedzi APDU
#5	1	'8Eh'	T_{CC}: znacznik kryptograficznej sumy kontrolnej
#6	1	'XXh'	L_{CC}: długość znajdującej się dalej kryptograficznej sumy kontrolnej '04h' dla bezpiecznej wymiany komunikatów 1. generacji (zob. dodatek 11 część A) '08h', '0Ch' lub '10h', w zależności od długości klucza AES, dla bezpiecznej wymiany komunikatów 2. generacji (zob. dodatek 11 część B)
#7-#(6+L)	L	'XX..XXh'	Kryptograficzna suma kontrolna
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

Stany „regularnego" przetwarzania, opisane dla polecenia UPDATE BINARY z bezpieczną wymianą komunikatów (zob. pkt 3.5.3.1), mogą być zwracane przy użyciu struktury komunikatu odpowiedzi opisanej powyżej.

Ponadto mogą wystąpić niektóre błędy, swoiście dotyczące bezpiecznej wymiany komunikatów. W takim przypadku zwracany jest po prostu stan przetwarzania bez struktury bezpiecznej wymiany komunikatów:

TCS_60 **Komunikat odpowiedzi w przypadku błędu w bezpiecznej wymianie komunikatów**

Bajt	Długość	Wartość	Opis
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

— Jeżeli klucz bieżącej sesji nie jest dostępny, zwracany jest stan przetwarzania **'6A88'**.

— Jeżeli w formacie bezpiecznej wymiany komunikatów brakuje pewnych oczekiwanych obiektów (określonych powyżej), zwracany jest stan przetwarzania **'6987'**: ten błąd ma miejsce, jeżeli brakuje oczekiwanego znacznika lub jeżeli treść polecenia nie jest prawidłowo skonstruowana.

— Jeżeli pewne obiekty danych są nieprawidłowe, zwróconym stanem przetwarzania jest **'6988'**: ten błąd ma miejsce, jeżeli obecne są wszystkie wymagane znaczniki, ale niektóre długości różnią się od oczekiwanych.

— Jeżeli weryfikacja kryptograficznej sumy kontrolnej wykaże niezgodność, zwróconym stanem przetwarzania jest **'6688'**.

3.5.3.2 Polecenie z krótkimi identyfikatorem EF

Ten wariant polecenia umożliwia IFD wybór EF przy pomocy krótkiego identyfikatora EF oraz zapis danych z tego EF.

TCS_61 Karta do tachografu obsługuje ten wariant polecenia dla wszystkich plików elementarnych z określonym krótkim identyfikatorem EF. Przedmiotowe krótkie identyfikatory EF zostały określone w rozdziale 4.

TCS_62 **Komunikat polecenia**

Bajt	Długość	Wartość	Opis
CLA	1	'00h'	
INS	1	'D6h'	Aktualizacja binarna licznika
P1	1	'XXh'	Bit 8 ustawiany jest na 1. Bity 7 i 6 ustawiane są na 00. Bity 5 – 1 kodują krótki identyfikator EF odpowiedniego EF.
P2	1	'XXh'	Koduje przesunięcie od 0 do 255 bajtów w EF przywołanym przez P1.
Lc	1	'NNh'	Lc długość aktualizowanych danych. Liczba zapisywanych bajtów.
#6-#(5+NN)	NN	'XX..XXh'	zapisywane dane

TCS_63 **Komunikat odpowiedzi**

Bajt	Długość	Wartość	Opis
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

Uwaga: Krótkie identyfikatory EF używane na potrzeby aplikacji tachograficznej 2. generacji zostały określone w rozdziale 4.

Jeżeli P1 koduje krótki identyfikator EF, a polecenie zostało pomyślnie wykonane, ustalone EF staje się bieżąco wybranym EF (bieżący EF).

— Jeżeli polecenie zostało pomyślnie wykonane, karta zwraca '**9000**'.

— Jeżeli nie znaleziono pliku odpowiadającego krótkiemu identyfikatorowi EF, zwróconym stanem przetwarzania jest **'6A82'**.

— Jeżeli warunki zabezpieczenia wybranego pliku nie są spełnione, polecenie zostaje przerwane z '**6982**'.

— Jeżeli przesunięcie nie jest zgodne z wielkością EF (przesunięcie > wielkość EF), zwróconym stanem przetwarzania jest **'6B00'**.

— Jeżeli wielkość danych, które mają być zapisane, nie jest zgodna z wielkością EF (przesunięcie + Lc > wielkość EF), zwróconym stanem przetwarzania jest **'6700'**.

— Jeżeli błąd integralności zostaje wykryty w atrybutach pliku, karta uznaje, że plik jest uszkodzony i nienaprawialny, a zwróconym stanem przetwarzania jest **'6400'** lub **'6581'**.

— Jeżeli zapis nie jest wykonany pomyślnie, zwróconym stanem przetwarzania jest **'6581'**.

3.5.3.3 Polecenie z nieparzystym bajtem instrukcji

Ten wariant polecenia umożliwia IFD zapis danych do EF, który ma 32 768 bajtów lub więcej.

TCS_64 Karta do tachografu obsługująca EF, który ma 32 768 bajtów lub więcej, musi obsługiwać ten wariant polecenia dla takich EF. Karta do tachografu może, ale nie musi obsługiwać tego wariantu polecenia dla innych EF.

TCS_65 **Komunikat polecenia**

Bajt	Długość	Wartość	Opis
CLA	1	'00h'	
INS	1	'D7h'	Aktualizacja binarna licznika
P1	1	'00h'	bieżący EF
P2	1	'00h'	
Lc	1	'NNh'	Lc długość danych w polu danych dotyczących polecenia
#6-#(5+NN)	NN	'XX..XXh'	przesunięty obiekt danych ze znacznikiem '54h' || nieokreślony obiekt danych ze znacznikiem '53h', który pakuje dane do zapisu

IFD koduje długość przesuniętego obiektu danych oraz długość nieokreślonego obiektu danych z możliwie najmniejszą liczbą oktetów, tzn. przy pomocy bajtu długości '01h' IFD koduje przesunięcie/długość od 0 do 255 bajtów, a przy pomocy bajtu długości '02h' koduje przesunięcie/długość od '256' do '65 535' bajtów.

TCS_66 **Komunikat odpowiedzi**

Bajt	Długość	Wartość	Opis
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

— Jeżeli polecenie zostało pomyślnie wykonane, karta zwraca '**9000**'.

— Jeżeli nie wybrano EF, zwróconym stanem przetwarzania jest **'6986'**.

— Jeżeli warunki zabezpieczenia wybranego pliku nie są spełnione, polecenie zostaje przerwane z '**6982**'.

— Jeżeli przesunięcie nie jest zgodne z wielkością EF (przesunięcie > wielkość EF), zwróconym stanem przetwarzania jest **'6B00'**.

— Jeżeli wielkość danych, które mają być zapisane, nie jest zgodna z wielkością EF (przesunięcie + Lc > wielkość EF), zwróconym stanem przetwarzania jest **'6700'**.

— Jeżeli błąd integralności zostaje wykryty w atrybutach pliku, karta uznaje, że plik jest uszkodzony i nienaprawialny, a zwróconym stanem przetwarzania jest **'6400'** lub **'6500'**.

— Jeżeli zapis nie jest wykonany pomyślnie, zwróconym stanem przetwarzania jest **'6581'**.

3.5.3.3.1 Polecenie z bezpieczną wymianą komunikatów (przykład)

Poniższy przykład ilustruje stosowanie bezpiecznej wymiany komunikatów, jeżeli zastosowanie ma warunek zabezpieczenia SM-MAC-G2.

TCS_67 Komunikat polecenia

Bajt	Długość	Wartość	Opis
CLA	1	'0Ch'	Żądana bezpieczna wymiana komunikatów
INS	1	'D7h'	Aktualizacja binarna licznika
P1	1	'00h'	bieżący EF
P2	1	'00h'	
Lc	1	'XXh'	długość chronionego pola danych
#6	1	'B3h'	znacznik wartości danych odkrytych kodowanych w BER-TLV
#7	L	'NNh' lub '81 NNh'	L_{PV}: długość transmitowanych danych. L ma 2 bajty, jeżeli L_{PV} >127 bajtów.
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	dane odkryte kodowane w BER-TLV, tj. przesunięty obiekt danych ze znacznikiem '54h' || nieokreślony obiekt danych ze znacznikiem '53h', który pakuje dane do zapisu
#(7+L+NN)	1	'8Eh'	T_{CC}: znacznik kryptograficznej sumy kontrolnej
#(8+L+NN)	1	'XXh'	L_{CC}: długość znajdującej się dalej kryptograficznej sumy kontrolnej '08h', '0Ch' lub '10h', w zależności od długości klucza AES, dla bezpiecznej wymiany komunikatów 2. generacji (zob. dodatek 11 część B)
#(9+L+NN)-#(8+M+L+NN)	M	'XX..XXh'	Kryptograficzna suma kontrolna
Le	1	'00h'	zgodnie ze specyfikacją w normie ISO/IEC 7816-4

TCS_68 komunikat odpowiedzi, jeżeli polecenie zostało pomyślnie wykonane

Bajt	Długość	Wartość	Opis
#1	1	'99h'	T_{SW}: znacznik słów stanu (chroniony przez CC)
#2	1	'02h'	L_{SW}: długość zwracanego słowa stanu
#3-#4	2	'XXXXh'	Stan przetwarzania niechronionej odpowiedzi APDU
#5	1	'8Eh'	T_{CC}: znacznik kryptograficznej sumy kontrolnej

Bajt	Długość	Wartość	Opis
#6	1	'XXh'	L_{CC}: długość znajdującej się dalej kryptograficznej sumy kontrolnej '08h', '0Ch' lub '10h', w zależności od długości klucza AES, dla bezpiecznej wymiany komunikatów 2. generacji (zob. dodatek 11 część B)
#7-#(6 + L)	L	'XX..XXh'	Kryptograficzna suma kontrolna
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

3.5.4 *GET CHALLENGE*

Polecenie to jest zgodne z normą ISO/IEC 7816-4, ale jego zastosowanie jest ograniczone w porównaniu z poleceniem zdefiniowanym w tej normie.

Polecenie GET CHALLENGE żąda od karty wydania wyzwania w celu użycia go w procedurze związanej z zabezpieczeniem, w której do karty wysyłany jest kryptogram lub pewne szyfrowane dane.

TCS_69 Wyzwanie wydane przez kartę ważne jest tylko dla następnego polecenia, które używa wyzwania, wysłanego do karty.

TCS_70 **Komunikat polecenia**

Bajt	Długość	Wartość	Opis
CLA	1	'00h'	
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (długość oczekiwanego wyzwania).

TCS_71 **Komunikat odpowiedzi**

Bajt	Długość	Wartość	Opis
#1-#8	8	'XX..XXh'	wyzwanie
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

— Jeżeli polecenie zostało pomyślnie wykonane, karta zwraca '**9000**'.

— Jeżeli Le jest inne niż '08h', zwracany jest stan przetwarzania **'6700'**.

— Jeżeli parametry P1-P2 są nieprawidłowe, zwracany jest stan przetwarzania **'6A86'**.

3.5.5 *VERIFY*

Polecenie to jest zgodne z normą ISO/IEC 7816-4, ale jego zastosowanie jest ograniczone w porównaniu z poleceniem zdefiniowanym w tej normie.

Jedynie karta warsztatowa jest zobowiązana do obsługi tego polecenia.

Inne rodzaje kart do tachografów mogą, ale nie muszą realizować tego polecenia, lecz w przypadku tych kart żadne referencyjne CHV nie jest zindywidualizowane. Karty te nie mogą zatem pomyślnie wykonywać tego polecenia. Jeśli chodzi o rodzaje kart do tachografów inne niż karta warsztatowa, ich zachowanie, tj. zwracany kod błędu, nie jest objęte zakresem zastosowania niniejszej specyfikacji, jeżeli polecenie to jest wysyłane.

Polecenie VERIFY inicjuje porównanie w karcie danych CHV (PIN) wysłanych w poleceniu z referencyjnymi CHV przechowywanymi na karcie.

TCS_72 PIN wprowadzony przez użytkownika musi być kodowany w ASCI i prawidłowo wypełniony przez IFD bajtami 'FFh' do długości 8 bajtów (zob. również typ danych WorkshopCardPIN w dodatku 1).

TCS_73 Aplikacje tachograficzne 1. i 2. generacji używają tego samego referencyjnego CHV.

TCS_74 Karta do tachografu sprawdza, czy polecenie jest prawidłowo zakodowane. Jeżeli polecenie nie jest prawidłowo zakodowane, karta nie porównuje wartości CHV, nie zmniejsza licznika dozwolonych prób CHV, ani nie zeruje stanu zabezpieczenia „PIN_Verified", lecz przerywa wykonanie polecenia. Polecenie jest prawidłowo zakodowane, jeżeli bajty CLA, INS, P1, P2 i Lc posiadają określone wartości, brak jest Le, a pole danych dotyczących polecenia posiada odpowiednią długość.

TCS_75 Jeżeli polecenie zostało pomyślnie wykonane, licznik dozwolonych prób CHV zostaje przywrócony do stanu wyjściowego. Wartość początkowa licznika dozwolonych prób CHV to 5. Jeżeli polecenie zostało pomyślnie wykonane, stan zabezpieczenia wewnętrznego karty otrzymuje status „PIN_Verified". Karta zeruje ten stan zabezpieczenia, jeżeli karta jest zresetowana lub jeżeli kod CHV przesłany w poleceniu nie odpowiada przechowywanemu referencyjnemu CHV.

Uwaga: Stosowanie tego samego referencyjnego CHV i globalnego stanu zabezpieczenia zapobiega konieczności ponownego wprowadzenia PIN przez pracownika warsztatu po wybraniu innej aplikacji tachograficznej DF.

TCS_76 Jeżeli porównanie wykaże niezgodność, jest ono rejestrowane na karcie, tzn. licznik dozwolonych prób CHV zmniejsza się o jeden, aby ograniczyć liczbę dalszych prób użycia referencyjnego CHV.

TCS_77 **Komunikat polecenia**

Bajt	Długość	Wartość	Opis
CLA	1	'00h'	
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (zweryfikowane CHV jest domniemanie znane)
Lc	1	'08h'	długość przesyłanego kodu CHV
#6-#13	8	'XX..XXh'	CHV

TCS_78 **Komunikat odpowiedzi**

Bajt	Długość	Wartość	Opis
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

— Jeżeli polecenie zostało pomyślnie wykonane, karta zwraca '**9000**'.

— Jeżeli nie znaleziono referencyjnego CHV, zwróconym stanem przetwarzania jest **'6A88'**.

— Jeżeli CHV jest zablokowane (licznik dozwolonych prób CHV jest wyzerowany), zwróconym stanem przetwarzania jest **'6983'**. Po znalezieniu się w tym stanie CHV nie może już nigdy być pomyślnie przekazane.

— Jeżeli porównanie wykaże niezgodność, licznik dozwolonych prób CHV jest zmniejszany i zwracany jest stan **'63CX'** (X > 0, gdzie X pokazuje stan licznika dozwolonych prób CHV).

— Jeżeli referencyjne CHV uznane jest za uszkodzone, zwróconym stanem przetwarzania jest **'6400'** lub **'6581'**.

— Jeżeli Lc jest inne niż '08h', zwracany jest stan przetwarzania '**6700**'.

3.5.6 *GET RESPONSE*

Polecenie to jest zgodne z normą ISO/IEC 7816-4.

Polecenia tego (niezbędnego i dostępnego tylko dla protokołu T=0) używa się do przesyłania przygotowanych danych z karty do urządzenia interfejsu (przypadek, gdy polecenie zawiera oba parametry Lc i Le).

Polecenie GET RESPONSE musi być wydane bezpośrednio po poleceniu przygotowującym dane, w przeciwnym przypadku dane są tracone. Po wykonaniu polecenia GET RESPONSE (z wyjątkiem sytuacji, gdy wystąpi błąd '**61xx**' lub '**6Cxx**', zob. poniżej) wcześniej przygotowane dane nie są już dostępne.

TCS_79 **Komunikat polecenia**

Bajt	Długość	Wartość	Opis
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	oczekiwana liczba bajtów

TCS_80 **Komunikat odpowiedzi**

Bajt	Długość	Wartość	Opis
#1-#X	X	'XX..XXh'	dane
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

— Jeżeli polecenie zostało pomyślnie wykonane, karta zwraca '**9000**'.

— Jeżeli karta nie przygotuje żadnych danych, zwróconym stanem przetwarzania jest **'6900'** lub **'6F00'.**.

— Jeżeli Le przekracza liczbę dostępnych bajtów lub Le to zero, zwróconym stanem przetwarzania jest **'6Cxx'**, gdzie „xx" oznacza dokładną liczbę dostępnych bajtów. W takim przypadku przygotowane dane pozostają dostępne dla kolejnego polecenia GET RESPONSE.

— Jeżeli Le jest różne od zera i jest mniejsze od liczby dostępnych bajtów, karta wysyła normalnie żądane dane, a zwróconym stanem przetwarzania jest **'61xx'**, gdzie „xx" oznacza liczbę dodatkowych bajtów jeszcze dostępnych dla kolejnego polecenia GET RESPONSE.

— Jeżeli polecenie nie jest obsługiwane (protokół T=1), karta zwraca **'6D00'**.

3.5.7 *PSO: VERIFY CERTIFICATE*

Polecenie to jest zgodne z normą ISO/IEC 7816-8, ale jego zastosowanie jest ograniczone w porównaniu z poleceniem zdefiniowanym w tej normie.

Karta używa polecenia VERIFY_CERTIFICATE do otrzymania klucza publicznego z zewnątrz i do sprawdzenia ważności tego klucza.

3.5.7.1 Para polecenie – odpowiedź 1. generacji

TCS_81 Ten wariant polecenia jest obsługiwany jedynie przez aplikację tachograficzną 1. generacji.

TCS_82 W przypadku pomyślnej weryfikacji poleceniem VERIFY CERTIFICATE klucz publiczny jest zapamiętany do przyszłego wykorzystania w środowisku zabezpieczeń. Klucz ten jest jawnie przydzielony do używania w poleceniach związanych z zabezpieczeniem (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE lub VERIFY CERTIFICATE) przez polecenie MSE (zob. pkt 3.5.11) przy użyciu jego identyfikatora klucza.

TCS_83 W każdym przypadku polecenie VERIFY CERTIFICATE używa klucza publicznego uprzednio wybranego przez polecenie MSE do otwarcia certyfikatu. Ten klucz publiczny musi być kluczem jednego z państw członkowskich lub Europy.

TCS_84 **Komunikat polecenia**

Bajt	Długość	Wartość	Opis
CLA	1	'00h'	
INS	1	'2Ah'	wykonanie operacji zabezpieczającej
P1	1	'00h'	P1
P2	1	'AEh'	P2: dane niekodowane w BER-TLV (konkatenacja elementów danych)
Lc	1	'C2h'	Lc: długość certyfikatu, 194 bajty
#6-#199	194	'XX..XXh'	certyfikat: konkatenacja elementów danych (opisana w dodatku 11)

TCS_85 **Komunikat odpowiedzi**

Bajt	Długość	Wartość	Opis
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

— Jeżeli polecenie zostało pomyślnie wykonane, karta zwraca '**9000**'.

— Jeżeli weryfikacja certyfikatu nie uda się, zwróconym stanem przetwarzania jest **'6688'**. Proces weryfikacji i otwierania certyfikatu opisano w dodatku 11 dla 1. generacji i 2. generacji.

— Jeżeli klucza publicznego nie ma w środowisku zabezpieczeń, zwróconym stanem przetwarzania jest **'6A88'**.

— Jeżeli wybrany klucz publiczny (użyty do otwierania certyfikatu) uznany jest za uszkodzony, zwróconym stanem przetwarzania jest **'6400'** lub **'6581'**.

— Wyłącznie 1. generacja: Jeżeli CHA.LSB (`CertificateHolderAuthorisation.equipmentType`) wybranego klucza publicznego (użytego do otwierania certyfikatu) różni się od '00' (tzn. nie jest kluczem państwa członkowskiego lub Europy), zwróconym stanem przetwarzania jest **'6985'**.

3.5.7.2 Para polecenie – odpowiedź 2. generacji

W zależności od wielkości krzywej certyfikaty ECC mogą być tak długie, że nie mogą być przekazywane w jednym APDU. W takim przypadku stosowany musi być łańcuch poleceń zgodny z ISO/IEC 7816-4, a certyfikat musi być przesyłany w dwóch kolejnych poleceniach APDU PSO: Verify Certificate.

Struktura certyfikatu i parametry domeny zostały określone w dodatku 11.

TCS_86 Polecenie może być wykonywane w MF, w DF Tachograph i w DF Tachograph_G2 (zob. również TCS_33).

TCS_87 **Komunikat polecenia**

Bajt	Długość	Wartość	Opis
CLA	1	'X0h'	bajt CLA wskazujący łańcuch poleceń: '00h' – jedyne lub ostatnie polecenie łańcucha '10h' – nieostatnie polecenie łańcucha
INS	1	'2Ah'	wykonanie operacji zabezpieczającej
P1	1	'00h'	
P2	1	'BEh'	weryfikacja samoopisującego certyfikatu
Lc	1	'XXh'	długość pola danych dotyczących polecenia (zob. TCS_88 oraz TCS_89).
#6-#5+L	L	'XX..XXh'	dane kodowane w DER-TLV: Obiekt danych jednostki certyfikującej ECC jako pierwszy obiekt danych konkatenowany z obiektem danych podpisu certyfikatu ECC jako drugim obiektem danych lub jako częścią tej konkatenacji. Znacznik '7F21' i odpowiednia długość nie są przekazywane. Kolejność tych obiektów danych jest stała.

TCS_88 W odniesieniu do APDU o krótkiej długości zastosowanie mają następujące postanowienia: IFD musi wykorzystywać minimalną liczbę APDU wymaganą do przesłania payloadu polecenia oraz transmisji maksymalnej liczby bajtów w pierwszym poleceniu APDU zgodnie z wartością bajtu wielkości pola informacyjnego dla karty (zob. TCS_14). Jeżeli IFD działa inaczej, zachowanie karty nie jest objęte zakresem zastosowania.

TCS_89 W odniesieniu do APDU o rozszerzonej długości zastosowanie mają następujące postanowienia: Jeżeli certyfikat nie jest dopasowany do pojedynczego APDU, karta musi obsługiwać łańcuch poleceń. IFD musi wykorzystywać minimalną liczbę APDU wymaganą do przesłania payloadu polecenia oraz transmisji maksymalnej liczby bajtów w pierwszym poleceniu APDU. Jeżeli IFD działa inaczej, zachowanie karty nie jest objęte zakresem zastosowania.

Uwaga: Zgodnie z dodatkiem 11 karta przechowuje certyfikat lub odpowiednie treści certyfikatu oraz uaktualnia jego currentAuthenticatedTime.

Struktura komunikatu odpowiedzi i słowa stanu zostały określone w TCS_85.

TCS_90 Oprócz kodów błędów wymienionych w TCS_85, karta może zwracać następujące kody błędów:

— jeżeli CHA.LSB (CertificateHolderAuthorisation.equipmentType) wybranego klucza publicznego (użytego do otwierania certyfikatu) nie jest odpowiednie dla weryfikacji certyfikatu zgodnie z dodatkiem 11, zwróconym stanem przetwarzania jest '**6985**'.

— Jeżeli currentAuthenticatedTime karty jest późniejszy niż data upływu ważności certyfikatu, zwróconym stanem przetwarzania jest '**6985**'.

— Jeżeli oczekiwane jest ostatnie polecenie łańcucha, karta zwraca '**6883**'.

— Jeżeli nieprawidłowe parametry są wysyłane w polu danych dotyczących polecenia, karta zwraca '**6A80**' (także w przypadku, gdy obiekty danych nie są wysyłane w określonej kolejności).

3.5.8 *INTERNAL AUTHENTICATE*

Polecenie to jest zgodne z normą ISO/IEC 7816-4.

TCS_91 Wszystkie karty do tachografów obsługują to polecenie w DF Tachograph_G1. Polecenie może, ale nie musi być dostępne w MF lub DF Tachograph_G2. W takim przypadku polecenie zostaje zakończone odpowiednim kodem błędu, ponieważ klucz prywatny karty (Card.SK) dla protokołu uwierzytelnienia 1. generacji jest dostępny tylko w DF_Tachograph G1.

Używając polecenia INTERNAL AUTHENTICATE, IFD może uwierzytelnić kartę. Proces uwierzytelnienia opisano w dodatku 11. W procesie tym używa się następujących instrukcji:

TCS_92 Polecenie INTERNAL AUTHENTICATE używa klucza prywatnego karty (wybranego niejawnie) do podpisania danych uwierzytelniających obejmujących K1 (pierwszy element do uzgodnienia kluczy sesyjnych) i RND1, a także używa bieżąco wybranego klucza publicznego (w ostatnim poleceniu MSE) do zaszyfrowania podpisu i utworzenia tokenu uwierzytelniania (dokładniej opisano w dodatku 11).

TCS_93 **Komunikat polecenia**

Bajt	Długość	Wartość	Opis
CLA	1	'00h'	CLA
INS	1	'88h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Lc	1	'10h'	długość danych wysłanych do karty
#6 – #13	8	'XX..XXh'	wyzwanie użyte do uwierzytelnienia karty
#14 -#21	8	'XX..XXh'	VU.CHR (zob. dodatek 11)
Le	1	'80h'	długość danych oczekiwanych z karty

TCS_94 **Komunikat odpowiedzi**

Bajt	Długość	Wartość	Opis
#1-#128	128	'XX..XXh'	token uwierzytelniania karty (zob. dodatek 11)
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

— Jeżeli polecenie zostało pomyślnie wykonane, karta zwraca '**9000**'.

— Jeżeli klucza publicznego nie ma w środowisku zabezpieczeń, zwróconym stanem przetwarzania jest **'6A88'**.

— Jeżeli klucza prywatnego nie ma w środowisku zabezpieczeń, zwróconym stanem przetwarzania jest **'6A88'**.

— Jeżeli VU.CHR nie zgadza się z bieżącym identyfikatorem klucza publicznego, zwróconym stanem przetwarzania jest **'6A88'**.

— Jeżeli wybrany klucz prywatny uznany jest za uszkodzony, zwróconym stanem przetwarzania jest **'6400'** lub **'6581'**.

TCS_95 Jeżeli uwierzytelnienie poleceniem INTERNAL AUTHENTICATE jest pomyślne, klucz bieżącej sesji (o ile istnieje) zostaje skasowany i nie jest dalej dostępny. W celu uzyskania nowego klucza sesji konieczne jest pomyślne wykonanie uwierzytelnienia poleceniem EXTERNAL AUTHENTICATE dla mechanizmu uwierzytelnienia 1. generacji.

3.5.9 *EXTERNAL AUTHENTICATE*

Polecenie to jest zgodne z normą ISO/IEC 7816-4.

Poleceniem EXTERNAL AUTHENTICATE karta może uwierzytelnić IFD. Proces uwierzytelnienia opisano w dodatku 11 dla tachografów 1. generacji i 2. generacji (uwierzytelnienie VU).

TCS_96 Wariant polecenia dla mechanizmu wzajemnego uwierzytelnienia 1. generacji jest obsługiwany jedynie przez aplikację tachograficzną 1. generacji.

TCS_97 Wariant polecenia dla wzajemnego uwierzytelnienia VU – karta drugiej generacji można wykonać w MF, DF Tachograph i DF Tachograph_G2 (zob. również TCS_34).

TCS_98 **Komunikat polecenia**

Bajt	Długość	Wartość	Opis
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	klucze i algorytmy domniemanie znane
P2	1	'00h'	
Lc	1	'XXh'	Lc (długość danych wysłanych do karty)
#6-#(5+L)	L	'XX..XXh'	uwierzytelnienie 1. generacji: kryptogram (zob. dodatek 11 część A) uwierzytelnienie 2. generacji: podpis wygenerowany przez IFD (zob. dodatek 11 część B)

TCS_99 **Komunikat odpowiedzi**

Bajt	Długość	Wartość	Opis
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

— Jeżeli polecenie zostało pomyślnie wykonane, karta zwraca '**9000**'.

— Jeżeli CHA bieżąco ustawionego klucza publicznego nie jest konkatenacją AID aplikacji tachograficznej i typu urządzenia VU, zwróconym stanem przetwarzania jest **'6F00'**.

— Jeżeli bezpośrednio przed poleceniem nie znajduje się polecenie GET CHALLENGE, zwróconym stanem przetwarzania jest **'6985'**.

Aplikacja tachograficzna 1. generacji może zwracać następujące dodatkowe kody błędów:

— Jeżeli klucza publicznego nie ma w środowisku zabezpieczeń, zwróconym stanem przetwarzania jest **'6A88'**.

— Jeżeli klucza prywatnego nie ma w środowisku zabezpieczeń, zwróconym stanem przetwarzania jest **'6A88'**.

— Jeżeli weryfikacja kryptogramu daje zły wynik, zwróconym stanem przetwarzania jest **'6688'**.

— Jeżeli wybrany klucz prywatny uznany jest za uszkodzony, zwróconym stanem przetwarzania jest **'6400'** lub **'6581'**.

Wariant polecenia dla uwierzytelnienia 2. generacji może zwracać następujący dodatkowy kod błędu:

— Jeżeli podpis jest zweryfikowany negatywnie, karta zwraca '**6300**'.

3.5.10 *GENERAL AUTHENTICATE*

Polecenie to jest używane na potrzeby protokołu uwierzytelnienia mikroprocesora 2. generacji, określonego w dodatku 11 część B, i jest zgodne z normą ISO/IEC 7816-4.

TCS_100 Polecenie może być wykonywane w MF, DF Tachograph i DF Tachograph_G2 (zob. również TCS_34).

TCS_101 **Komunikat polecenia**

Bajt	Długość	Wartość	Opis
CLA	1	'00h'	
INS	1	'86h'	
P1	1	'00h'	klucze i protokół domniemanie znane
P2	1	'00h'	
Lc	1	'NNh'	Lc: długość następnego pola danych
#6-#(5+L)	L	'7Ch' + L_{7C} + '80h' + L_{80} + 'XX..XXh'	Wartość efemerycznego klucza publicznego kodowana w DER-TLV (zob. dodatek 11) VU wysyła obiekty danych w tej kolejności.

TCS_102 **Komunikat odpowiedzi**

Bajt	Długość	Wartość	Opis
#1-#L	L	'7Ch' + L_{7C} + '81h' + '08h' + 'XX..XXh' + '82h' + L_{82} + 'XX..XXh'	dane dynamicznego uwierzytelniania kodowane w DER-TLV: nonce i token uwierzytelniania (zob. dodatek 11)
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

— Jeżeli polecenie zostało pomyślnie wykonane, karta zwraca '**9000**'.

— Karta zwraca '**6A80**', aby wskazać nieprawidłowe parametry w polu danych.

— Karta zwraca '**6982**', jeżeli uwierzytelnienie poleceniem EXTERNAL AUTHENTICATE nie zostało pomyślnie wykonane.

Obiekt danych dynamicznego uwierzytelnienia odpowiedzi '7Ch'

— musi być obecny, jeżeli operacja została pomyślnie wykonana, tzn. słowa stanu to '**9000**',

— musi być nieobecny w przypadku błędu wykonania lub błędu kontroli, tzn. jeśli słowa stanu mieszczą się w zakresie '**6400**' – '**6FFF**', oraz

— musi być nieobecny w przypadku ostrzeżenia, tzn. jeśli słowa stanu mieszczą się w zakresie '**6200**' – '**63FF**'.

3.5.11 *MANAGE SECURITY ENVIRONMENT*

Poleceniem tym ustawia się klucz publiczny na potrzeby uwierzytelnienia.

3.5.11.1 Para polecenie – odpowiedź 1. generacji

Polecenie to jest zgodne z normą ISO/IEC 7816-4. Zastosowanie tego polecenia jest ograniczone w porównaniu z poleceniem zdefiniowanym w tej normie.

TCS_103 To polecenie jest obsługiwane jedynie przez aplikację tachograficzną 1. generacji.

TCS_104 Klucz powołany w polu danych MSE pozostaje bieżącym kluczem publicznym aż do następnego prawidłowego polecenia MSE, DF zostaje wybrany lub karta zostaje zresetowana.

TCS_105 Jeżeli powołanego klucza nie ma (już) na karcie, środowisko zabezpieczeń pozostaje niezmienione.

TCS_106 **Komunikat polecenia**

Bajt	Długość	Wartość	Opis
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: powołany klucz ważny dla wszystkich czynności kryptograficznych
P2	1	'B6h'	P2 (powołane dane dotyczące podpisu cyfrowego)
Lc	1	'0Ah'	Lc: długość następnego pola danych
#6	1	'83h'	znacznik do powołanego klucza publicznego w przypadkach asymetrycznych
#7	1	'08h'	długość referencji klucza (identyfikator klucza)
#8-#15	8	'XX..XXh'	identyfikator klucza określony w dodatku 11

TCS_107 **Komunikat odpowiedzi**

Bajt	Długość	Wartość	Opis
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

— Jeżeli polecenie zostało pomyślnie wykonane, karta zwraca '**9000**'.

— Jeżeli powołany klucz nie znajduje się na karcie, zwróconym stanem przetwarzania jest **'6A88'**.

— Jeżeli niektórych oczekiwanych obiektów danych brakuje w formacie bezpiecznej wymiany komunikatów, zwracany jest stan przetwarzania **'6987'**. To może zdarzyć się, gdy brakuje znacznika '83h'.

— Jeżeli pewne obiekty danych są nieprawidłowe, zwróconym stanem przetwarzania jest **'6988'**. To może zdarzyć się, gdy długość identyfikatora klucza różna jest od '08h'.

— Jeżeli wybrany klucz uznany jest za uszkodzony, zwróconym stanem przetwarzania jest **'6400'** lub **'6581'**.

3.5.11.2 Pary polecenie – odpowiedź 2. generacji

Jeśli chodzi o uwierzytelnienie 2. generacji, karta do tachografu obsługuje następujące MSE: Wersje zbioru poleceń, które są zgodne z normą ISO/IEC 7816-4. Te wersje poleceń nie są obsługiwane na potrzeby uwierzytelnienia 1. generacji.

3.5.11.2.1 MSE:SET AT na potrzeby uwierzytelnienia mikroprocesora

Poniższego polecenia MSE:SET AT używa się do wyboru parametrów na potrzeby uwierzytelnienia mikroprocesora, które jest wykonywane kolejnym poleceniem General Authenticate.

TCS_108 Polecenie może być wykonywane w MF, DF Tachograph i DF Tachograph_G2 (zob. również TCS_34).

TCS_109 **Komunikat polecenia MSE:SET AT na potrzeby uwierzytelnienia mikroprocesora**

Bajt	Długość	Wartość	Opis
CLA	1	'00h'	
INS	1	'22h'	

Bajt	Długość	Wartość	Opis
P1	1	'41h'	przydzielone do uwierzytelnienia wewnętrznego
P2	1	'A4h'	Uwierzytelnienie
Lc	1	'NNh'	Lc: długość następnego pola danych
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	Odniesienie do mechanizmu kryptograficznego kodowanego w DER-TLV: identyfikator obiektu uwierzytelnienia mikroprocesora (wyłącznie wartość, znacznik '06h' jest pomijany). Zob. dodatek 1 dla wartości identyfikatorów obiektu; Stosuje się zapis bajtowy. Zob. dodatek 11 zawierający wytyczne dotyczące sposobu wyboru jednego z tych identyfikatorów obiektu.

3.5.11.2.2 MSE:SET AT na potrzeby uwierzytelnienia VU

Poniższego polecenia MSE:SET AT używa się do wyboru parametrów i kluczy na potrzeby uwierzytelnienia VU, które jest wykonywane kolejnym poleceniem External Authenticate.

TCS_110 Polecenie może być wykonywane w MF, DF Tachograph i DF Tachograph_G2 (zob. również TCS_34).

TCS_111 **Komunikat polecenia MSE:SET AT na potrzeby uwierzytelnienia VU**

Bajt	Długość	Wartość	Opis
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'81h'	przydzielone do uwierzytelnienia zewnętrznego
P2	1	'A4h'	Uwierzytelnienie
Lc	1	'NNh'	Lc: długość następnego pola danych
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	Odniesienie do mechanizmu kryptograficznego kodowanego w DER-TLV: identyfikator obiektu uwierzytelnienia VU (wyłącznie wartość, znacznik '06h' jest pomijany). Zob. dodatek 1 dla wartości identyfikatorów obiektu; Stosuje się zapis bajtowy. Zob. dodatek 11 zawierający wytyczne dotyczące sposobu wyboru jednego z tych identyfikatorów obiektu.
		'83h' + '08h' + 'XX..XXh'	kodowane w DER-TL odniesienie klucza publicznego VU przez Certificate Holder Reference wymienione w jego certyfikacie
		'91h' + L_{91} + 'XX..XXh'	kodowana w DER-TLV skompresowana reprezentacja efemerycznego klucza publicznego VU do stosowania podczas uwierzytelnienia mikroprocesora (zob. dodatek 11)

3.5.11.2.3 MSE:SET DST

Poniższego polecenia MSE:SET DST używa się do ustawienia klucza publicznego

— albo do weryfikacji podpisu, który znajduje się w następnym poleceniu PSO: Verify Digital Signature

— albo do weryfikacji podpisem certyfikatu, który znajduje się w następnym poleceniu PSO: Verify Certificate.

TCS_112 Polecenie może być wykonywane w MF, w DF Tachograph i w DF Tachograph_G2 (zob. również TCS_33).

TCS_113 **Komunikat polecenia MSE:SET DST**

Bajt	Długość	Wartość	Opis
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'81h'	przydzielone do weryfikacji
P2	1	'B6h'	podpis cyfrowy
Lc	1	'NNh'	Lc: długość następnego pola danych
#6-#(5+L)	L	'83h' + '08h' + 'XX...XXh'	kodowane w DER-TLV odniesienie klucza publicznego, tj. Certificate Holder Reference w certyfikacie klucza publicznego (zob.dodatek 11)

Dla wszystkich wersji polecenia struktura komunikatu odpowiedzi i słowa stanu podane są przez:

TCS_114 **Komunikat odpowiedzi**

Bajt	Długość	Wartość	Opis
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

— Jeżeli polecenie zostało pomyślnie wykonane, karta zwraca '**9000**'. Protokół został wybrany i zainicjowany.

— **'6A80'** oznacza nieprawidłowe parametry w polu danych dotyczących polecenia.

— **'6A88'** oznacza, że przywołane dane (tj. powołany klucz) nie są dostępne.

3.5.12 *PSO: HASH*

Polecenia tego używa się do przesłania na kartę wyniku obliczeń funkcji skrótu dla niektórych danych. Polecenia tego używa się do weryfikowania podpisów cyfrowych. Wartość skrótu jest tymczasowo zachowywana dla kolejnego polecenia PSO: Verify Digital Signature.

Polecenie to jest zgodne z normą ISO/IEC 7816-8. Zastosowanie tego polecenia jest ograniczone w porównaniu z poleceniem zdefiniowanym w tej normie.

Tylko karta kontrolna jest zobowiązana obsługiwać to polecenie w DF Tachograph i DF Tachograph_G2.

Inne rodzaje kart do tachografów mogą, ale nie muszą realizować tego polecenia. Polecenie może, ale nie musi być dostępne w MF.

Aplikacja karty kontrolnej 1. generacji obsługuje tylko SHA-1.

TCS_115 Tymczasowo zachowana wartość skrótu jest usuwana, jeżeli nowa wartość skrótu zostaje obliczona za pomocą polecenia PSO: HASH, jeżeli DF jest wybrany oraz jeżeli karta do tachografu jest zresetowana.

TCS_116 **Komunikat polecenia**

Bajt	Długość	Wartość	Opis
CLA	1	'00h'	CLA
INS	1	'2Ah'	wykonanie operacji zabezpieczającej
P1	1	'90h'	zwróć kod skrótu
P2	1	'A0h'	Znacznik: pole danych zawiera DO stosowne do obliczania skrótu
Lc	1	'XXh'	Lc długość następnego pola danych
#6	1	'90h'	znacznik dla kodu skrótu
#7	1	'XXh'	długość L kodu skrótu: '14h' dla aplikacji 1. generacji (zob. dodatek 11 część A) '20h', '30h' lub '40h' dla aplikacji 2. generacji (zob. dodatek 11 część B)
#8-#(7+L)	L	'XX..XXh'	kod skrótu

TCS_117 **Komunikat odpowiedzi**

Bajt	Długość	Wartość	Opis
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

— Jeżeli polecenie zostało pomyślnie wykonane, karta zwraca '**9000**'.

— Jeżeli brakuje niektórych oczekiwanych obiektów danych (jak określone powyżej), zwracany jest stan przetwarzania **'6987'**. To może zdarzyć się, jeżeli brakuje jednego ze znaczników '90h'.

— Jeżeli pewne obiekty danych są nieprawidłowe, zwróconym stanem przetwarzania jest **'6988'**. Ten błąd zdarza się, gdy wymagany znacznik jest obecny, ale ma długość różną niż '14h' dla SHA-1, '20h' dla SHA-256, '30h' dla SHA-384, '40h' dla SHA-512 (aplikacja 2. generacji).

3.5.13 *PERFORM HASH of FILE*

Polecenie to nie jest zgodne z normą ISO/IEC 7816-8. Tym samym bajt CLA w tym poleceniu wskazuje na zastrzeżone użycie polecenia PERFORM SECURITY OPERATION/HASH.

Tylko karta kierowcy i karta warsztatowa są zobowiązane obsługiwać to polecenie w DF Tachograph i DF Tachograph_G2.

Inne rodzaje kart do tachografów mogą, ale nie muszą realizować tego polecenia. Jeżeli przedsiębiorstwo lub karta kontrolna realizują to polecenie, odbywa się to zgodnie z opisem w niniejszym rozdziale.

Polecenie może, ale nie musi być dostępne w MF. W takim przypadku polecenie realizowane jest zgodnie z opisem w niniejszym rozdziale, tzn. nie pozwala na obliczenie wartości skrótu, ale zostaje zakończone odpowiednim kodem błędu.

TCS_118 Polecenia PERFORM HASH of FILE używa się do obliczenia skrótu obszaru danych aktualnie wybranego przezroczystego pliku EF.

TCS_119 Karta do tachografu obsługuje to polecenie jedynie dla EF, które są wymienione w rozdziale 4 pod DF_Tachograph i DF_Tachograph_G2 z poniższym wyjątkiem. Karta do tachografu nie obsługuje polecenia dla EF Sensor_Installation_Data w DF_Tachograph_G2.

TCS_120 Wynik operacji obliczania skrótu przechowywany jest tymczasowo na karcie. Następnie może być używany do otrzymania podpisu cyfrowego pliku przy pomocy polecenia PSO: COMPUTE DIGITAL SIGNATURE.

TCS_121 Tymczasowo zachowana wartość skrótu pliku jest usuwana, jeżeli nowa wartość skrótu zostaje obliczona za pomocą polecenia PSO: Hash of File, jeżeli DF jest wybrany oraz jeżeli karta do tachografu jest zresetowana.

TCS_122 Aplikacja tachograficzna 1. generacji obsługuje SHA-1.

TCS_123 Aplikacja tachograficzna 2. generacji obsługuje SHA-1 i SHA-2 (256 bitów, 384 bity i 512 bitów).

TCS_124 **Komunikat polecenia**

Bajt	Długość	Wartość	Opis
CLA	1	'80h'	CLA
INS	1	'2Ah'	wykonanie operacji zabezpieczającej
P1	1	'90h'	znacznik: Hash
P2	1	'XXh'	P2: Wskazuje algorytm, jaki ma zostać użyty do haszowania danych dla aktualnie wybranego przezroczystego pliku: '00h' dla SHA-1 '01h' dla SHA-256 '02h' dla SHA-384 '03h' dla SHA-512

TCS_125 **Komunikat odpowiedzi**

Bajt	Długość	Wartość	Opis
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

— Jeżeli polecenie zostało pomyślnie wykonane, karta zwraca '**9000**'.

— Jeżeli bieżący EF nie dopuszcza tego polecenia (EF Sensor_Installation_Data in DF Tachograph_G2), zwróconym stanem przetwarzania jest **'6985'**.

— Jeżeli wybrany plik EF uznany jest za uszkodzony (błąd atrybutów pliku lub błąd integralności przechowywanych danych), zwróconym stanem przetwarzania jest '**6400**' lub **'6581'**.

— Jeżeli wybrany plik nie jest plikiem przezroczystym, zwróconym stanem przetwarzania jest '**6986**'.

3.5.14 *PSO: COMPUTE DIGITAL SIGNATURE*

Polecenia tego używa się do obliczania podpisu cyfrowego z obliczonego wcześniej kodu skrótu (zob. polecenie PERFORM HASH of FILE, pkt 3.5.13).

Tylko karta kierowcy i karta warsztatowa są zobowiązane obsługiwać to polecenie w DF Tachograph i DF Tachograph_G2.

Inne rodzaje kart do tachografów mogą, ale nie muszą realizować tego polecenia, lecz nie mogą mieć klucza podpisu. Dlatego też karty te nie mogą wykonać pomyślnie polecenia, ale kończą je odpowiednim kodem błędu.

Polecenie może, ale nie musi być dostępne w MF. W takim przypadku polecenie zostaje zakończone odpowiednim kodem błędu.

Polecenie to jest zgodne z normą ISO/IEC 7816-8. Zastosowanie tego polecenia jest ograniczone w porównaniu z poleceniem zdefiniowanym w tej normie.

TCS_126 Polecenie to nie oblicza podpisu cyfrowego z obliczonego wcześniej kodu skrótu poleceniem PSO: HASH.

TCS_127 Klucza prywatnego karty, który jest niejawnie znany karcie, używa się do obliczania podpisu cyfrowego.

TCS_128 Aplikacja tachograficzna 1. generacji wykonuje podpis cyfrowy metodą wypełniania zgodną z PKCS1 (zob. dokładniejszy opis w dodatku 11).

TCS_129 Aplikacja tachograficzna 2. generacji oblicza podpis cyfrowy oparty na krzywej eliptycznej (zob. dokładniejszy opis w dodatku 11).

TCS_130 **Komunikat polecenia**

Bajt	Długość	Wartość	Opis
CLA	1	'00h'	CLA
INS	1	'2Ah'	wykonanie operacji zabezpieczającej
P1	1	'9Eh'	zwracany podpis cyfrowy
P2	1	'9Ah'	znacznik: pole danych zawiera dane do podpisania. Gdy nie zawarto pola danych, przyjmuje się, że dane te są już na karcie (skrót pliku).
Le	1	'NNh'	długość oczekiwanego podpisu

TCS_131 **Komunikat odpowiedzi**

Bajt	Długość	Wartość	Opis
#1-#L	L	'XX..XXh'	podpis uprzednio obliczonego skrótu
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

— Jeżeli polecenie zostało pomyślnie wykonane, karta zwraca '**9000**'.

— Jeżeli niejawnie wybrany klucz prywatny uznany jest za uszkodzony, zwróconym stanem przetwarzania jest '**6400**' lub **'6581'**.

— Jeżeli skrót, który został obliczony w ramach poprzedniego polecenia Perform Hash of File nie jest dostępny, zwróconym stanem przetwarzania jest **'6985'**.

3.5.15 *PSO: VERIFY DIGITAL SIGNATURE*

Polecenia tego używa się do weryfikowania podpisu cyfrowego dostarczanego jako dane wejściowe, którego skrót jest znany karcie. Algorytm podpisu jest niejawnie znany karcie.

Polecenie to jest zgodne z normą ISO/IEC 7816-8. Zastosowanie tego polecenia jest ograniczone w porównaniu z poleceniem zdefiniowanym w tej normie.

Tylko karta kontrolna jest zobowiązana obsługiwać to polecenie w DF Tachograph i DF Tachograph_G2.

Inne rodzaje kart do tachografów mogą, ale nie muszą realizować tego polecenia. Polecenie może, ale nie musi być dostępne w MF.

TCS_132 Polecenie VERIFY DIGITAL SIGNATURE zawsze używa klucza publicznego wybranego poprzednim poleceniem Manage Security Environment MSE: Set DST i poprzednim kodem skrótu wprowadzonym poleceniem PSO: HASH.

TCS_133 **Komunikat polecenia**

Bajt	Długość	Wartość	Opis
CLA	1	'00h'	CLA
INS	1	'2Ah'	wykonanie operacji zabezpieczającej
P1	1	'00h'	
P2	1	'A8h'	Znacznik: pole danych zawiera obiekty DO stosowne do weryfikacji
Lc	1	'83h'	Lc długość następnego pola danych
6	1	'9Eh'	znacznik dla podpisu cyfrowego
#7-#8	2	'81 XXh'	Długość podpisu cyfrowego: 128 bajtów kodowanych zgodnie z dodatkiem 11 część A dla aplikacji tachograficznej 1. generacji. w zależności od wybranej krzywej dla aplikacji tachograficznej 2. generacji (zob. dodatek 11 część B)
#9-#(8+L)	L	'XX..XXh'	treść podpisu cyfrowego

TCS_134 **Komunikat odpowiedzi**

Bajt	Długość	Wartość	Opis
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

— Jeżeli polecenie zostało pomyślnie wykonane, karta zwraca '**9000**'.

— Jeżeli podpis jest zweryfikowany negatywnie, zwróconym stanem przetwarzania jest **'6688'**. Proces weryfikacji opisano w dodatku 11.

— Jeżeli nie wybrano klucza publicznego, zwróconym stanem przetwarzania jest **'6A88'**.

— Jeżeli brakuje niektórych oczekiwanych obiektów danych (jak określone powyżej), zwracany jest stan przetwarzania **'6987'**. To może się zdarzyć, gdy brakuje jednego z wymaganych znaczników.

— Jeżeli kod skrótu nie jest dostępny dla przetwarzania polecenia (w wyniku poprzedniego polecenia PSO: Hash), zwróconym stanem przetwarzania jest **'6985'**.

— Jeżeli pewne obiekty danych są nieprawidłowe, zwróconym stanem przetwarzania jest **'6988'**. To może się zdarzyć, gdy długość jednego z wymaganych obiektów danych jest nieprawidłowa.

— Jeżeli wybrany klucz publiczny uznany jest za uszkodzony, zwróconym stanem przetwarzania jest **'6400'** lub **'6581'**.

3.5.16 *PROCESS DSRC MESSAGE*

Polecenia tego używa się do weryfikowania integralności i autentyczności komunikatu DSRC oraz odszyfrowania danych przekazywanych z VU do organu kontrolnego lub warsztatu poprzez łącze DSRC. Karta wyprowadza klucz szyfrujący oraz klucz MAC stosowane do zabezpieczenia komunikatu DSRC zgodnie z opisem w dodatku 11 część B rozdział 13.

Tylko karta kontrolna i karta warsztatowa są zobowiązane obsługiwać to polecenie w DF Tachograph_G2.

Inne rodzaje kart do tachografów mogą, ale nie muszą realizować tego polecenia, lecz nie mogą mieć klucza głównego DSRC. Dlatego też karty te nie mogą wykonać pomyślnie polecenia, ale kończą je odpowiednim kodem błędu.

Polecenie może, ale nie musi być dostępne w MF lub DF Tachograph. W takim przypadku polecenie zostaje zakończone odpowiednim kodem błędu.

TCS_135 Klucz główny DSRC jest dostępny tylko w DF Tachograph_G2, tzn. karta kontrolna i karta warsztatowa obsługują pomyślne wykonanie polecenia tylko w DF Tachograph_G2.

TCS_136 Polecenie służy jedynie do odszyfrowania danych i weryfikacji kryptograficznej sumy kontrolnej, ale nie ma interpretować danych wejściowych.

TCS_137 Kolejność obiektów danych w polu danych dotyczących polecenia jest ustalona w niniejszej specyfikacji.

TCS_138 **Komunikat polecenia**

Bajt	Długość	Wartość	Opis
CLA	1	'80h'	zastrzeżone CLA
INS	1	'2Ah'	wykonanie operacji zabezpieczającej
P1	1	'80h'	dane reakcji: wartość odkryta
P2	1	'B0h'	dane dotyczące polecenia: wartość odkryta kodowana w BER-TLV i z uwzględnieniem obiektów danych SM
Lc	1	'NNh'	Lc długość następnego pola danych
#6-#(5+L)	L	'87h' + L_{87} + 'XX..XXh'	Kodowany w DER-TLV bajt wskaźnika wypełnienia, a następnie zaszyfrowany payload tachografu. Na potrzeby bajtu wskaźnika wypełnienia używa się wartości '00h' („brak dalszych wskazań" zgodnie z normą ISO/IEC 7816-4:2013 tabela 52). Informacje dotyczące mechanizmu szyfrowania znajdują się w dodatku 11 część B rozdział 13. Dozwolone wartości dla długości L_{87} to wielokrotności długości bloku AES plus 1 dla bajtu wskaźnika wypełnienia, tj. od 17 bajtów do 193 bajtów włącznie. *Uwaga:* zob. ISO/IEC 7816-4:2013 tabela 49 dla obiektów danych SM ze znacznikiem '87h'.
		'81h' + '10h'	kodowany w DER-TLV referencyjny szablon kontrolny, zagnieżdżający konkatenację następujących elementów danych (zob. dodatek 1 DSRCSecurityData oraz dodatek 11 część B rozdział 13): — 4-bajtowy znacznik czasu — 3-bajtowy licznik — 8-bajtowy numer seryjny VU — 1-bajtowa wersja klucza głównego DSRC *Uwaga:* zob. ISO/IEC 7816-4:2013 tabela 49 dla obiektów danych SM ze znacznikiem '81h'.
		'8Eh' + L_{8E} + 'XX..XXh'	Kodowany w DER-TLV MAC nad komunikatem DSRC. Informacje dotyczące algorytmu i obliczania MAC znajdują się w dodatku 11 część B rozdział 13. *Uwaga:* zob. ISO/IEC 7816-4:2013 tabela 49 dla obiektów danych SM ze znacznikiem '8Eh'.

TCS_139 **Komunikat odpowiedzi**

Bajt	Długość	Wartość	Opis
#1-#L	L	'XX..XXh'	nieobecny (w przypadku błędu) lub dane odszyfrowane (wypełnienie usunięte)
SW	2	'XXXXh'	Słowa stanu (SW1, SW2)

— Jeżeli polecenie zostało pomyślnie wykonane, karta zwraca '**9000**'.

— **'6A80'** oznacza nieprawidłowe parametry w polu danych dotyczących polecenia (używane także w przypadku, gdy obiekty danych nie są wysyłane w określonej kolejności).

— **'6A88'** oznacza, że przywołane dane nie są dostępne, tzn. nie jest dostępny powołany klucz główny DSRC.

— **'6900'** oznacza, że nie udało się wykonać weryfikacji kryptograficznej sumy kontrolnej lub odszyfrowywania danych.

4. STRUKTURA KART DO TACHOGRAFÓW

W niniejszym punkcie opisano struktury plików na kartach do tachografów przeznaczonych do gromadzenia dostępnych danych.

Nie stanowi to opisu wewnętrznych struktur właściwych dla producenta, takich jak nagłówki plików, ani sposobu gromadzenia elementów danych tylko do użytku wewnętrznego (takich jak `EuropeanPublicKey`, `CardPrivateKey`, `TdesSessionKey` lub `WorkshopCardPin`) i manipulowania tymi elementami danych.

TCS_140 Karta do tachografu 2. generacji jest hostem dla pliku głównego MF oraz aplikacji tachograficznej 1. generacji i 2. generacji tego samego typu (np. aplikacje karty kierowcy).

TCS_141 Karta do tachografu musi obsługiwać co najmniej minimalną liczbę rekordów określoną dla odpowiednich aplikacji i nie może obsługiwać więcej rekordów niż maksymalna liczba rekordów określona dla odpowiednich aplikacji.

Minimalne i maksymalne liczby rekordów zostały określone w niniejszym rozdziale dla poszczególnych aplikacji.

Jeśli chodzi o warunki zabezpieczenia stosowane w zasadach dostępu w niniejszym rozdziale, zob. rozdział 3.3. Ogólnie tryb dostępu „odczyt" oznacza polecenie READ BINARY z parzystym i (jeżeli obsługiwane) z nieparzystym bajtem INS, z wyjątkiem EF Sensor_Installation_Data na karcie warsztatowej (zob. TCS_156 i TCS_160). Tryb dostępu „aktualizacja" oznacza polecenie Update Binary z parzystym i (jeżeli obsługiwany) z nieparzystym bajtem INS, a tryb dostępu „wybór" – polecenie SELECT.

4.1. Plik główny MF

TCS_142 Po personalizacji plik główny MF ma następującą, trwałą strukturę plików i zasady dostępu do plików:

Uwaga: The short EF identifier SFID podany jest jako liczba dziesiętna, np. wartość 30 odpowiada zapisowi 11110 w systemie binarnym.

			Zasady dostępu	
Plik	**ID pliku**	**SFID**	**Odczyt / Wybór**	**Aktualizacja**
MF	'3F00h'			
├─ EF ICC	'0002h'		ALW	NEV
├─ EF IC	'0005h'		ALW	NEV
├─ EF DIR	'2F00h'	30	ALW	NEV
├─ EF ATR/INFO (conditional)	'2F01h'	29	ALW	NEV
├─ EF Extended_Length (conditional)	'0006h'	28	ALW	NEV
├─ DF Tachograph	'0500h'		SC1	
└─ DF Tachograph_G2			SC1	

W tabeli zastosowano następujący skrót dla warunku zabezpieczenia:

SC1 ALW OR SM-MAC-G2

TCS_143 Wszystkie struktury plików EF są przezroczyste.

TCS_144 Plik główny (MF) ma następującą strukturę danych:

Plik / element danych	Liczba rekordów	Wielkość (w bajtach) Min.	Maks.	Wartości domyślne
MF		*63*	*184*	
EF ICC		*25*	*25*	
CardIccIdentification		*25*	*25*	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00 00}
EF IC		*8*	*8*	
CardChipIdentification		*8*	*8*	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00..00}
EF DIR		*20*	*20*	
See TCS_145		*20*	*20*	{00..00}
EF ATR/INFO		*7*	*128*	
See TCS_146		*7*	*128*	{00..00}
EF EXTENDED_LENGTH		*3*	*3*	
See TCS_147		*3*	*3*	{00..00}
DF Tachograph				
DF Tachograph_G2				

TCS_145 Plik elementarny EF DIR zawiera następujące obiekty danych dotyczące aplikacji: '61 08 4F 06 FF 54 41 43 48 4F 61 08 4F 06 FF 53 4D 52 44 54'

TCS_146 Plik elementarny EF ATR/INFO musi być obecny, jeżeli karta do tachografu wskaże w swojej ATR, że obsługuje pola o rozszerzonej długości. W takim przypadku EF ATR/INFO zawiera obiekt danych z informacjami o rozszerzonej długości (DO'7F66') zgodnie z opisem w normie ISO/IEC 7816-4:2013 pkt 12.7.1.

TCS_147 Plik elementarny EF Extended_Length musi być obecny, jeżeli karta do tachografu wskaże w swojej ATR, że obsługuje pola o rozszerzonej długości. W takim przypadku EF zawiera następujący obiekt danych: '02 01 xx', gdzie wartość „xx" wskazuje, czy pola o rozszerzonej długości są obsługiwane dla protokołu T = 1 lub T = 0.

Wartość '01' oznacza obsługiwanie pola o rozszerzonej długości dla protokołu T = 1.

Wartość '10' oznacza obsługiwanie pola o rozszerzonej długości dla protokołu T = 0.

Wartość '11' oznacza obsługiwanie pola o rozszerzonej długości dla protokołu T = 1 i T = 0.

4.2. Aplikacje karty kierowcy

4.2.1 *Aplikacja karty kierowcy 1. generacji*

TCS_148 Po personalizacji aplikacja karty kierowcy 1. generacji ma trwałą strukturę plików i zasady dostępu do plików, jak określono poniżej:

		Zasady dostępu		
Plik	**ID pliku**	**Odczyt**	**Wybór**	**Aktualizacja**
└─DF Tachograph	'0500h'		SC1	
├─EF Application_Identification	'0501h'	SC2	SC1	NEV
├─EF Card_Certificate	'C100h'	SC2	SC1	NEV
├─EF CA_Certificate	'C108h'	SC2	SC1	NEV
├─EF Identification	'0520h'	SC2	SC1	NEV
├─EF Card_Download	'050Eh'	SC2	SC1	SC1
├─EF Driving_Licence_Info	'0521h'	SC2	SC1	NEV
├─EF Events_Data	'0502h'	SC2	SC1	SC3
├─EF Faults_Data	'0503h'	SC2	SC1	SC3
├─EF Driver_Activity_Data	'0504h'	SC2	SC1	SC3
├─EF Vehicles_Used	'0505h'	SC2	SC1	SC3
├─EF Places	'0506h'	SC2	SC1	SC3
├─EF Current_Usage	'0507h'	SC2	SC1	SC3
├─EF Control_Activity_Data	'0508h'	SC2	SC1	SC3
└─EF Specific_Conditions	'0522h'	SC2	SC1	SC3

W tabeli zastosowano następujące skróty dla warunków bezpieczeństwa:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

TCS_149 Wszystkie struktury plików EF są przezroczyste.

TCS_150 Aplikacja karty kierowcy 1. generacji ma następującą strukturę danych:

Plik / element danych	Liczba rekordów	Wielkość (w bajtach) Min.	Wielkość (w bajtach) Maks.	Wartości domyślne
DF Tachograph		*11378*	*24926*	
EF Application_Identification		*10*	*10*	
DriverCardApplicationIdentification		*10*	*10*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*864*	*1728*	
CardEventData		*864*	*1728*	
cardEventRecords	6	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				

├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
└CardDriverActivity		*5548*	*13780*	
├─activityPointerOldestDayRecord		2	2	{00 00}
├─activityPointerNewestRecord		2	2	{00 00}
└─activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*2606*	*6202*	
└CardVehiclesUsed		*2606*	*6202*	
├─vehiclePointerNewestRecord		2	2	{00 00}
└─cardVehicleRecords		*2604*	*6200*	
└─CardVehicleRecord	n_3	*31*	*31*	
├─vehicleOdometerBegin		3	3	{00..00}
├─vehicleOdometerEnd		3	3	{00..00}
├─vehicleFirstUse		4	4	{00..00}
├─vehicleLastUse		4	4	{00..00}
├─vehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
└─vuDataBlockCounter		2	2	{00 00}
EF Places		*841*	*1121*	
└CardPlaceDailyWorkPeriod		*841*	*1121*	
├─placePointerNewestRecord		1	1	{00}
└─placeRecords		*840*	*1120*	
└─PlaceRecord	n_4	*10*	*10*	
├─entryTime		4	4	{00..00}
├─entryTypeDailyWorkPeriod		1	1	{00}
├─dailyWorkPeriodCountry		1	1	{00}
├─dailyWorkPeriodRegion		1	1	{00}
└─vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├─sessionOpenTime		4	4	{00..00}
└─sessionOpenVehicle				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├─controlType		1	1	{00}
├─controlTime		4	4	{00..00}
├─controlCardNumber				
├─cardType		1	1	{00}
├─cardIssuingMemberState		1	1	{00}
└─cardNumber		16	16	{20..20}
├─controlVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─controlDownloadPeriodBegin		4	4	{00..00}
└─controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*280*	*280*	
└SpecificConditionRecord	56	*5*	*5*	
├─entryTime		4	4	{00..00}
└─SpecificConditionType		1	1	{00}

TCS_151 W tabeli poniżej podano wartości odnoszące się do tabeli powyżej, wyznaczające minimalne i maksymalne liczby rekordów, które musi stosować struktura danych karty kierowcy dla aplikacji 1. generacji:

		Min.	**Maks.**
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 bajty (28 dni * 93 zmiany czynności)	13 776 bajtów (28 dni * 240 zmian czynności)

4.2.2 *Aplikacja karty kierowcy 2. generacji*

TCS_152 Po personalizacji aplikacja karty kierowcy 2. generacji ma trwałą strukturę plików i zasady dostępu do plików, jak określono poniżej.

Uwaga: .The short EF identifier SFID podany jest jako liczba dziesiętna, np. wartość 30 odpowiada zapisowi 11110 w systemie binarnym.

			Zasady dostępu	
Plik	**ID pliku**	**SFID**	**Odczyt/ Wybór**	**Aktualizacja**
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	'0501h'	1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─EF CardSignCertificate	'C101h'	3	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	NEV
├─EF Identification	'0520h'	6	SC1	NEV
├─EF Card_Download	'050Eh'	7	SC1	SC1
├─EF Driving_Licence_Info	'0521h'	10	SC1	NEV
├─EF Events_Data	'0502h'	12	SC1	SM-MAC-G2
├─EF Faults_Data	'0503h'	13	SC1	SM-MAC-G2
├─EF Driver_Activity_Data	'0504h'	14	SC1	SM-MAC-G2
├─EF Vehicles_Used	'0505h'	15	SC1	SM-MAC-G2
├─EF Places	'0506h'	16	SC1	SM-MAC-G2
├─EF Current_Usage	'0507h'	17	SC1	SM-MAC-G2
├─EF Control_Activity_Data	'0508h'	18	SC1	SM-MAC-G2
├─EF Specific_Conditions	'0522h'	19	SC1	SM-MAC-G2
├─EF VehicleUnits_Used	'0523h'	20	SC1	SM-MAC-G2
└─EF GNSS_Places	'0524h'	21	SC1	SM-MAC-G2

W tabeli zastosowano następujący skrót dla warunku zabezpieczenia:

SC1 ALW OR SM-MAC-G2

TCS_153 Wszystkie struktury plików EF są przezroczyste.

TCS_154 Aplikacja karty kierowcy 2. generacji ma następującą strukturę danych:

Plik / element danych	Liczba rekordów	Wielkość (w bajtach) Min.	Maks.	Wartości domyślne
DF Tachograph_G2		*19510*	*39306*	
EF Application_Identification		*15*	*15*	
DriverCardApplicationIdentification		*15*	*15*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00 00}
noOfSpecificConditionRecords		2	2	{00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*1584*	*3168*	
CardEventData		*1584*	*3168*	
cardEventRecords	11	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	

faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
CardDriverActivity		*5548*	*13780*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*4034*	*9602*	
CardVehiclesUsed		*4034*	*9602*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*4032*	*9600*	
CardVehicleRecord	n_3	*48*	*48*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
vehicleIdentificationNumber		17	17	{20..20}
EF Places		*1766*	*2354*	
CardPlaceDailyWorkPeriod		*1766*	*2354*	
placePointerNewestRecord		2	2	{00 00}
placeRecords		*1764*	*2352*	
PlaceRecord	n_4	*21*	*21*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
entryGNSSPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

EF Specific_Conditions		*282*	*562*	
SpecificConditions		*282*	*562*	
conditionPointerNewestRecord		2	2	{00 00}
specificConditionRecords		*280*	*560*	
SpecificConditionRecord	n_9	*5*	*5*	
entryTime		4	4	{00..00}
specificConditionType		1	1	{00}
EF VehicleUnits_Used		*842*	*2002*	
CardVehicleUnitsUsed		*842*	*2002*	
vehicleUnitPointerNewestRecord		2	2	{00 00}
cardVehicleUnitRecords		*840*	*2000*	
CardVehicleUnitRecord	n_7	*10*	*10*	
timeStamp		4	4	{00..00}
manufacturerCode		1	1	{00}
deviceID		1	1	{00}
vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*3782*	*5042*	
GNSSContinuousDriving		*3782*	*5042*	
gnssCDPointerNewestRecord		2	2	{00 00}
gnssContinuousDrivingRecords		3780	5040	{00}
GNSSContinuousDrivingRecord	n_8	*15*	*15*	
timeStamp		4	4	{00..00}
gnssPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}

TCS_155 W tabeli poniżej podano wartości odnoszące się do tabeli powyżej, wyznaczające minimalne i maksymalne liczby rekordów, które musi stosować struktura danych karty kierowcy dla aplikacji 2. generacji:

		Min.	**Maks.**
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 bajty (28 dni * 93 zmiany czynności)	13 776 bajtów (28 dni * 240 zmian czynności)
n_7	NoOfCardVehicleUnitRecords	84	200
n_8	NoOfGNSSCDRecords	252	336
n_9	NoOfSpecificConditionRecords	56	112

4.3. Aplikacje karty warsztatowej

4.3.1 *Aplikacja karty warsztatowej 1. generacji*

TCS_156 Po personalizacji aplikacja karty warsztatowej 1. generacji ma trwałą strukturę plików i zasady dostępu do plików, jak określono poniżej.

		Zasady dostępu		
Plik	**ID pliku**	**Odczyt**	**Wybór**	**Aktualizacja**
└─DF Tachograph	'0500h'		SC1	
├─EF Application_Identification	'0501h'	SC2	SC1	NEV
├─EF Card_Certificate	'C100h'	SC2	SC1	NEV
├─EF CA_Certificate	'C108h'	SC2	SC1	NEV
├─EF Identification	'0520h'	SC2	SC1	NEV
├─EF Card_Download	'0509h'	SC2	SC1	**SC1**
├─EF Calibration	'050Ah'	SC2	SC1	SC3
├─EF Sensor_Installation_Data	'050Bh'	**SC4**	SC1	NEV
├─EF Events_Data	'0502h'	SC2	SC1	SC3
├─EF Faults_Data	'0503h'	SC2	SC1	SC3
├─EF Driver_Activity_Data	'0504h'	SC2	SC1	SC3
├─EF Vehicles_Used	'0505h'	SC2	SC1	SC3
├─EF Places	'0506h'	SC2	SC1	SC3
├─EF Current_Usage	'0507h'	SC2	SC1	SC3
├─EF Control_Activity_Data	'0508h'	SC2	SC1	SC3
└─EF Specific_Conditions	'0522h'	SC2	SC1	SC3

W tabeli zastosowano następujące skróty dla warunków bezpieczeństwa:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC4 Dla polecenia READ BINARY z parzystym bajtem INS:

(PLAIN-C AND SM-R-ENC-G1) OR (SM-C-MAC-G1 AND SM-R-ENC-MAC-G1) OR

(SM-C-MAC-G2 AND SM-R-ENC-MAC-G2)

Dla polecenia READ BINARY z nieparzystym bajtem INS (jeżeli obsługiwane): NEV

TCS_157 Wszystkie struktury plików EF są przezroczyste.

TCS_158 Aplikacja karty warsztatowej 1. generacji ma następującą strukturę danych:

Plik / element danych	Liczba rekordów	Wielkość (w bajtach) Min.	Maks.	Wartości domyślne
DF Tachograph		*11055*	*29028*	
EF Application_Identification		*11*	*11*	
WorkshopCardApplicationIdentification		*11*	*11*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
noOfCalibrationRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*9243*	*26778*	
WorkshopCardCalibrationData		*9243*	*26778*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		1	1	{00}
calibrationRecords		*9240*	*26775*	
WorkshopCardCalibrationRecord	n_5	*105*	*105*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}
oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}

EF Sensor_Installation_Data		*16*	*16*	
└SensorInstallationSecData		16	16	{00..00}
EF Events_Data		*432*	*432*	
└CardEventData		*432*	*432*	
└cardEventRecords	6	*72*	*72*	
└CardEventRecord	n_1	*24*	*24*	
├eventType		1	1	{00}
├eventBeginTime		4	4	{00..00}
├eventEndTime		4	4	{00..00}
└eventVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
└CardFaultData		*288*	*288*	
└cardFaultRecords	2	*144*	*144*	
└CardFaultRecord	n_2	*24*	*24*	
├faultType		1	1	{00}
├faultBeginTime		4	4	{00..00}
├faultEndTime		4	4	{00..00}
└faultVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
└CardDriverActivity		*202*	*496*	
├activityPointerOldestDayRecord		2	2	{00 00}
├activityPointerNewestRecord		2	2	{00 00}
└activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*126*	*250*	
└CardVehiclesUsed		*126*	*250*	
├vehiclePointerNewestRecord		2	2	{00 00}
└cardVehicleRecords		*124*	*248*	
└CardVehicleRecord	n_3	*31*	*31*	
├vehicleOdometerBegin		3	3	{00..00}
├vehicleOdometerEnd		3	3	{00..00}
├vehicleFirstUse		4	4	{00..00}
├vehicleLastUse		4	4	{00..00}
├vehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
└vuDataBlockCounter		2	2	{00 00}
EF Places		*61*	*81*	
└CardPlaceDailyWorkPeriod		*61*	*81*	
├placePointerNewestRecord		1	1	{00}
└placeRecords		*60*	*80*	
└PlaceRecord	n_4	*10*	*10*	
├entryTime		4	4	{00..00}
├entryTypeDailyWorkPeriod		1	1	{00}
├dailyWorkPeriodCountry		1	1	{00}
├dailyWorkPeriodRegion		1	1	{00}
└vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├sessionOpenTime		4	4	{00..00}
└sessionOpenVehicle				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}

EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*10*	*10*	
SpecificConditionRecord	2	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_159 W tabeli poniżej podano wartości odnoszące się do tabeli powyżej, wyznaczające minimalne i maksymalne liczby rekordów, które musi stosować struktura danych karty warsztatowej dla aplikacji 1. generacji:

		Min.	**Maks.**
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 bajtów (1 dzień * 93 zmiany czynności)	492 bajty (1 dzień * 240 zmian czynności)

4.3.2 *Aplikacja karty warsztatowej 2. generacji*

TCS_160 Po personalizacji aplikacja karty warsztatowej 2. generacji ma trwałą strukturę plików i zasady dostępu do plików, jak określono poniżej.

Uwaga: .The short EF identifier SFID podany jest jako liczba dziesiętna, np. wartość 30 odpowiada zapisowi 11110 w systemie binarnym.

			Zasady dostępu		
Plik	**ID pliku**	**SFID**	**Odczyt**	**Wybór**	**Aktualizacja**
└─DF Tachograph_G2			SC1	SC1	
├─EF Application_Identification	'0501h'	1	SC1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	SC1	NEV
├─EF CardSignCertificate	'C101h'	3	SC1	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	SC1	NEV
├─EF Identification	'0520h'	6	SC1	SC1	NEV
├─EF Card_Download	'0509h'	7	SC1	SC1	SC1
├─EF Calibration	'050Ah'	10	SC1	SC1	SM-MAC-G2
├─EF Sensor_Installation_Data	'050Bh'	11	**SC5**	SM-MAC-G2	NEV
├─EF Events_Data	'0502h'	12	SC1	SC1	SM-MAC-G2
├─EF Faults_Data	'0503h'	13	SC1	SC1	SM-MAC-G2
├─EF Driver_Activity_Data	'0504h'	14	SC1	SC1	SM-MAC-G2
├─EF Vehicles_Used	'0505h'	15	SC1	SC1	SM-MAC-G2
├─EF Places	'0506h'	16	SC1	SC1	SM-MAC-G2
├─EF Current_Usage	'0507h'	17	SC1	SC1	SM-MAC-G2
├─EF Control_Activity_Data	'0508h'	18	SC1	SC1	SM-MAC-G2
├─EF Specific_Conditions	'0522h'	19	SC1	SC1	SM-MAC-G2
├─EF VehicleUnits_Used	'0523h'	20	SC1	SC1	SM-MAC-G2
└─EF GNSS_Places	'0524h'	21	SC1	SC1	SM-MAC-G2

W tabeli zastosowano następujące skróty dla warunków bezpieczeństwa:

SC1 ALW OR SM-MAC-G2

SC5 Dla polecenia Read Binary z parzystym bajtem INS: SM-C-MAC-G2 AND SM-R-ENC-MAC-G2

Dla polecenia Read Binary z nieparzystym bajtem INS (jeżeli obsługiwane): NEV

TCS_161 Wszystkie struktury plików EF są przezroczyste.

TCS_162 Aplikacja karty warsztatowej 2. generacji ma następującą strukturę danych:

Plik / element danych	Liczba rekordów	Wielkość (w bajtach) Min.	Maks.	Wartości domyślne
DF Tachograph_G2		*17837*	*47163*	
EF Application_Identification		*17*	*17*	
WorkshopCardApplicationIdentification		*17*	*17*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00}
noOfCalibrationRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00..00}
noOfSpecificConditionRecords		2	2	{00..00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*14788*	*42844*	
WorkshopCardCalibrationData		*14788*	*42844*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		2	2	{00}
calibrationRecords		*14784*	*42840*	
WorkshopCardCalibrationRecord	n_5	*168*	*168*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}

oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}
sensorGNSSSerialNumber		8	8	{00..00}
rcmSerialNumber		8	8	{00..00}
vuAbility		1	1	{00}
sealDataCard		46	46	
noOfSealRecords		1	1	{00}
SealRecords		45	45	
SealRecord	5	9	9	
equipmentType		1	1	{00}
extendedSealIdentifier		8	8	{00..00}
EF Sensor_Installation_Data		*18*	*102*	
SensorInstallationSecData		18	102	{00..00}
EF Events_Data		*792*	*792*	
CardEventData		*792*	*792*	
cardEventRecords	11	*72*	*72*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
CardFaultData		*288*	*288*	
cardFaultRecords	2	*144*	*144*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
CardDriverActivity		*202*	*496*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*194*	*386*	
CardVehiclesUsed		*194*	*386*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*192*	*384*	
CardVehicleRecord	n_3	*48*	*48*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
vehicleIdentificationNumber		*17*	17	{20..20}
EF Places		*128*	*170*	

└CardPlaceDailyWorkPeriod		*128*	*170*	
├placePointerNewestRecord		2	2	{00 00}
└placeRecords		*126*	*168*	
└PlaceRecord	n_4	*21*	*21*	
├entryTime		4	4	{00..00}
├entryTypeDailyWorkPeriod		1	1	{00}
├dailyWorkPeriodCountry		1	1	{00}
├dailyWorkPeriodRegion		1	1	{00}
├vehicleOdometerValue		3	3	{00..00}
└entryGNSSPlaceRecord		11	11	{00..00}
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├sessionOpenTime		4	4	{00..00}
└sessionOpenVehicle				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├controlType		1	1	{00}
├controlTime		4	4	{00..00}
├controlCardNumber				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├controlVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├controlDownloadPeriodBegin		4	4	{00..00}
└controlDownloadPeriodEnd		4	4	{00..00}
EF VehicleUnits_Used		*42*	*42*	
└CardVehicleUnitsUsed		*42*	*82*	
├vehicleUnitPointerNewestRecord		2	2	{00 00}
└cardVehicleUnitRecords		*40*	*80*	
└CardVehicleUnitRecord	n_7	*10*	*10*	
├timeStamp		4	4	{00..00}
├manufacturerCode		1	1	{00..00}
├deviceID		1	1	{00..00}
└vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*262*	*362*	
└GNSSContinuousDriving		*262*	*362*	
├gnssCDPointerNewestRecord		2	2	{00 00}
└gnssContinuousDrivingRecords		*260*	*360*	
└GNSSContinuousDrivingRecord	n_8	*15*	*15*	
├timeStamp		4	4	{00..00}
└gnssPlaceRecord		11	11	
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Specific_Conditions		*12*	*22*	
└SpecificConditions		*12*	*22*	
├conditionPointerNewestRecord		2	2	{00 00}
└specificConditionRecords		10	20	
└SpecificConditionRecord	n_9	*5*	*5*	
├entryTime		4	4	{00..00}
└specificConditionType		1	1	{00}

TCS_163 W tabeli poniżej podano wartości odnoszące się do tabeli powyżej, wyznaczające minimalne i maksymalne liczby rekordów, które musi stosować struktura danych karty warsztatowej dla aplikacji 2. generacji:

		Min.	Maks.
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 bajtów (1 dzień * 93 zmiany czynności)	492 bajty (1 dzień * 240 zmian czynności)
n_7	NoOfCardVehicleUnitRecords	4	8
n_8	NoOfGNSSCDRecords	18	24
n_9	NoOfSpecificConditionRecords	2	4

4.4. Aplikacje karty kontrolnej

4.4.1 *Aplikacja karty kontrolnej 1. generacji*

TCS_164 Po personalizacji aplikacja karty kontrolnej 1. generacji ma trwałą strukturę plików i zasady dostępu do plików, jak określono poniżej.

		Zasady dostępu		
Plik	**ID pliku**	**Odczyt**	**Wybór**	**Aktualizacja**
└─DF Tachograph	'0500h'			
├─EF Application_Identification	'0501h'	SC2	SC1	NEV
├─EF Card_Certificate	'C100h'	SC2	SC1	NEV
├─EF CA_Certificate	'C108h'	SC2	SC1	NEV
├─EF Identification	'0520h'	**SC6**	SC1	NEV
└─EF Controller_Activity_Data	'050Ch'	SC2	SC1	SC3

W tabeli zastosowano następujące skróty dla warunków bezpieczeństwa:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC6 EXT-AUT-G1 OR SM-MAC-G1 OR SM-MAC-G2

TCS_165 Wszystkie struktury plików EF są przezroczyste.

TCS_166 Aplikacja karty kontrolnej 1. generacji ma następującą strukturę danych:

Plik / element danych	Liczba rekordów	Wielkość (w bajtach) Min.	Maks.	
DF Tachograph		*11186*	*24526*	
EF Application_Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_167 W tabeli poniżej podano wartości odnoszące się do tabeli powyżej, wyznaczające minimalne i maksymalne liczby rekordów, które musi stosować struktura danych karty kontrolnej dla aplikacji 1. generacji:

		Min.	Mask.
n_7	NoOfControlActivityRecords	230	520

4.4.2 *Aplikacja karty kontrolnej 2. generacji*

TCS_168 Po personalizacji aplikacja karty kontrolnej 2. generacji ma trwałą strukturę plików i zasady dostępu do plików, jak określono poniżej.

Uwaga: .The short EF identifier SFID podany jest jako liczba dziesiętna, np. wartość 30 odpowiada zapisowi 11110 w systemie binarnym.

			Zasady dostępu	
Plik	**ID pliku**	**SFID**	**Odczyt / Wybór**	**Aktualizacja**
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	'0501h'	1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	NEV
├─EF Identification	'0520h'	6	SC1	NEV
└─EF Controller_Activity_Data	'050Ch'	14	SC1	SM-MAC-G2

W tabeli zastosowano następujący skrót dla warunku zabezpieczenia:

SC1 ALW OR SM-MAC-G2

TCS_169 Wszystkie struktury plików EF są przezroczyste.

TCS_170 Aplikacja karty kontrolnej 2. generacji ma następującą strukturę danych:

Plik / element danych	Liczba rekordów	Wielkość (w bajtach) Min.	Maks.	
DF Tachograph_G2		*11410*	*25161*	
EF Application_Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_171 W tabeli poniżej podano wartości odnoszące się do tabeli powyżej, wyznaczające minimalne i maksymalne liczby rekordów, które musi stosować struktura danych karty kontrolnej dla aplikacji 2. generacji:

		Min.	Maks.
n_7	NoOfControlActivityRecords	230	520

4.5. Aplikacje karty firmowej

4.5.1 *Aplikacja karty firmowej 1. generacji*

TCS_172 Po personalizacji aplikacja karty firmowej 1. generacji ma trwałą strukturę plików i zasady dostępu do plików, jak określono poniżej.

		Zasady dostępu		
Plik	**ID pliku**	**Odczyt**	**Wybór**	**Aktualizacja**
└DF Tachograph	'0500h'		SC1	
├EF Application_Identification	'0501h'	SC2	SC1	NEV
├EF Card_Certificate	'C100h'	SC2	SC1	NEV
├EF CA_Certificate	'C108h'	SC2	SC1	NEV
├EF Identification	'0520h'	**SC6**	SC1	NEV
└EF Company_Activity_Data	'050Dh'	SC2	SC1	SC3

W tabeli zastosowano następujące skróty dla warunków bezpieczeństwa:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC6 EXT-AUT-G1 OR SM-MAC-G1 OR SM-MAC-G2

TCS_173 Wszystkie struktury plików EF są przezroczyste.

TCS_174 Aplikacja karty firmowej 1. generacji ma następującą strukturę danych:

Plik / element danych	**Liczba rekordów**	**Wielkość (w bajtach) Min.**	**Maks.**	**Wartości domyślne**
└DF Tachograph		*11114*	*24454*	
├EF Application_Identification		*5*	*5*	
│└CompanyCardApplicationIdentification		*5*	*5*	
│├typeOfTachographCardId		1	1	{00}
│├cardStructureVersion		2	2	{00 00}
│└noOfCompanyActivityRecords		2	2	{00 00}
├EF Card_Certificate		*194*	*194*	
│└CardCertificate		194	194	{00..00}
├EF CA_Certificate		*194*	*194*	
│└MemberStateCertificate		194	194	{00..00}
├EF Identification		*139*	*139*	
│├CardIdentification		*65*	*65*	
││├cardIssuingMemberState		1	1	{00}
││├cardNumber		16	16	{20..20}
││├cardIssuingAuthorityName		36	36	{00, 20..20}
││├cardIssueDate		4	4	{00..00}
││├cardValidityBegin		4	4	{00..00}
││└cardExpiryDate		4	4	{00..00}
│└CompanyCardHolderIdentification		*74*	*74*	
│├companyName		36	36	{00, 20..20}
│├companyAddress		36	36	{00, 20..20}
│└cardHolderPreferredLanguage		2	2	{20 20}
└EF Company_Activity_Data		*10582*	*23922*	
└CompanyActivityData		*10582*	*23922*	
├companyPointerNewestRecord		2	2	{00 00}
└companyActivityRecords		*10580*	*23920*	
└companyActivityRecord	n_8	*46*	*46*	
├companyActivityType		1	1	{00}
├companyActivityTime		4	4	{00..00}
├cardNumberInformation				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├vehicleRegistrationInformation				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├downloadPeriodBegin		4	4	{00..00}
└downloadPeriodEnd		4	4	{00..00}

TCS_175 W tabeli poniżej podano wartości odnoszące się do tabeli powyżej, wyznaczające minimalne i maksymalne liczby rekordów, które musi stosować struktura danych karty firmowej dla aplikacji 1. generacji:

		Min.	**Maks.**
n_8	NoOfCompanyActivityRecords	230	520

4.5.2 *Aplikacja karty firmowej 2. generacji*

TCS_176 Po personalizacji aplikacja karty firmowej 2. generacji ma trwałą strukturę plików i zasady dostępu do plików, jak określono poniżej.

Uwaga: Krótki identyfikator EF (SFID) podany jest jako liczba dziesiętna, np. wartość 30 odpowiada zapisowi 11110 w systemie binarnym.

			Zasady dostępu	
Plik	**ID pliku**	**SFID**	**Odczyt / Wybór**	**Aktualizacja**
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	'0501h'	1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	NEV
├─EF Identification	'0520h'	6	SC1	NEV
└─EF Company_Activity_Data	'050Dh'	14	SC1	SM-MAC-G2

W tabeli zastosowano następujący skrót dla warunku zabezpieczenia:

SC1 ALW OR SM-MAC-G2

TCS_177 Wszystkie struktury plików EF są przezroczyste.

TCS_178 Aplikacja karty firmowej 2. generacji ma następującą strukturę danych:

Plik / element danych	Liczba rekordów	Wielkość (w bajtach) Min.	Maks.	Wartości domyślne
DF Tachograph_G2		*11338*	*25089*	
EF Application_Identification		*5*	*5*	
CompanyCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfCompanyActivityRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*139*	*139*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		*74*	*74*	
companyName		36	36	{00, 20..20}
companyAddress		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Company_Activity_Data		*10582*	*23922*	
CompanyActivityData		*10582*	*23922*	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		*10580*	*23920*	
companyActivityRecord	n_8	*46*	*46*	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
cardNumberInformation				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
downloadPeriodBegin		4	4	{00..00}
downloadPeriodEnd		4	4	{00..00}

TCS_179 W tabeli poniżej podano wartości odnoszące się do tabeli powyżej, wyznaczające minimalne i maksymalne liczby rekordów, które musi stosować struktura danych karty firmowej dla aplikacji 2. generacji:

		Min.	Maks.
n_8	NoOfCompanyActivityRecords	230	520

Dodatek 3

PIKTOGRAMY

PIC_001 Tachograf może opcjonalnie używać następujących piktogramów i kombinacji piktogramów (lub piktogramów i kombinacji wystarczająco do nich podobnych, aby można je było z nimi jednoznacznie identyfikować):

1. PODSTAWOWE PIKTOGRAMY

	Osoby	**Operacje**	**Tryby pracy**
	firma		tryb firmowy
	kontroler	kontrola	tryb kontrolny
	kierowca	prowadzenie pojazdu	tryb eksploatacyjny
	warsztat/stanowisko badań	przegląd/kalibracja	tryb kalibracyjny
	producent		
	Czynności	**Czas trwania**	
	gotowość	bieżący okres gotowości	
	prowadzenie pojazdu	nieprzerwany czas prowadzenia pojazdu	
	odpoczynek	bieżący okres odpoczynku	
	inna praca	bieżący okres pracy	
	przerwa	skumulowany czas przerwy	
	nieznane		
	Urządzenie	**Funkcje**	
	szczelina karty kierowcy		
	szczelina karty współkierowcy		
	karta		
	zegar		
	wyświetlacz	wyświetlanie	
	zewnętrzne gromadzenie danych	pobieranie danych	
	zasilanie		
	drukarka/wydruk	drukowanie	
	czujnik		
	rozmiar opon		
	pojazd/przyrząd rejestrujący		
	urządzenie GNSS		
	urządzenie wykrywania na odległość		
	interfejs ITS		
	Warunki szczególne		
	poza zakresem		
	przeprawa promowa/przejazd kolejowy		

Różne

!	zdarzenia	⤫	usterki
⏵|	początek dziennego okresu pracy	|⏵	koniec dziennego okresu pracy
●	umiejscowienie		
M	ręczne wprowadzenie czynności kierowcy		
🔒	zabezpieczenie		
>	prędkość		
🕒	godzina		
Σ	razem/podsumowanie		

Kwalifikatory

24h	dobowo
I	tygodniowo
II	dwa tygodnie
+	od lub do

2. KOMBINACJE PIKTOGRAMÓW

Różne

🏛●	miejsce kontroli		
●⏵|	miejsce rozpoczęcia dziennego okresu pracy	|⏵●	miejsce zakończenia dziennego okresu pracy
🕒+	od godziny	+🕒	do godziny
🚙+	z pojazdu		
OUT+	początek poza zakresem	+OUT	koniec poza zakresem

Karty

👤💳	karta kierowcy
🏢💳	karta firmowa
🏛💳	karta kontrolna
🔧💳	karta warsztatowa
💳– – –	brak karty

Prowadzenie pojazdu

👤👤	załoga
👤 I	czas prowadzenia w ciągu jednego tygodnia
👤 II	czas prowadzenia w ciągu dwóch tygodni

Wydruki

24h 💳🖨	wydruk dzienny czynności kierowcy z karty
24h 🚙🖨	wydruk dzienny czynności kierowcy z VU
! ⤫ 💳🖨	wydruk zdarzeń i usterek z karty
! ⤫ 🚙🖨	wydruk zdarzeń i usterek z VU
🔧🕒🖨	wydruk danych technicznych
>>🖨	wydruk przekroczenia prędkości

Zdarzenia

	włożenie nieważnej karty
	konflikt kart
	nakładające się czasy
	prowadzenie pojazdu bez prawidłowej karty
	włożenie karty podczas prowadzenia pojazdu
	sesja ostatniej karty niezamknięta prawidłowo
	przekroczenie prędkości
	przerwa w zasilaniu
	błąd danych dotyczących ruchu
	konflikt ruchu pojazdu
	naruszenie zabezpieczenia
	korekta czasu (w warsztacie)
	kontrola przekroczenia prędkości

Usterki

	usterka karty (szczelina karty kierowcy)
	usterka karty (szczelina karty współkierowcy)
	usterka wyświetlacza
	usterka pobierania danych
	usterka drukarki
	usterka czujnika
	usterka wewnętrzna VU
	usterka GNSS
	usterka urządzenia wykrywania na odległość

Procedura ręcznego wprowadzania danych

	Czy nadal ten sam dzienny okres pracy?
	Czy koniec poprzedniego okresu pracy?
	potwierdź lub wprowadź miejsce zakończenia okresu pracy
	wprowadź godzinę rozpoczęcia
	wprowadź miejsce rozpoczęcia okresu pracy

Uwaga: dodatkowe kombinacje piktogramów używane do tworzenia bloków wydruków lub identyfikatorów zapisów określono w dodatku 4.

Dodatek 4

WYDRUKI

SPIS TREŚCI

1. ZASADY OGÓLNE

Wszystkie wydruki tworzy się poprzez zbudowanie łańcucha różnych bloków danych, w miarę możliwości identyfikowanych identyfikatorem bloku.

Blok danych składa się z jednego lub więcej rekordów, o ile możliwe identyfikowanych identyfikatorem rekordu.

PRT_001 Jeżeli identyfikator bloku bezpośrednio poprzedza identyfikator rekordu, identyfikator rekordu nie jest drukowany.

PRT_002 W przypadku gdy pozycja danych nie jest znana lub nie może być drukowana z uwagi na prawa dostępu do danych, zamiast tej pozycji drukowane są spacje.

PRT_003 Jeżeli zawartość pełnego wiersza nie jest znana lub nie wymaga drukowania, cały wiersz jest pomijany.

PRT_004 Numeryczne pola danych są drukowane z wyrównaniem do prawej strony, ze spacją oddzielającą tysiące i miliony i bez zer z lewej strony.

PRT_005 Pola danych tekstowych są drukowane z wyrównaniem do lewej strony i wypełniane spacjami do długości danej pozycji danych lub w razie potrzeby obcinane do długości danej pozycji (nazwy, nazwiska i adresy).

PRT_006 W przypadku łamania wiersza w związku z długością tekstu pierwszym znakiem w nowym wierszu powinien być znak specjalny (kropka w połowie wysokości wiersza: „•”).

2. SPECYFIKACJA BLOKÓW DANYCH

W tym rozdziale przyjęto następujące konwencje zapisu formatu:

— Znaki drukowane **wytłuszczonym** drukiem oznaczają zwykły tekst, który ma być drukowany (wydruk normalną czcionką),

— Znaki normalną czcionką oznaczają zmienne (piktogramy lub dane), które na wydruku są zastępowane odpowiednimi wartościami,

— Nazwy zmiennych wypełniono znakami podkreślenia w celu pokazania długości pozycji danych dostępnej dla zmiennej,

— Daty podawane są w układzie „dd/mm/rrrr” (dzień, miesiąc, rok). Dopuszczalny jest także układ „dd.mm.rrrr”.

— Wyrażenie „identyfikacja karty” oznacza następujący zestaw danych: typ karty w postaci kombinacji piktogramów, kod państwa członkowskiego, które wydało kartę, ukośnik prawy i numer karty wraz z numerem wymiany i numerem odnowienia rozdzielonymi spacjami:

P		x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x
Kombinacja piktogramów		Kod państwa wydającego				Pierwsze 14 znaków numeru karty (ewentualnie z numerem kolejnym)														Numer wymiany		Numer odnowienia

PRT_007 W wydrukach korzysta się z następujących bloków danych lub rekordów danych w opisanym poniżej znaczeniu i formacie:

Numer bloku lub rekordu Znaczenie	Data Format
1 ***Data i godzina wydruku dokumentu***	▼ dd/mm/yyyy hh:mm **(UTC)**
2 ***Typ wydruku*** Identyfikator bloku Wydruk kombinacji piktogramu (zob. dodatek 3), ustawienie urządzenia ograniczenia prędkości (tylko wydruk przekroczenia prędkości)	----------▼---------- Picto xxx **km/h**
3 ***Identyfikacja posiadacza karty*** Identyfikator bloku P = piktogram indywidualny Nazwisko posiadacza karty Imię (imiona) posiadacza karty (w stosownych przypadkach) Identyfikacja karty Termin ważności karty (w stosownych przypadkach) oraz numer generacji karty (GEN 1 lub GEN 2) (*)	----------P---------- P Last_Name_____ First_Name_____ Card_Identification_____ dd/mm/yyyy - GEN 2

W przypadku gdy karta nie jest kartą osobistą i nie zawiera nazwiska posiadacza karty, zamiast nazwiska drukuje się nazwę przedsiębiorstwa, warsztatu lub organu kontrolnego.

(*) Numer generacji karty może być drukowany tylko przez tachograf inteligentny.

4 ***Identyfikacja pojazdu*** Identyfikator bloku VIN Państwo członkowskie rejestracji i numer VRN	----------▲---------- ▲ VIN_____ Nat/VRN_____
5 ***Identyfikacja VU (przyrządu rejestrującego)*** Identyfikator bloku Nazwa producenta VU Numer części VU Numer generacji VU (*)	----------⊟---------- ⊟ VU_Manufacturer_____ VU_Part_Number__ GEN 2

(*) Numer generacji karty może być drukowany tylko przez tachograf inteligentny.

6 ***Ostatnia kalibracja tachografu*** Identyfikator bloku Nazwa warsztatu Identyfikacja karty warsztatowej Data kalibracji	----------▼---------- ▼ Last_Name_____ Card_Identification_____ ▼ dd/mm/yyyy

7 ***Ostatnia kontrola (przez funkcjonariusza służb kontrolnych)***

Identyfikator bloku
Identyfikacja karty kontrolera
Data, godzina i typ kontroli

```
----------D----------
Card_Identification_____
D dd/mm/yyyy hh:mm ppppp
```

Typ kontroli: Maksymalnie pięć piktogramów. Typ kontroli odpowiada jednemu z poniższych piktogramów (lub ich kombinacji): : Pobieranie danych z karty, : Pobieranie danych z VU, : Drukowanie, : Wyświetlanie, : Kontrola drogowa kalibracji

8 ***Czynności kierowcy zapisane na karcie w kolejności chronologicznej***

Identyfikator bloku
Data zapytania (dzień kalendarzowy będący przedmiotem wydruku) + dzienny licznik obecności karty

```
----------O----------
    dd/mm/yyyy xxx
```

8a *Stan poza zakresem na początku danego dnia* (nie wypełniać, jeżeli nie występuje stan poza zakresem)

```
----------OUT----------
```

8.1 *Okres, w którym nie wkładano karty*
8.1a Identyfikator rekordu (początek okresu)
8.1b *Okres czynności nieznanych*. Godzina rozpoczęcia, czas trwania
8.1c *Czynność wprowadzona ręcznie*.
Piktogram czynności, godzina rozpoczęcia, czas trwania

```
  --------------------
?       hh:mm hhhmm
A    hh:mm hhhmm
```

8.2 *Włożenie karty w szczelinę czytnika S*
Identyfikator rekordu; S = piktogram szczeliny czytnika
Państwo członkowskie rejestracji pojazdu i numer VRN
Stan licznika kilometrów pojazdu przy wkładaniu karty

```
  ---------S---------
 Nat/VRN__________
  x xxx xxx km
```

8.3 *Czynność (przy włożonej karcie)*
Piktogram czynności, godzina rozpoczęcia, czas trwania, status załogi (piktogram załogi, jeżeli ZAŁOGA, puste, jeżeli JEDEN KIEROWCA).

```
A    hh:mm hhhmm OO
```

8.3a *Warunki szczególne*. Godzina wprowadzenia wpisu, piktogram warunku szczególnego (lub kombinacja piktogramów).

```
        hh:mm ---pppp---
```

8.4 *Wyjęcie karty*
Stan licznika kilometrów pojazdu i odległość przebyta od ostatniego włożenia karty, dla którego znany jest stan licznika kilometrów

```
  x xxx xxx km; x xxx km
```

9 ***Czynności kierowcy zapisane na przyrządzie rejestrującym (VU) według szczelin czytnika oraz w kolejności chronologicznej***

Identyfikator bloku
Data zapytania (dzień kalendarzowy będący przedmiotem wydruku)
Stan licznika kilometrów pojazdu o godzinie 00:00 i 24:00

```
----------O----------
       dd/mm/yyyy
x xxx xxx - x xxx xxx km
```

10 ***Czynności wykonane przy karcie w szczelinie czytnika S***

Identyfikator bloku

```
----------S----------
```

10a *Stan poza zakresem na początku danego dnia* (nie wypełniać, jeżeli nie występuje stan poza zakresem)

```
----------OUT----------
```

10.1 *Okres, gdy brak jest karty w szczelinie czytnika S*
Identyfikator rekordu.
Brak karty
Stan licznika kilometrów na początku okresu

```
  --------------------
O---
  x xxx xxx km
```

10.2 *Włożenie karty*
Identyfikator rekordu włożenia karty
Nazwisko kierowcy

```
  --------------------
O Last_Name_____________
```

	Imię kierowcy	First_Name_____
	Identyfikacja karty kierowcy	Card_Identification_____
	Termin ważności karty (w stosownych przypadkach) oraz numer generacji karty (GEN 1 lub GEN 2) (*)	dd/mm/yyyy - GEN 2
	Państwo członkowskie rejestracji i numer VRN poprzednio używanego pojazdu	+Nat/VRN_____
	Data i godzina wyjęcia karty z poprzedniego pojazdu	dd/mm/yyyy hh:mm
	Pusty wiersz	
	Stan licznika kilometrów pojazdu przy wkładaniu karty, wskaźnik pokazujący ręczne wprowadzenie informacji o wykonywaniu czynności (M, jeżeli wprowadzono, puste, jeżeli nie wprowadzono). Jeżeli w dniu wydruku nie włożono karty kierowcy, wówczas w odniesieniu do bloku 10.2 stosuje się wskazania licznika z ostatniego dostępnego włożenia karty, które miało miejsce przed tym dniem.	x xxx xxx **km** **M**
10.3	*Czynność*	
	Piktogram czynności, godzina rozpoczęcia, czas trwania, status załogi (piktogram załogi, jeżeli ZAŁOGA, puste, jeżeli JEDEN KIEROWCA).	A hh:mm hh**h**mm
10.3a	*Warunki szczególne*. Godzina wprowadzenia wpisu, piktogram warunku szczególnego (lub kombinacja piktogramów).	hh:mm ---pppp---
10.4	*Wyjęcie karty lub koniec okresu „brak karty”*	
	Stan licznika kilometrów pojazdu przy wyjęciu karty lub na koniec okresu „brak karty” i odległość przebyta od włożenia karty lub od początku okresu „brak karty”.	x xxx xxx **km**; x xxx **km**

(*) Numer generacji karty może być drukowany tylko przez tachograf inteligentny.

11	***Dzienne zestawienie***	
	Identyfikator bloku	----------Σ----------
11.1	***Zestawienie VU okresów bez karty w szczelinie czytnika karty kierowcy***	
	Identyfikator bloku	1
11.2	***Zestawienie VU okresów bez karty w szczelinie czytnika karty współkierowcy***	
	Identyfikator bloku	2
11.3	***Dzienne zestawienie VU dla poszczególnych kierowców***	
	Identyfikator rekordu	----------
	Nazwisko kierowcy	Last_Name_____
	Imię (imiona) kierowcy	First_Name_____
	Identyfikacja karty kierowcy	Card_Identification_____
11.4	*Wprowadzanie miejsca rozpoczęcia lub zakończenia dziennego okresu pracy*	
	pi=piktogram miejsca rozpoczęcia / zakończenia, godzina, kraj, region	pihh:mm Cou Reg
	Stan licznika kilometrów	x xxx xxx **km**
11.5	*Wprowadzanie miejsca rozpoczęcia lub zakończenia dziennego okresu pracy*	
	i po 3 godzinach nieprzerwanego czasu prowadzenia pojazdu	hh:mm
	Stan licznika kilometrów	x xxx xxx **km**
11.6	*Podsumowania dla czynności (z karty)*	
	Całkowity czas prowadzenia pojazdu, przebyta odległość	hh**h**mm x xxx **km**
	Całkowity czas pracy i gotowości	hh**h**mm hh**h**mm
	Całkowity czas odpoczynku i nieznanych czynności	hh**h**mm hh**h**mm
	Całkowity czas czynności załogi	hh**h**mm
11.7	*Podsumowania dla czynności (okresy bez karty w szczelinie czytnika karty kierowcy)*	
	Całkowity czas prowadzenia pojazdu, przebyta odległość	hh**h**mm x xxx **km**
	Całkowity czas pracy i gotowości	hh**h**mm hh**h**mm
	Całkowity czas odpoczynku	hh**h**mm

11.8	*Podsumowania dla czynności (okresy bez karty w szczelinie czytnika karty współkierowcy)*	
	Całkowity czas pracy i gotowości	⚒ hh**h**mm ⧈ hh**h**mm
	Całkowity czas odpoczynku	⊢ hh**h**mm
11.9	*Podsumowania dla czynności (dla poszczególnych kierowców, z uwzględnieniem obu szczelin czytnika kart)*	
	Całkowity czas prowadzenia pojazdu, przebyta odległość	⊙ hh**h**mm x xxx **km**
	Całkowity czas pracy i gotowości	⚒ hh**h**mm ⧈ hh**h**mm
	Całkowity czas odpoczynku	⊢ hh**h**mm
	Całkowity czas czynności załogi	⊙⊙ hh**h**mm

Gdy bieżącego dnia potrzebny jest dzienny wydruk, dzienne zestawienie informacji oblicza się na podstawie danych dostępnych w czasie wydruku.

12	***Zdarzenia lub usterki zapisane na karcie***	
12.1	Identyfikator bloku ostatnich 5 „Zdarzeń i usterek" na karcie	----------!×▪----------
12.2	Identyfikator bloku wszystkich „zdarzeń" zarejestrowanych na karcie	----------!▪----------
12.3	Identyfikator bloku wszystkich „usterek" zarejestrowanych na karcie	----------×▪----------
12.4	*Rekord zdarzenia lub usterki*	
	Identyfikator rekordu	----------
	Piktogram zdarzenia/usterki, cel rekordu, data i godzina rozpoczęcia,	Pic (p) dd/mm/yyyy hh:mm
	Dodatkowy kod zdarzenia/usterki (w stosownych przypadkach), czas trwania	!xx hh**h**mm
	Państwo członkowskie rejestracji i numer VRN pojazdu, w którym zaistniało zdarzenie lub usterka	🚗 Nat/VRN_____

13	***Zdarzenia lub usterki zapisane lub trwające na VU***	
13.1	Identyfikator bloku ostatnich 5 „zdarzeń i usterek" z VU	----------!×🚗----------
13.2	Identyfikator bloku wszystkich „zdarzeń" zarejestrowanych lub trwających na VU	----------!🚗----------
13.3	Identyfikator bloku wszystkich „usterek" zarejestrowanych lub trwających na VU	----------×🚗----------
13.4	*Rekord zdarzenia lub usterki*	
	Identyfikator rekordu	----------
	Piktogram zdarzenia/usterki, cel rekordu, data i godzina rozpoczęcia,	Pic (p) dd/mm/yyyy hh:mm
	Dodatkowy kod zdarzenia/usterki (w stosownych przypadkach), liczba podobnych zdarzeń zaistniałych tego dnia, czas trwania	!xx (xxx) hh**h**mm
	Identyfikacja karty włożonej na początku lub końcu zdarzenia lub usterki (maksymalnie 4 wiersze bez powtarzania tych samych numerów kart)	Card_Identification_____ Card_Identification_____ Card_Identification_____ Card_Identification_____
	Przypadek, gdy nie włożono żadnej karty	▪---
	Dane swoiste producenta	< Literal><ErrorCode>

Cel rekordu (p) jest kodem numerycznym wyjaśniającym, dlaczego zapisano zdarzenie lub usterkę, i jest kodowany zgodnie z elementem danych `EventFaultRecordPurpose`.

`Literal` to tekst swoisty dla producenta tachografu o długości maksymalnie 12 znaków.

`ErrorCode` to kod błędu swoisty dla producenta tachografu o długości maksymalnie 12 znaków.

14	***Identyfikacja VU***	
	Identyfikator bloku	----------B----------
	Nazwa producenta VU	B Name_____
	Adres producenta VU	Address_____
	Numer części VU	PartNumber_____
	Numer homologacji VU	Apprv_____
	Numer seryjny VU	S/N_____
	Rok produkcji VU	yyyy
	Wersja oprogramowania i data instalacji VU	V xxxx dd/mm/yyyy
15	***Identyfikacja czujnika***	
	Identyfikator bloku	----------Л----------
15.1	*Rekord sparowania*	
	Numer seryjny czujnika	Л S/N_____
	Numer homologacji czujnika	Apprv_____
	Data sparowania czujnika	dd/mm/yyyy hh:mm
16	***Identyfikacja urządzenia GNSS***	
	Identyfikator bloku	----------▚----------
16.1	*Rekord powiązania*	
	Numer seryjny urządzenia zewnętrznego GNSS	▚ S/N_____
	Numer homologacji urządzenia zewnętrznego GNSS	Apprv_____
	Data powiązania urządzenia zewnętrznego GNSS	dd/mm/yyyy hh:mm
17	***Dane kalibracyjne***	
	Identyfikator bloku	----------T----------
17.1	*Rekord kalibracji*	
	Identyfikator rekordu	----------
	Warsztat, który przeprowadził kalibrację	T Workshop_name_____
	Adres warsztatu	Workshop_address_____
	Identyfikacja karty warsztatowej	Card_Identification_____
	Termin ważności karty warsztatowej	dd/mm/yyyy
	Pusty wiersz	
	Data kalibracji + cel kalibracji	T dd/mm/yyyy (p)
	VIN	A VIN_____
	Państwo członkowskie rejestracji i numer VRN	Nat/VRN_____
	Współczynnik charakterystyczny pojazdu	w xx xxx Imp/km
	Stała urządzenia rejestrującego	k xx xxx Imp/km
	Effective circumference of wheel tyres	l xx xxx mm
	Rozmiar zamontowanych opon	● TyreSize_____
	Ustawienie urządzenia ograniczenia prędkości	> xxx km/h
	Stary i nowy stan licznika kilometrów	x xxx xxx – x xxx xxx km

Cel kalibracji (p) jest kodem numerycznym wyjaśniającym, dlaczego zapisano parametry kalibracji, i jest kodowany zgodnie z elementem danych `CalibrationPurpose`.

18	***Korekta czasu***	
	Identyfikator bloku	`----------◷----------`
18.1	*Rekord korekty czasu*	
	Identyfikator rekordu	`--------------------`
	Stara data i godzina	`!◷ dd/mm/yyyy hh:mm`
	Nowa data i godzina	`◷ dd/mm/yyyy hh:mm`
	Warsztat, który przeprowadził korektę czasu	`T Workshop_name_____`
	Adres warsztatu	`Workshop_address_____`
	Identyfikacja karty warsztatowej	`Card_Identification_____`
	Termin ważności karty warsztatowej	`dd/mm/yyyy`

19	***Ostatnie zdarzenie i usterka zarejestrowane w VU***	
	Identyfikator bloku	`----------!×▲----------`
	Data i godzina ostatniego zdarzenia	`! dd/mm/yyyy hh:mm`
	Data i godzina ostatniej usterki	`× dd/mm/yyyy hh:mm`

20	***Informacje dotyczące kontroli przekroczenia prędkości***	
	Identyfikator bloku	`----------»»----------`
	Data i godzina ostatniej KONTROLI PRZEKROCZENIA PRĘDKOŚCI	`»▫dd/mm/yyyy hh:mm`
	Data/godzina pierwszego przekroczenia prędkości i liczba przekroczeń prędkości od tego czasu	`»»dd/mm/yyyy hh:mm (nnn)`

21	***Rekord przekroczenia prędkości***	
21.1	Identyfikator bloku „Pierwsze przekroczenie prędkości po ostatniej kalibracji”	`--------»»T---------`
21.2	Identyfikator bloku „5 najpoważniejszych zdarzeń w ciągu ostatnich 365 dni”	`-------»»(365)------`
21.3	Identyfikator bloku „najpoważniejsze zdarzenie dla każdego z 10 ostatnich dni od zaistnienia zdarzenia”	`-------»»(10)-------`
21.4	Identyfikator rekordu	`--------------------`
	Data, godzina i czas trwania	`»»dd/mm/yyyy hh:mm hhhmm`
	Prędkości maksymalne i przeciętne, liczba podobnych zdarzeń zaistniałych tego dnia	`xxx km/h xxx km/h(xxx)`
	Nazwisko kierowcy	`◙ Last_Name_____`
	Imię (imiona) kierowcy	`First_Name_____`
	Identyfikacja karty kierowcy	`Card_Identification_____`
21.5	Jeżeli w bloku nie ma rekordu przekroczenia prędkości	`»»---`

22	***Informacje wpisywane ręcznie***	
	Identyfikator bloku	`------------------------`
22.1	Miejsce kontroli	`▫• .....`
22.2	Podpis kontrolera	`▫ .....`
22.3	Od godziny	`◷+ .....`
22.4	Do godziny	`+◷ .....`
22.5	Podpis kierowcy	`◙ .....`

„Informacje wpisywane ręcznie”; Należy wstawić wystarczającą liczbę pustych wierszy ponad elementem wpisywanym ręcznie, tak aby zmieściły się wymagane informacje lub podpis.

23 ***Karty ostatnio włożone do VU***

Identyfikator bloku

23.1 Włożona karta

Identyfikator rekordu

Typ karty, generacja, wersja, producent (*)

Identyfikacja karty

Numer seryjny karty

Data i godzina ostatniego włożenia karty

```
-------- ⊟■◷ --------

----
↑ <gen> <version> <MC>
Card Identification
Card Serial Number
dd/mm/yyyy hh:mm
```

(*) (wszystko w jednym wierszu)

gdzie

typ karty: piktogram, jeden znak + spacja

gen: GEN1 lub GEN2, 4 znaki + spacja

version: do 10 znaków

MC: kod producenta, 3 znaki

3. SPECYFIKACJE WYDRUKU

W tym rozdziale przyjęto następujące konwencje zapisu:

N	Wydruk bloku lub rekordu o numerze N
N	Wydruk bloku lub rekordu o numerze N powtarzany tyle razy, ile jest to niezbędne
X/Y	Wydruk bloków lub rekordów X lub Y w zależności od potrzeby i powtórzenie tyle razy, ile jest to niezbędne

3.1. **Wydruk dzienny czynności kierowcy z karty**

PRT_008 Wydruk dzienny czynności kierowcy z karty jest zgodny z poniższym formatem:

1	Data i godzina drukowania dokumentu
2	Typ wydruku
3	Identyfikacja kontrolera (jeżeli w czytniku VU znajduje się karta kontrolna)
3	Identyfikacja kierowcy (z karty, dla której sporządzany jest wydruk)
4	Identyfikacja pojazdu (tego, dla którego sporządzany jest wydruk)
5	Identyfikacja VU (z którego uzyskano wydruk)
6	Ostatnia kalibracja VU
7	Ostatnia kontrola sprawdzanego kierowcy
8	Ogranicznik czynności kierowcy
8a	Stan poza zakresem na początku danego dnia
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Czynności kierowcy w kolejności chronologicznej
11	Ogranicznik dziennego zestawienia

11.4	Miejsca wprowadzone w kolejności chronologicznej
11.5	Dane GNSS
11.6	Podsumowania dla czynności
12.1	Zdarzenia lub usterki z ogranicznika karty
12.4	Rekordy zdarzeń/ usterek (5 ostatnich zdarzeń lub usterek zapisanych na karcie)
13.1	Zdarzenia lub usterki z ogranicznika VU
13.4	Rekordy zdarzeń/ usterek (5 ostatnich zdarzeń lub usterek zapisanych lub trwających na VU)
22.1	Miejsce kontroli
22.2	Podpis kontrolera
22.5	Podpis kierowcy

3.2. **Wydruk dzienny czynności kierowcy z VU**

PRT_009 Wydruk dzienny czynności kierowcy z VU jest zgodny z poniższym formatem:

1	Data i godzina drukowania dokumentu
2	Typ wydruku
3	Identyfikacja posiadacza karty (dla wszystkich kart włożonych do VU + GEN)
4	Identyfikacja pojazdu (tego, dla którego sporządzany jest wydruk)
5	Identyfikacja VU (z którego uzyskano wydruk)
6	Ostatnia kalibracja VU
7	Ostatnia kontrola tego tachografu
9	Ogranicznik czynności kierowcy
10	Ogranicznik szczeliny czytnika karty kierowcy (szczelina 1)
10a	Stan poza zakresem na początku danego dnia
10.1 / 10.2 / 10.3 /10.3a / 10.4	Czynności w kolejności chronologicznej (szczelina czytnika karty kierowcy)
10	Ogranicznik szczeliny czytnika karty współkierowcy (szczelina 2)
10a	Stan poza zakresem na początku danego dnia
10.1 / 10.2 / 10.3 /10.3a / 10.4	Czynności w kolejności chronologicznej (szczelina czytnika karty współkierowcy)
11	Ogranicznik dziennego zestawienia
11.1	Zestawienie okresów bez karty w szczelinie czytnika karty kierowcy
11.4	Miejsca wprowadzone w kolejności chronologicznej
11.5	Dane GNSS
11.6	Podsumowania dla czynności
11.2	Zestawienie okresów bez karty w szczelinie czytnika karty współkierowcy
11.4	Miejsca wprowadzone w kolejności chronologicznej
11.5	Dane GNSS

11.7	Podsumowania dla czynności
11.3	Zestawienie czynności dla kierowcy z uwzględnieniem obu szczelin czytnika kart
11.4	Miejsca wprowadzone przez danego kierowcę w kolejności chronologicznej
11.5	Dane GNSS
11.8	Podsumowania dla czynności danego kierowcy
13.1	Ogranicznik zdarzeń/ usterek
12.4	Rekordy zdarzeń/ usterek (5 ostatnich zdarzeń lub usterek zapisanych lub trwających na VU)
13.1	Miejsce kontroli
22.2	Podpis kontrolera
22.3	Od godziny (miejsce przeznaczone dla kierowcy bez karty w celu wskazania dotyczących go okresów)
22.4	Do godziny
22.5	Podpis kierowcy

3.3. **Wydruk zdarzeń i usterek z karty**

PRT_010 Wydruk zdarzeń i usterek z karty jest zgodny z poniższym formatem:

1	Data i godzina drukowania dokumentu
2	Typ wydruku
3	Identyfikacja kontrolera (jeżeli w czytniku VU znajduje się karta kontrolna + GEN)
3	Identyfikacja kierowcy (z karty, dla której sporządzany jest wydruk)
4	Identyfikacja pojazdu (tego, dla którego sporządzany jest wydruk)
12.2	Ogranicznik zdarzeń
12.4	Rekordy zdarzeń (wszystkie zdarzenia zarejestrowane na karcie)
12.3	Ogranicznik usterek
12.4	Rekordy usterek (wszystkie usterki zarejestrowane na karcie)
22.1	Miejsce kontroli
22.2	Podpis kontrolera
22.5	Podpis kierowcy

3.4. **Wydruk zdarzeń i usterek z VU**

PRT_011 Wydruk zdarzeń i usterek z VU jest zgodny z poniższym formatem:

1	Data i godzina drukowania dokumentu
2	Typ wydruku
3	Identyfikacja posiadacza karty (dla wszystkich kart włożonych do VU + GEN)
4	Identyfikacja pojazdu (tego, dla którego sporządzany jest wydruk)

13.2	Ogranicznik zdarzeń
13.4	Rekordy zdarzeń (wszystkie zdarzenia zarejestrowane lub trwające w VU)
13.3	Ogranicznik usterek
13.4	Rekordy usterek (wszystkie usterki zarejestrowane lub trwające w VU)
22.1	Miejsce kontroli
22.2	Podpis kontrolera
22.5	Podpis kierowcy

3.5. **Wydruk danych technicznych**

PRT_012 Wydruk danych technicznych jest zgodny z poniższym formatem:

1	Data i godzina drukowania dokumentu
2	Typ wydruku
3	Identyfikacja posiadacza karty (dla wszystkich kart włożonych do VU + GEN)
4	Identyfikacja pojazdu (tego, dla którego sporządzany jest wydruk)
14	Identyfikacja VU
15	Identyfikacja czujnika
15.1	Dane sparowania czujnika (wszystkie dane dostępne w kolejności chronologicznej)
16	Identyfikacja urządzenia GNSS
16.1	Dane powiązania urządzenia zewnętrznego GNSS (wszystkie dane dostępne w kolejności chronologicznej)
17	Ogranicznik danych kalibracyjnych
17.1	Rekordy kalibracji (wszystkie dostępne rekordy w kolejności chronologicznej)
18	Ogranicznik korekty czasu
18.1	Rekordy korekty czasu (wszystkie dostępne rekordy z rekordów korekty czasu i kalibracji)
19	Ostatnie zdarzenie i usterka zarejestrowane w VU

3.6. **Wydruk przekroczenia prędkości**

PRT_013 Wydruk przekroczenia prędkości jest zgodny z poniższym formatem:

1	Data i godzina drukowania dokumentu
2	Typ wydruku
3	Identyfikacja posiadacza karty (dla wszystkich kart włożonych do VU + GEN)
4	Identyfikacja pojazdu (tego, dla którego sporządzany jest wydruk)
20	Informacje dotyczące kontroli przekroczenia prędkości
21.1	Identyfikator danych dotyczących przekroczenia prędkości
21.4 / 21.5	Pierwsze przekroczenie prędkości po ostatniej kalibracji

21.2	Identyfikator danych dotyczących przekroczenia prędkości
21.4 / 21.5	5 najpoważniejszych przekroczeń prędkości w ciągu ostatnich 365 dni
21.3	Identyfikator danych dotyczących przekroczenia prędkości
21.4 / 21.5	Najpoważniejsze przekroczenie prędkości dla każdego z ostatnich 10 dni ich występowania
22.1	Miejsce kontroli
22.2	Podpis kontrolera
22.5	Podpis kierowcy

3.7. **Historia włożonych kart**

PRT_014 Wydruk historii włożonych kart jest zgodny z poniższym formatem:

1	Data i godzina drukowania dokumentu
2	Typ wydruku
3	Identyfikacja posiadacza karty (dla wszystkich kart włożonych do przyrządu rejestrującego)
23	Karta ostatnio włożona do VU
23.1	Włożone karty (maks. 88 rekordów)
12.3	Ogranicznik usterek

Dodatek 5

WYŚWIETLACZ

W niniejszym dodatku przyjęto następujące konwencje zapisu formatu:

— znaki **wytłuszczonym** drukiem oznaczają odkryty tekst widoczny na wyświetlaczu (są wyświetlane jako normalne znaki),

— znaki normalne oznaczają zmienne (piktogramy lub dane), które na wyświetlaczu zastępowane są przez odpowiadające im wartości:

  — dd mm yyyy: dzień, miesiąc, rok,

  — hh: godziny,

  — mm: minuty,

  — D: piktogram czasu trwania,

  — EF: kombinacja piktogramów zdarzeń lub usterek,

  — O: piktogram trybu pracy.

DIS_001 Tachograf wyświetla dane zgodnie z poniższymi formatami:

Dane	Format
Domyślne informacje na wyświetlaczu	
Czas miejscowy	hh:mm
Tryb pracy	O
Informacje dotyczące kierowcy	**1** Dhh**h**mm **II**hh**h**mm
Informacje dotyczące współkierowcy	**2**Dhh**h**mm
Otwarty warunek poza zakresem	**OUT**
Wyświetlanie ostrzeżeń	
Nadmierny nieprzerwany czas prowadzenia pojazdu	**1** hh**h**mm **II**hh**h**mm
Zdarzenie lub usterka	EF
Inne wyświetlane informacje	
Data UTC godzina	**UTC** dd/mm/yyyy lub **UTC** dd.mm.yyyy hh:mm
Nieprzerwany czas prowadzenia pojazdu przez kierowcę i skumulowany czas przerwy	**1** hh**h**mm **II**hh**h**mm
Nieprzerwany czas prowadzenia pojazdu przez współkierowcę i skumulowany czas przerwy	**2** hh**h**mm **II**hh**h**mm
Skumulowany czas prowadzenia pojazdu przez kierowcę za ubiegły i obecny tydzień	**1** **II** hhh**h**mm
Skumulowany czas prowadzenia pojazdu przez współkierowcę za ubiegły i obecny tydzień	**2** **II** hhh**h**mm

Dodatek 6

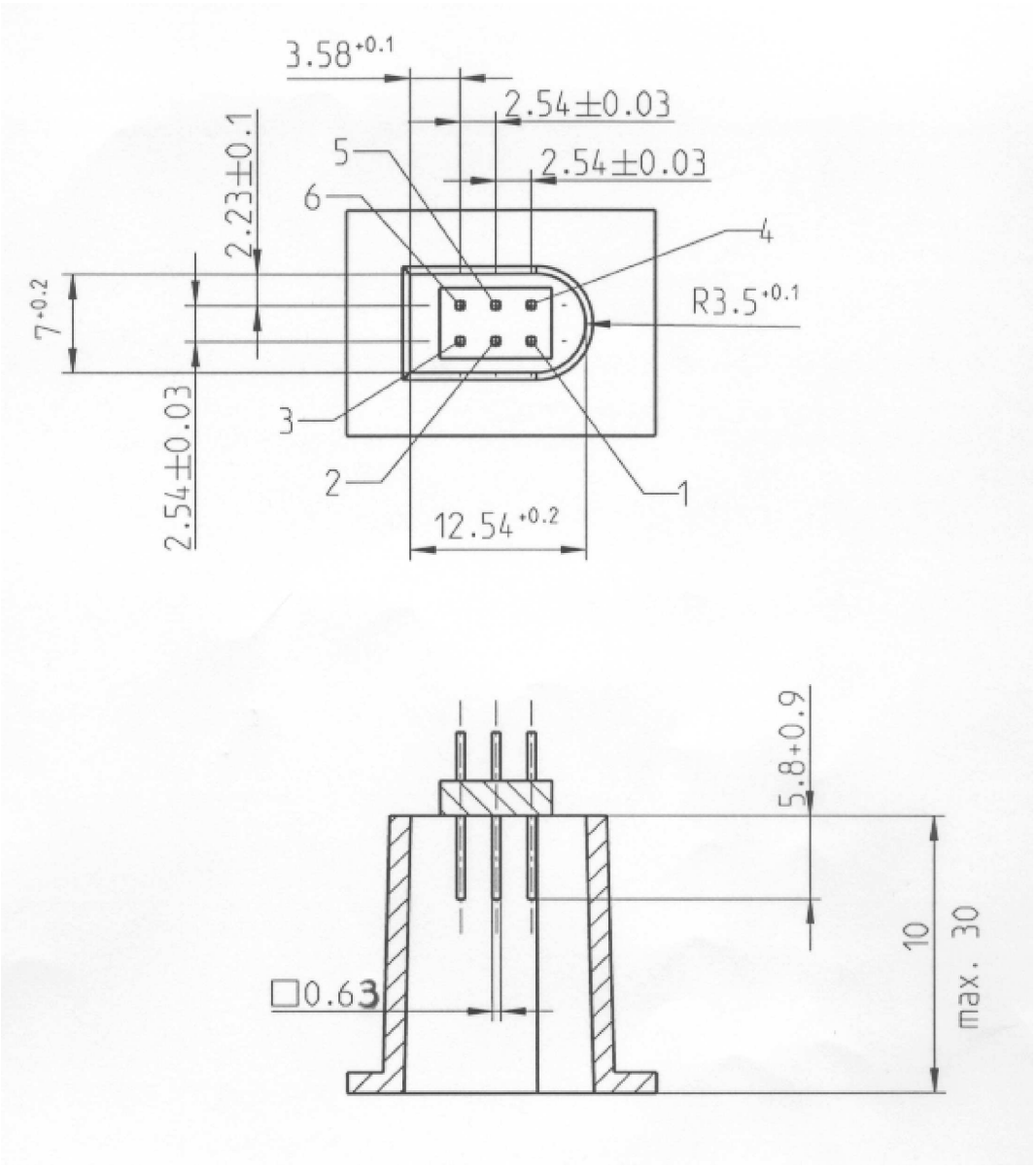
PRZEDNIE ZŁĄCZE KALIBRACJI I POBIERANIA DANYCH

SPIS TREŚCI

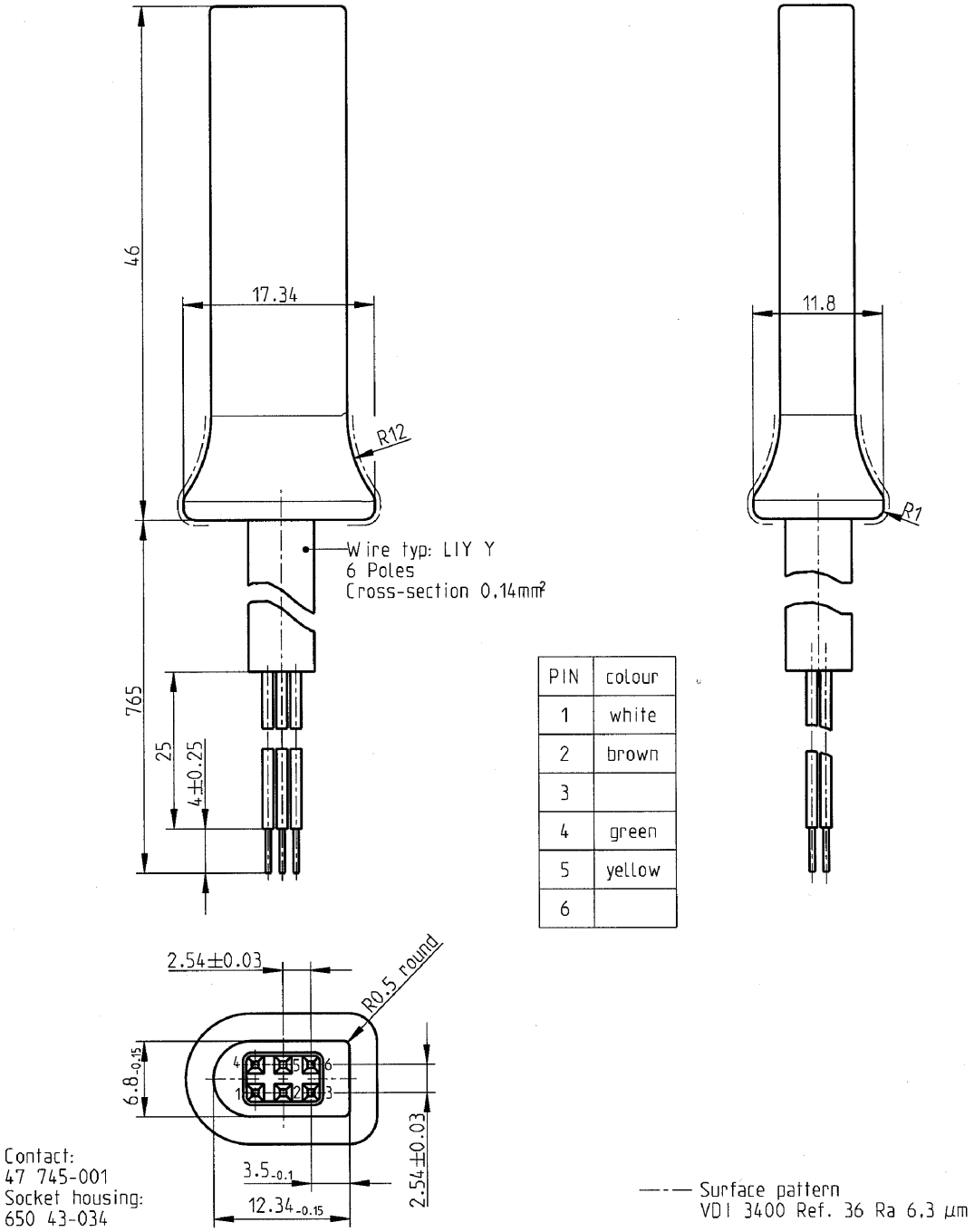
1. SPRZĘT

1.1. **Złącze**

INT_001 Złącze pobierania danych/kalibracji jest złączem sześciopinowym, dostępnym od strony panelu czołowego bez potrzeby odłączania jakiejkolwiek części tachografu. Złącze musi mieć wymiary zgodne z pokazanymi na rysunku poniżej (wszystkie wymiary w milimetrach):



Na rysunku poniżej pokazano typową sześciopinową wtyczkę złączną:



1.2. **Rozmieszczenie styków**

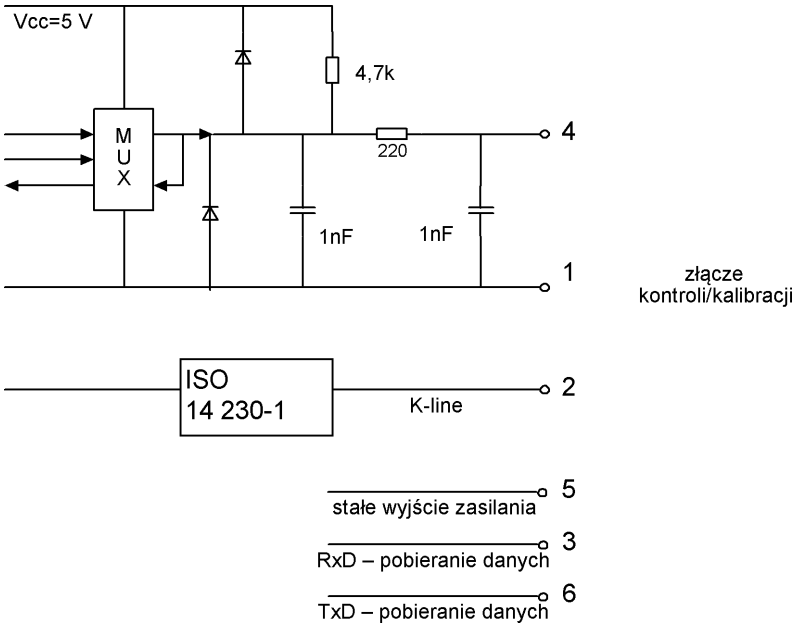
INT_002 Rozmieszczenie styków opisuje poniższa tabela:

Pin	Wyszczególnienie	Uwagi
1	minus akumulatora	przyłączony do minusa akumulatora pojazdu
2	przesyłanie danych	K-line (ISO 14230-1)

Pin	Wyszczególnienie	Uwagi
3	RxD – pobieranie danych	dane wprowadzane do tachografu
4	sygnał we/wy	kalibracja
5	stałe wyjście zasilania	Zakres napięcia musi być taki jak dla zasilania pojazdu minus 3V w celu umożliwienia spadku napięcia na obwodzie ochronnym. Wyjście 40 mA
6	TxD – pobieranie danych	dane pobierane z tachografu

1.3. **Schemat blokowy**

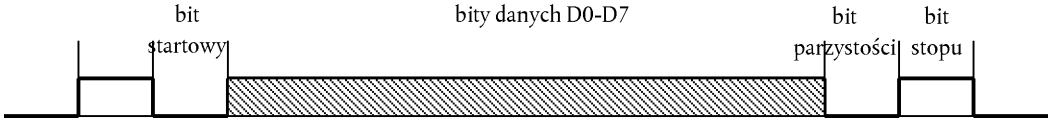
INT_003 Schemat blokowy jest następujący:



2. INTERFEJS POBIERANIA DANYCH

INT_004 Interfejs pobierania danych musi być zgodny z wymaganiami RS232.

INT_005 Interfejs pobierania danych jest skonfigurowany w następujący sposób: jeden bit startowy, 8 bitów danych najmniej znaczących na początku, jeden bit parzystości i jeden bit stopu.



Organizacja bajtu danych

bit startowy: jeden bit na poziomie logicznym 0

bity danych: przesyłane z najmniej znaczącym na początku

bit parzystości: kontrola parzystości;

bit stopu: jeden bit na poziomie logicznym 1

W przypadku przesyłania danych liczbowych złożonych z więcej niż jednego bajtu bajt najbardziej znaczący jest przesyłany pierwszy, a bajt najmniej znaczący – ostatni.

INT_006 Szybkość transmisji danych w bodach regulowana jest w zakresie od 9 600 b/s do 115 200 b/s. Transmisja odbywa się z najwyższą możliwą szybkością, przy czym szybkość początkowa przy inicjowaniu sesji ustawiona jest na 9 600 b/s.

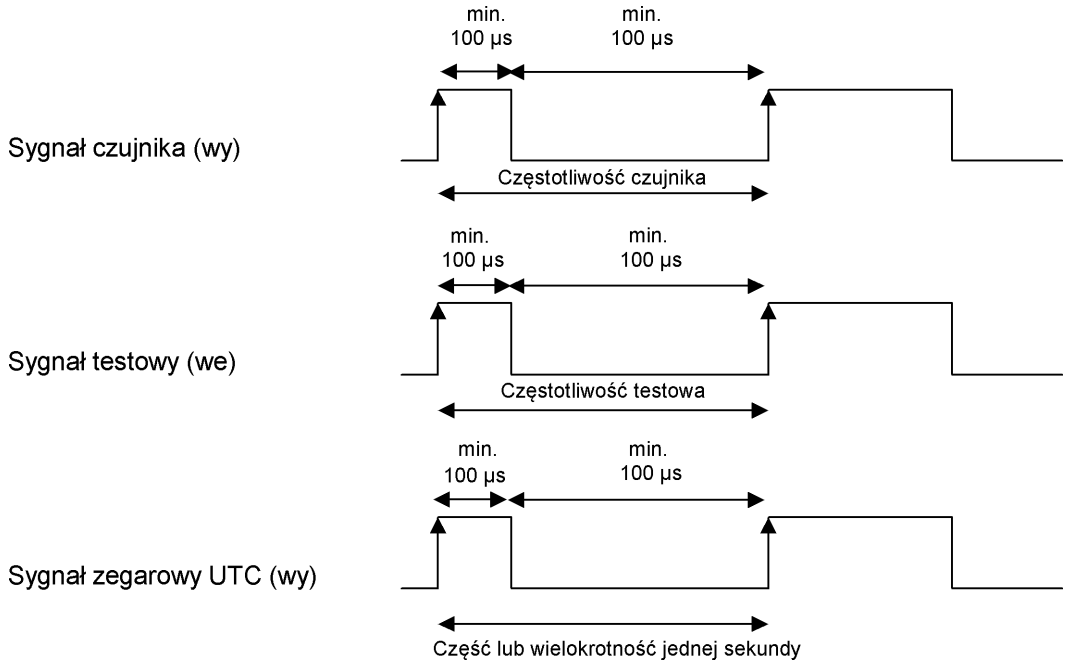
3. Interfejs kalibracyjny

INT_007 Przesyłanie danych musi być zgodne z normą ISO 14230-1 Pojazdy drogowe – Systemy diagnostyczne – Protokół słów kluczowych 2000 – część 1: Warstwa fizyczna (wydanie pierwsze: 1999 r.).

INT_008 Sygnał we/wy musi być zgodny z następującymi wymaganiami elektrycznymi:

Parametr	Min.	Typowy	Maks.	Uwagi
U_{low} (we)			1,0 V	I = 750 µA
U_{high} (we)	4 V			I = 200 µA
Częstotliwość			4 kHz	
U_{low} (wy)			1,0 V	I = 1 mA
U_{high} (wy)	4 V			I = 1 mA

INT_009 Sygnał we/wy musi być zgodny z następującymi przebiegami czasowymi:



Dodatek 7

PROTOKOŁY POBIERANIA DANYCH

SPIS TREŚCI

1. WPROWADZENIE

Niniejszy dodatek zawiera procedury stosowane przy pobieraniu danych różnych typów na zewnętrzny nośnik danych (ESM), wraz z protokołami, które muszą być wdrożone w celu zagwarantowania prawidłowego przesyłania danych i pełnej zgodności formatu pobranych danych, tak by umożliwić każdemu kontrolerowi sprawdzenie tych danych oraz sprawdzenie autentyczności i integralności przed przystąpieniem do analizy danych.

1.1. **Zakres**

Dane mogą być pobierane na ESM:

— z przyrządu rejestrującego za pośrednictwem inteligentnego, wydzielonego urządzenia (IDE) przyłączonego do VU;

— z karty do tachografu za pośrednictwem IDE spasowanego z czytnikiem karty (IFD);

— z karty do tachografu za pośrednictwem przyrządu rejestrującego poprzez IDE przyłączone do VU.

Aby umożliwić weryfikację autentyczności i integralności pobranych danych przechowywanych na ESM, dane są pobierane razem z dołączonym podpisem, zgodnie z dodatkiem 11 Wspólne mechanizmy zabezpieczenia. Razem z danymi pobierane są również identyfikacja urządzenia źródłowego (VU lub karta) i jego świadectwa bezpieczeństwa (państwo członkowskie i urządzenie). Niezależnie od tego weryfikator danych musi mieć zaufany europejski klucz publiczny.

DDP_001 Dane pobrane podczas jednej sesji pobierania muszą być przechowywane na ESM w jednym pliku.

1.2. **Akronimy i skróty**

W niniejszym dodatku używa się następujących skrótów:

AID [Application Identifier] identyfikator aplikacji

ATR [Answer To Reset] reakcja na sprowadzenie do stanu wyjściowego

CS [Checksum byte] bajt sumy kontrolnej

DF [Dedicated File] plik dedykowany

DS_ [Diagnostic Session] sesja diagnostyczna

EF [Elementary File] plik elementarny

ESM [External Storage Medium] zewnętrzny nośnik danych

FID [File Identifier] identyfikator pliku (ID pliku)

FMT [Format Byte] bajt formatu (pierwszy bajt nagłówka komunikatu)

ICC [Integrated Circuit Card] karta z układem scalonym

IDE [Intelligent Dedicated Equipment] inteligentne urządzenie dedykowane: urządzenie służące do pobierania danych na ESM (np. komputer osobisty)

IFD [Interface Device] urządzenie interfejsu

KWP [Keyword Protocol 2000] protokół słowa kluczowego 2000

LEN [Length Byte] bajt długości (ostatni bajt nagłówka komunikatu)

PPS [Protocol Parameter Selection] wybór parametru protokołu

PSO [Perform Security Operation] wykonanie operacji zabezpieczającej

SID [Service Identifier] identyfikator usługi

SRC [Source byte] bajt źródłowy

TGT [Target Byte] bajt docelowy

TLV [Tag Length Value] wartość długości znacznika

TREP [Transfer Response Parameter] parametr odpowiedzi na przesłanie danych

TRTP [Transfer Request Parameter] parametr żądania przesłania danych

VU [Vehicle Unit] przyrząd rejestrujący

2. POBIERANIE DANYCH Z VU

2.1. **Procedura pobierania danych**

W celu pobrania danych z VU operator musi wykonać następujące czynności:

— włożyć swoją kartę do tachografu do czytnika karty w VU (*);

— podłączyć IDE do gniazda pobierania w VU;

— nawiązać połączenie między IDE i VU;

— wybrać w IDE dane do pobrania i wysłać żądanie do VU;

— zamknąć sesję pobierania danych.

2.2. **Protokół pobierania danych**

Protokół skonstruowany jest zgodnie z zasadą nadrzędny-podległy, gdzie IDE jest urządzeniem nadrzędnym a VU podległym.

Struktura komunikatu, typy komunikatów i przepływ są zasadniczo oparte na Protokole słowa kluczowego 2000 (KWP) (według normy ISO 14230-2 Pojazdy drogowe – Systemy diagnostyczne – Protokół słowa kluczowego 2000 – część 2: Warstwa łącza danych).

Warstwa aplikacji zbudowana jest zasadniczo w oparciu o bieżący projekt normy ISO 14229-1 (Pojazdy drogowe – Systemy diagnostyczne – część 1: Usługi diagnostyczne, wersja 6 z dnia 22 lutego 2001 r.)

2.2.1 *Struktura komunikatu*

DDP_002 Wszystkie komunikaty wymieniane między IDE i VU mają strukturę złożoną z następujących trzech części:

— nagłówek zawierający bajt formatu (FMT), bajt docelowy (TGT), bajt źródłowy (SRC) i ewentualnie bajt długości (LEN);

— pole danych zawierające bajt identyfikator usługi (SID) i zmienną liczbę bajtów z danymi, w których może być bajt opcjonalnej sesji diagnostycznej (DS_) lub bajt opcjonalnego parametru przesyłania (TRTP lub TREP);

— suma kontrolna zawierająca bajt sumy kontrolnej (CS).

Nagłówek				Pole danych					Suma kontrolna
FMT	TGT	SRC	LEN	SID	DATA	…	…	…	CS
4 bajty				Maks. 255 bajtów					1 bajt

(*) Włożenie karty spowoduje aktywację właściwych praw dostępu do funkcji pobierania i do danych. Możliwe jest jednak pobieranie danych z karty kierowcy włożonej do jednej ze szczelin VU, jeżeli w drugiej szczelinie nie ma żadnej innej karty.

Bajty TGT i SRC reprezentują fizyczny adres adresata i źródła komunikatu. Przyjmują one wartości F0 Hex dla IDE i EE Hex dla VU.

Bajt LEN jest długością pola danych.

Bajt sumy kontrolnej jest ośmiobitową sumą serii modulo 256 wszystkich bajtów komunikatu, z wyłączeniem bajtu CS.

Bajty FMT, SID, DS_, TRTP i TREP są zdefiniowane w dalszej części niniejszego dokumentu.

DDP_003 W przypadku gdy dane przesyłane komunikatem są dłuższe niż dysponowane pole danych, komunikat wysyła się w kilku podkomunikatach. Każdy podkomunikat ma nagłówek, te same bajty SID i TREP oraz dwubajtowy licznik podkomunikatu pokazujący liczbę podkomunikatów w całym komunikacie. Aby umożliwić kontrolę błędów i przerwanie przesyłania, IDE potwierdza każdy podkomunikat. IDE może przyjmować podkomunikat, żądać powtórzenia transmisji, żądać od VU powtórzenia transmisji od początku lub przerwania transmisji.

DDP_004 Jeżeli ostatni podkomunikat ma dokładnie 255 bajtów w polu danych, musi być dołączony końcowy podkomunikat z pustym polem danych (z wyjątkiem SID TREP i licznika podkomunikatów) w celu pokazania końca komunikatu.

Przykład:

Nagłówek	SID	TREP	Komunikat	CS
4 bajty	dłuższy niż 255 bajtów			

zostanie przesłany w następujący sposób:

Nagłówek	SID	TREP	00	01	Podkomunikat 1	CS
4 bajty	255 bajtów					

Nagłówek	SID	TREP	00	02	Podkomunikat 2	CS
4 bajty	255 bajtów					

…

Nagłówek	SID	TREP	xx	yy	Podkomunikat n	CS
4 bajty	mniej niż 255 bajtów					

lub w taki sposób:

Nagłówek	SID	TREP	00	01	Podkomunikat 1	CS
4 bajty	255 bajtów					

Nagłówek	SID	TREP	00	02	Podkomunikat 2	CS
4 bajty	255 bajtów					

…

Nagłówek	SID	TREP	xx	yy	Podkomunikat n	CS
4 bajty	255 bajtów					

Nagłówek	SID	TREP	xx	yy + 1	CS
4 bajty	4 bajty				

2.2.2 *Typy komunikatów*

Protokół komunikacyjny pobierania danych między VU i IDE wymaga wymiany komunikatów 8 różnych typów.

W tabeli poniżej opisano te komunikaty.

Struktura komunikatu	Maks. 4 bajty Nagłówek				Maks. 255 bajtów Dane			1 bajt Suma kontrolna
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Start Communication Request	81	EE	F0		81			E0
Positive Response Start Communication	80	F0	EE	03	C1		EA, 8F	9B
Start Diagnostic Session Request	80	EE	F0	02	10	81		F1
Positive Response Start Diagnostic	80	F0	EE	02	50	81		31
Link Control Service Verify Baud Rate (stage 1)								
9 600 Bd	80	EE	F0	04	87		01,01, 01	EC
19 200 Bd	80	EE	F0	04	87		01,01, 02	ED
38 400 Bd	80	EE	F0	04	87		01,01, 03	EE
57 600 Bd	80	EE	F0	04	87		01,01, 04	EF
115 200 Bd	80	EE	F0	04	87		01,01, 05	F0
Positive Response Verify Baud Rate	80	F0	EE	02	C7		01	28
Transition Baud Rate (stage 2)	80	EE	F0	03	87		02,03	ED
Request Upload	80	EE	F0	0A	35		00,00, 00,00, 00,FF,FF, FF,FF	99
Positive Response Request Upload	80	F0	EE	03	75		00,FF	D5

Struktura komunikatu	Maks. 4 bajty Nagłówek				Maks. 255 bajtów Dane			1 bajt Suma kontrolna
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Transfer Data Request								
Overview	80	EE	F0	02	36	01		97
Activities	80	EE	F0	06	36	02	Date	CS
Events & Faults	80	EE	F0	02	36	03		99
Detailed Speed	80	EE	F0	02	36	04		9A
Technical Data	80	EE	F0	02	36	05		9B
Card download	80	EE	F0	02	36	06	Slot	CS
Positive Response Transfer Data	80	F0	EE	Len	76	TREP	Data	CS
Request Transfer Exit	80	EE	F0	01	37			96
Positive Response Request Transfer Exit	80	F0	EE	01	77			D6
Stop Communication Request	80	EE	F0	01	82			E1
Positive Response Stop Communication	80	F0	EE	01	C2			21
Acknowledge sub message	80	EE	F0	Len	83		Data	CS
Negative responses								
General reject	80	F0	EE	03	7F	Sid Req	10	CS
Service not supported	80	F0	EE	03	7F	Sid Req	11	CS
Sub function not supported	80	F0	EE	03	7F	Sid Req	12	CS
Incorrect Message Length	80	F0	EE	03	7F	Sid Req	13	CS
Conditions not correct or Request sequence error	80	F0	EE	03	7F	Sid Req	22	CS
Request out of range	80	F0	EE	03	7F	Sid Req	31	CS
Upload not accepted	80	F0	EE	03	7F	Sid Req	50	CS
Response pending	80	F0	EE	03	7F	Sid Req	78	CS
Data not available	80	F0	EE	03	7F	Sid Req	FA	CS

Uwagi:

— Sid Req = Sid odpowiadającego żądania.

— TREP = TRTP odpowiadającego żądania.

— Ciemne rubryki oznaczają, że nic nie jest przesyłane.

— Pojęcia „ładowanie” (z perspektywy IDE) używa się zgodnie z normą ISO 14229. Oznacza to samo co pobieranie (z perspektywy VU).

— W tabeli nie pokazano potencjalnych dwubajtowych liczników podkomunikatów.

— „Szczelina” dotyczy numeru szczeliny: „1” (karta w szczelinie czytnika karty kierowcy) albo „2” (karta w szczelinie czytnika karty współkierowcy)

— W przypadku gdy szczelina nie jest określona, VU wybiera szczelinę 1, jeżeli karta jest włożona w tę szczelinę, a szczelinę 2 wybiera tylko wówczas, gdy użytkownik specjalnie ją wybierze.

2.2.2.1 Start Communication Request (SID 81)

DDP_005 Komunikat ten wysyła IDE w celu zestawienia łącza komunikacyjnego z VU. Początkowe komunikaty są zawsze wysyłane z szybkością 9 600 bodów (aż do ewentualnej zmiany szybkości transmisji przy wykorzystaniu odpowiedniej obsługi sterowania łączem).

2.2.2.2 Positive Response Start Communication (SID C1)

DDP_006 Komunikat ten wysyła VU w celu przesłania pozytywnej odpowiedzi na żądanie rozpoczęcia transmisji. Komunikat zawiera 2 kluczowe bajty („EA" „8F") wskazujące, że urządzenie obsługuje protokół z nagłówkiem zawierającym informacje o adresie, źródle i długości.

2.2.2.3 Start Diagnostic Session Request (SID 10)

DDP_007 IDE wysyła komunikat „Start Diagnostic Session Request" w celu zażądania nowej sesji diagnostycznej z VU. Podfunkcja „default session" (81 Hex) wskazuje, że IDE żąda otwarcia standardowej sesji diagnostycznej.

2.2.2.4 Positive Response Start Diagnostic (SID 50)

DDP_008 VU wysyła komunikat „Positive Response Start Diagnostic" w celu przesłania pozytywnej odpowiedzi na żądanie „Diagnostic Session Request".

2.2.2.5 Link Control Service (SID 87)

DDP_052 IDE używa obsługi sterowania łączem do zainicjowania zmiany szybkości transmisji w bodach. Odbywa się to dwustopniowo. Najpierw IDE proponuje zmianę szybkości transmisji podając nową szybkość (pierwszy krok). Po otrzymaniu pozytywnej odpowiedzi od VU IDE wysyła do VU potwierdzenie zmiany szybkości (drugi krok). Następnie IDE przechodzi na nową szybkość transmisji. Po otrzymaniu potwierdzenia VU przechodzi na nową szybkość transmisji.

2.2.2.6 Link Control Positive Response (SID C7)

DDP_053 VU wysyła odpowiedź „Link Control Positive Response" w celu przesłania pozytywnej odpowiedzi na żądanie „Link Control Service" (pierwszy krok). Należy zwrócić uwagę, że na żądanie potwierdzenia (drugi krok) nie ma odpowiedzi.

2.2.2.7 Request Upload (SID 35)

DDP_009 IDE wysyła komunikat „Request Upload" w celu przekazania VU, że żądana jest operacja pobierania. Aby spełnić wymagania normy ISO14229 przesyłane są szczegółowe informacje dotyczące adresu, wielkości i szczegółów żądanych danych. Ponieważ informacje te nie są znane IDE przed pobieraniem, adres pamięci ustawiony jest na 0, format jest nieszyfrowany i bez kompresji, a wielkość pamięci ustawiona na maksimum.

2.2.2.8 Positive Response Request Upload (SID 75)

DDP_010 VU wysyła komunikat „Positive Response Request Upload", aby wskazać IDE, że VU jest gotowe do pobierania danych. Aby spełnić wymagania normy ISO 14229 ten komunikat pozytywnej odpowiedzi zawiera dane wskazujące IDE, że dalsze komunikaty „Positive Response Transfer Data" będą zawierały maksymalnie 00FF hex bajtów.

2.2.2.9 Transfer Data Request (SID 36)

DDP_011 IDE wysyła żądanie „Transfer Data Request" w celu wskazania VU typu danych, które mają być pobierane. Jednobajtowy parametr „Transfer Request Parameter" (TRTP) wskazuje typ przesyłania.

Rozróżnia się sześć typów przesyłania danych:

— Informacje ogólne (TRTP 01);

— Czynności o określonej dacie (TRTP 02);

— Zdarzenia i usterki (TRTP 03);

— Szczegółowe dane dotyczące prędkości (TRTP 04);

— Dane techniczne (TRTP 05);

— Pobieranie danych z karty (TRTP 06).

DDP_054 IDE musi obowiązkowo zażądać przesłania danych Informacje ogólne (TRTP 01) w czasie sesji pobierania, ponieważ tylko to zagwarantuje, że certyfikaty VU są zarejestrowane w pobieranym pliku (i umożliwi weryfikację podpisu cyfrowego).

W drugim przypadku (TRTP 02) w komunikacie „Transfer Data Request" znajduje się informacja o dniu kalendarzowym (format `TimeReal`), dla którego dane mają być pobrane.

2.2.2.10 Positive Response Transfer Data (SID 76)

DDP_012 VU wysyła pozytywną odpowiedź „Positive Response Transfer Data" w odpowiedzi na żądanie „Transfer Data Request". Komunikat zawiera żądane dane z parametrem „Transfer Response Parameter" (TREP) odpowiadającym TRTP żądania.

DDP055 W pierwszym przypadku (TREP 01) VU wyśle dane pomagające operatorowi IDE w wyborze danych, które chce dalej pobrać. Komunikat ten zawiera następujące informacje:

— świadectwa bezpieczeństwa;

— identyfikacja pojazdu;

— bieżąca data i godzina VU;

— minimalna i maksymalna data, dla której można dokonać pobrania (dane z VU);

— sygnalizacja obecności kart w VU;

— poprzednie pobranie dla firmy;

— blokady firmowe;

— poprzednie kontrole.

2.2.2.11 Request Transfer Exit (SID 37)

DDP_013 IDE wysyła komunikat „Request Transfer Exit" w celu zawiadomienia VU, że sesja pobierania jest zakończona.

2.2.2.12 Positive Response Request Transfer Exit (SID 77)

DDP_014 VU wysyła komunikat „Positive Response Request Transfer Exit" w celu potwierdzenia otrzymania żądania wyjścia z przesyłania danych „Request Transfer Exit".

2.2.2.13 Stop Communication Request (SID 82)

DDP_015 IDE wysyła komunikat „Stop Communication Request" w celu rozłączenia łącza komunikacyjnego z VU.

2.2.2.14 Positive Response Stop Communication (SID C2)

DDP_016 VU wysyła komunikat „Positive Response Stop Communication" w celu potwierdzenia otrzymania żądania „Stop Communication Request".

2.2.2.15 Acknowledge Sub Message (SID 83)

DDP_017 IDE wysyła potwierdzenie podkomunikatu w celu potwierdzenia otrzymania każdej części komunikatu przesyłanego w kilku podkomunikatach. W polu danych znajduje się SID otrzymany z VU i dwubajtowy kod opisany poniżej:

— MsgC +1 potwierdza prawidłowy odbiór podkomunikatu o numerze MsgC.

Żądanie od IDE dla VU wysłania następnego podkomunikatu.

— MsgC wskazuje na problem z odbiorem podkomunikatu o numerze MsgC.

Żądanie od IDE dla VU wysłania powtórnie następnego podkomunikatu.

— FFFF żąda zakończenia komunikatu.

IDE może użyć tego do zakończenia transmisji komunikatu z VU z dowolnej przyczyny.

Ostatni podkomunikat komunikatu (bajt LEN < 255) może być potwierdzony przy pomocy dowolnego z tych kodów lub być niepotwierdzony.

Odpowiedziami VU, które składają się z kilku podkomunikatów są:

— Positive Response Transfer Data (SID 76)

2.2.2.16 Negative Response (SID 7F)

DDP_018 VU wysyła komunikat „Negative Response" w odpowiedzi na powyższe komunikaty żądań, gdy VU nie może obsłużyć żądania. Pole danych komunikatu zawiera SID odpowiedzi (7F), SID żądania i kod podający przyczynę negatywnej odpowiedzi. Dozwolone są następujące kody:

— 10 generalne odrzucenie

Czynności nie można wykonać z przyczyny innej niż określone poniżej.

— 11 usługa nieobsługiwana

SID żądania nie jest zrozumiany.

— 12 podfunkcja nieobsługiwana

DS_ lub TRTP żądania nie jest zrozumiany lub nie ma dalszych komunikatów do wysłania.

— 13 nieprawidłowa długość komunikatu

Długość odebranego komunikatu jest nieprawidłowa.

— 22 nieprawidłowe warunki lub błąd kolejności żądań

Żądana usługa nie jest aktywna lub sekwencja komunikatów żądań nie jest prawidłowa.

— 31 żądanie poza zakresem

Żądany rekord dotyczący parametru (pole danych) nie jest ważny.

— 50 ładowanie nieprzyjęte

Żądania nie można obsłużyć (VU w nieodpowiednim trybie pracy lub usterka wewnętrzna VU).

— 78 odpowiedź zawieszona

Czynności nie można zakończyć na czas i VU nie jest gotowe do przyjęcia innego żądania.

— FA brak dostępnych danych

Obiekt danych żądania przesłania danych nie jest dostępny w VU (np. karta nie jest włożona, …).

2.2.3 *Przepływ komunikatów*

Typowy przepływ komunikatów podczas normalnej procedury pobierania danych wygląda następująco:

IDE		VU
Start Communication Request	⇨ ⇦	Positive Response
Start Diagnostic Service Request	⇨ ⇦	Positive Response
Request Upload	⇨ ⇦	Positive Response

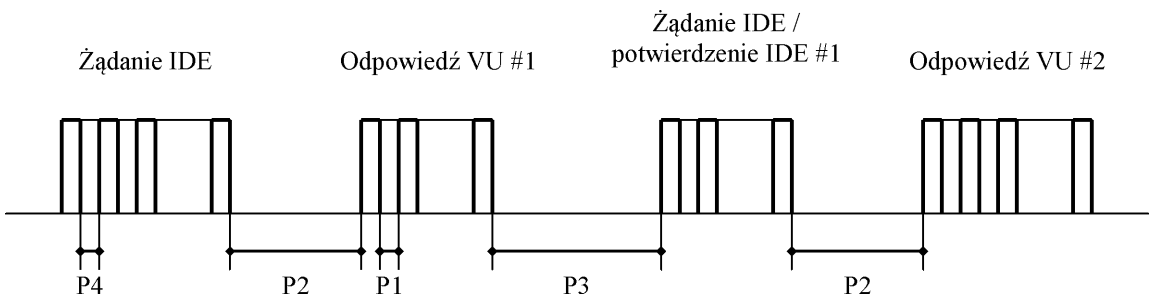
IDE		VU
Transfer Data Request Overview	⇨	
	⇦	Positive Response
Transfer Data Request #2	⇨	
	⇦	Positive Response #1
Acknowledge Sub Message #1	⇨	
	⇦	Positive Response #2
Acknowledge Sub Message #2	⇨	
	⇦	Positive Response #m
Acknowledge Sub Message #m	⇨	
	⇦	Positive Response (Data Field<255 Bytes)
Acknowledge Sub Message (optional)	⇨	
…		
Transfer Data Request #n	⇨	
	⇦	Positive Response
Request Transfer Exit	⇨	
	⇦	Positive Response
Stop Communication Request	⇨	
	⇦	Positive Response

2.2.4 *Przebiegi czasowe*

DDP_019 Podczas normalnej pracy przebiegi czasowe wyglądają tak jak na poniższym rysunku:

Rysunek 1

Przepływ komunikatów, przebiegi czasowe



Gdzie:

P1 = czas między bajtami dla odpowiedzi VU.

P2 = czas między końcem żądania IDE a początkiem odpowiedzi VU, lub między końcem potwierdzenia IDE a początkiem następnej odpowiedzi VU.

P3 = czas między końcem odpowiedzi VU a początkiem nowego żądania IDE, bądź między końcem odpowiedzi VU a początkiem potwierdzenia IDE, bądź między końcem żądania IDE a początkiem nowego żądania IDE, jeżeli VU nie odpowiada.

P4 = czas między bajtami dla żądania IDE.

P5 = przedłużona wartość P3 dla pobierania danych z karty.

Dozwolone wartości przebiegów czasowych pokazano w tabeli poniżej (KWP rozszerzony zestaw parametrów przebiegów czasowych używany w przypadku adresowania fizycznego w celu uzyskania szybszej komunikacji).

Parametr czasowy	Dolna wartość graniczna (ms)	Górna wartość graniczna (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 minut

(*) Jeżeli VU daje negatywną odpowiedź „Negative Response" zawierającą kod o znaczeniu „żądanie odebrane prawidłowo, odpowiedź zawieszona", wartość ta zostaje przedłużona do górnej wartości granicznej P3.

2.2.5 *Obsługa błędów*

W przypadku wystąpienia błędu w czasie wymiany komunikatów, schemat przepływu komunikatów zostaje zmodyfikowany zależnie od tego, które urządzenia wykryło błąd, i od komunikatu generującego błąd.

Na rysunkach 2 i 3 pokazano odpowiednio procedury obsługi błędów dla VU i IDE.

2.2.5.1 Faza rozpoczęcia komunikacji

DDP_020 Jeżeli w czasie fazy rozpoczęcia komunikacji IDE wykryje błąd synchronizacji lub strumienia bitowego, to odczekuje okres P3min przed powtórnym wysłaniem żądania.

DDP_021 Jeżeli VU wykryje błąd w sekwencji przychodzącej z IDE, to nie wysyła żadnej odpowiedzi i czeka na następny komunikat „Start Communication Request" przez okres P3 max.

2.2.5.2 Faza komunikacji

W tym przypadku można zdefiniować dwa różne obszary obsługi błędów:

1. **VU wykrywa błąd transmisji IDE.**

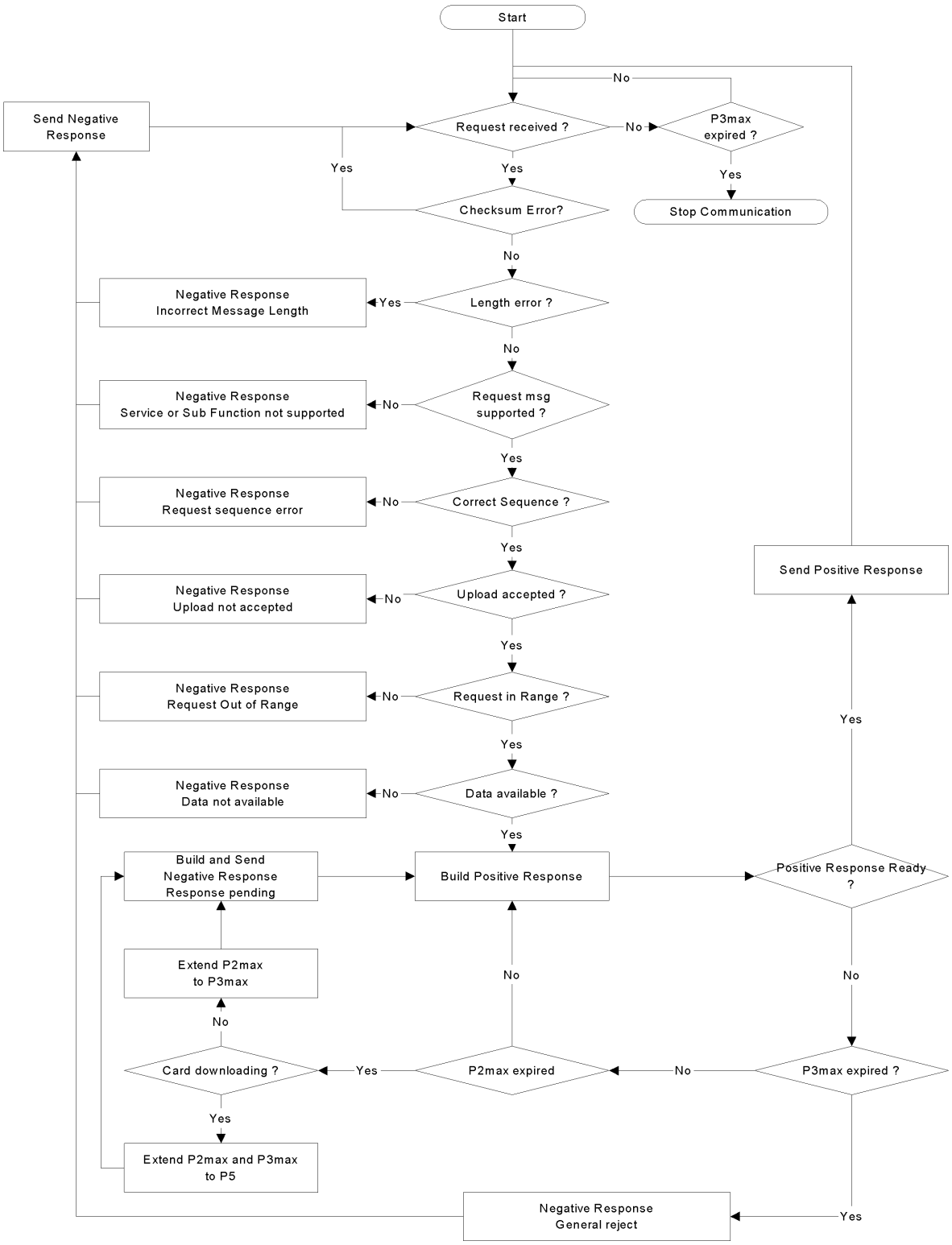
DDP_022 Dla każdego odebranego komunikatu VU wykrywa błędy synchronizacji, błędy formatu bajtowego (np. błędy bitów startu i stopu) i błędy ramki (zła liczba odebranych bajtów, zły bajt sumy kontrolnej).

DDP_023 Jeżeli VU wykryje jeden z powyższych błędów, to nie wysyła odpowiedzi i ignoruje odebrany komunikat.

DDP_024 VU może wykrywać inne błędy formatu lub treści otrzymanego komunikatu (np. komunikat nieobsługiwany), nawet jeżeli długości i sumy kontrolne są prawidłowe; w takim przypadku VU wysyła do IDE komunikat negatywnej odpowiedzi „Negative Response" określający charakter błędu.

Rysunek 2

Obsługa błędów w VU



2. **IDE WYKRYWA BŁĄD TRANSMISJI VU**

DDP_025 Dla każdego odebranego komunikatu IDE wykrywa błędy synchronizacji, błędy formatu bajtowego (np. błędy bitów startu i stopu) i błędy ramki (zła liczba odebranych bajtów, zły bajt sumy kontrolnej).

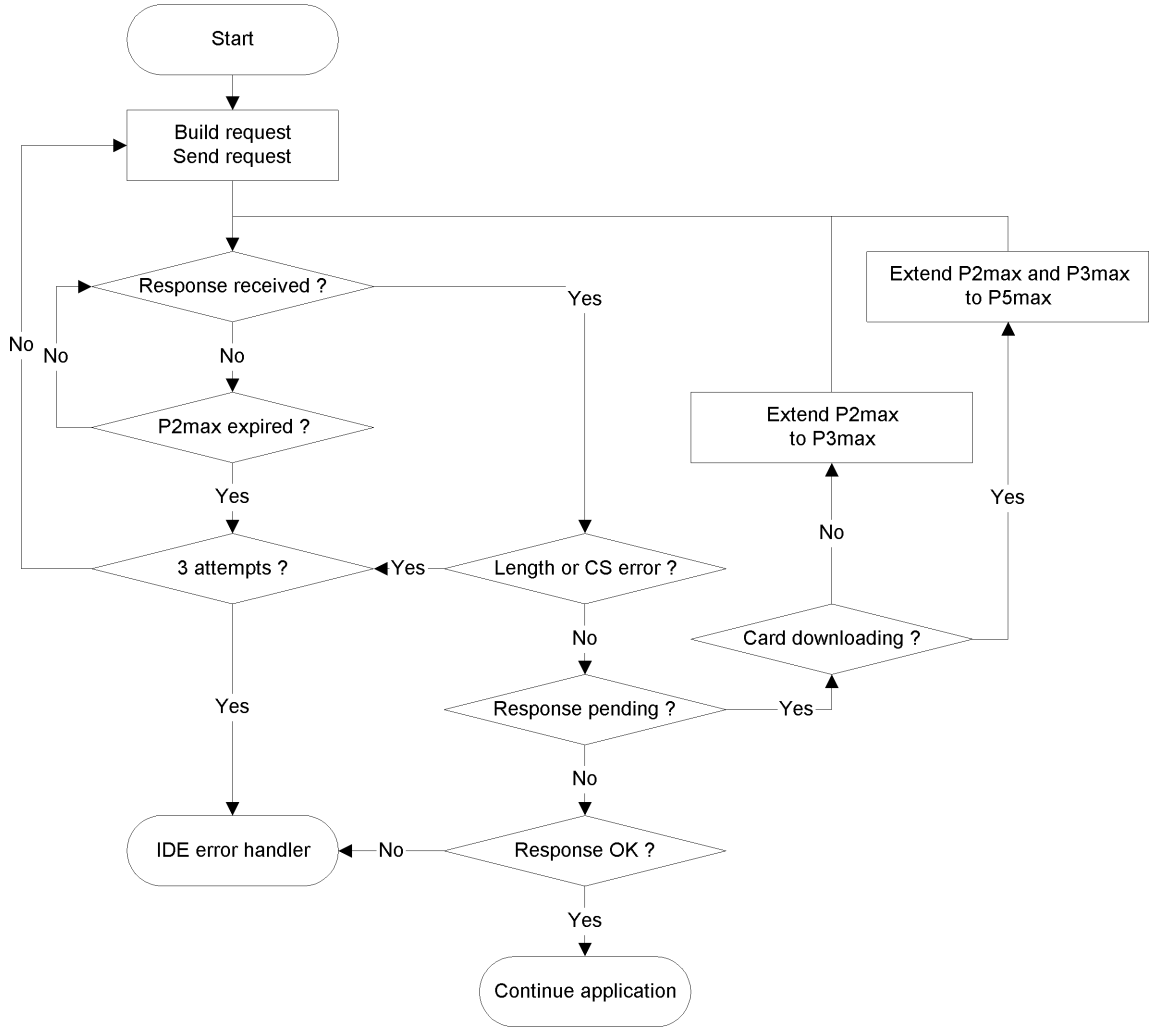
DDP_026 IDE wykrywa błędy kolejności, np. nieprawidłowe zwiększenie stanu licznika podkomunikatów w kolejnych komunikatach.

DDP_027 Jeżeli IDE wykrywa błąd lub nie ma odpowiedzi z VU w okresie P2max, wysyła ponownie komunikat żądania, z tym że mogą być maksymalnie trzy transmisje. Na potrzeby tego wykrywania błędów VU traktuje potwierdzenie podkomunikatu jako żądanie.

DDP_028 Przed rozpoczęciem każdej transmisji IDE oczekuje przez okres P3min; okres oczekiwania odmierza się od ostatniego bitu stopu po wykryciu błędu.

Rysunek 3

Obsługa błędów w IDE



2.2.6 *Treść komunikatu odpowiedzi*

W tym punkcie określono treść pól danych w różnych komunikatach pozytywnej odpowiedzi.

Elementy danych zdefiniowano w dodatku 1 „Słownik danych”.

Uwaga: W przypadku pobrań 2. generacji każdy element danych najwyższego poziomu jest reprezentowany przez tablicę rekordów, nawet jeśli zawiera tylko jeden rekord. Tablica rekordów zaczyna się od nagłówka; nagłówek ten zawiera typ rekordu, wielkość rekordu i liczbę rekordów. Tablice rekordów oznaczone są za pomocą „…RecordArray” (z nagłówkiem) w poniższych tabelach.

2.2.6.1 Positive Response Transfer Data Overview

DDP_029 Pole danych w komunikacie „Positive Response Transfer Data Overview" zawiera następujące dane w określonej tu kolejności pod SID 76 Hex, TREP 01 Hex z odpowiednim podziałem na podkomunikaty i licznikami:

Struktura danych 1. generacji

Element danych	Uwagi
MemberStateCertificate VUCertificate	świadectwa bezpieczeństwa VU
VehicleIdentificationNumber VehicleRegistrationIdentification	identyfikacja pojazdu
CurrentDateTime	bieżąca data i godzina VU
VuDownloadablePeriod	okres do pobrania
CardSlotsStatus	typy kart włożonych do VU
VuDownloadActivityData	poprzednie pobranie danych z VU
VuCompanyLocksData	Wszystkie przechowywane blokady firmowe. Jeżeli sekcja jest pusta, wysyłany jest jedynie noOfLocks = 0.
VuControlActivityData	Wszystkie rekordy dotyczące kontroli przechowywane w VU. Jeżeli sekcja jest pusta, wysyłany jest jedynie noOfControls = 0.
Signature	Podpis RSA wszystkich danych (z wyjątkiem certyfikatów), począwszy od elementu VehicleIdentificationNumber aż do ostatniego bajtu ostatniego elementu VuControlActivityData.

Struktura danych 2. Generacji

Element danych	Uwagi
MemberStateCertificateRecordArray	certyfikat państwa członkowskiego
VUCertificateRecordArray	certyfikat VU
VehicleIdentificationNumberRecordArray	identyfikacja pojazdu
VehicleRegistrationNumberRecordArray	numer rejestracyjny pojazdu
CurrentDateTimeRecordArray	bieżąca data i godzina VU
VuDownloadablePeriodRecordArray	okres do pobrania
CardSlotsStatusRecordArray	typy kart włożonych do VU
VuDownloadActivityDataRecordArray	poprzednie pobranie danych z VU
VuCompanyLocksRecordArray	Wszystkie przechowywane blokady firmowe. Jeżeli sekcja jest pusta, wysyłany jest nagłówek tablicy z noOfRecords = 0.
VuControlActivityRecordArray	Wszystkie rekordy dotyczące kontroli przechowywane w VU. Jeżeli sekcja jest pusta, wysyłany jest nagłówek tablicy z noOfRecords = 0.
SignatureRecordArray	Podpis ECC wszystkich poprzednich danych, z wyjątkiem certyfikatów.

2.2.6.2 Positive Response Transfer Data Activities

DDP_030 Pole danych w komunikacie „Positive Response Transfer Data Activities" zawiera następujące dane w określonej tu kolejności pod SID 76 Hex, TREP 02 Hex z odpowiednim podziałem na podkomunikaty i licznikami:

Struktura danych 1. generacji

Element danych	Uwagi
TimeReal	data pobieranego dnia
OdometerValueMidnight	stan licznika kilometrów na koniec pobieranego dnia
VuCardIWData	Dane dotyczące cykli wkładania wyjmowania kart. — Jeżeli sekcja ta nie zawiera dostępnych danych, wysyłany jest jedynie noOfVuCardIWRecords = 0. — Jeżeli VuCardIWRecord wykracza poza 00:00 (włożenie karty poprzedniego dnia) lub poza 24:00 (wyjęcie karty następnego dnia), musi pojawiać się w pełni w ciągu dwóch odpowiednich dni.
VuActivityDailyData	Stan szczelin o godzinie 00:00 i zmiany czynności zapisane dla pobieranego dnia.
VuPlaceDailyWorkPeriodData	Dane dotyczące miejsc zapisane dla pobieranego dnia. Jeżeli sekcja jest pusta, wysyłany jest jedynie noOfPlaceRecords = 0.
VuSpecificConditionData	Dane dotyczące warunków szczególnych zapisane dla pobieranego dnia. Jeżeli sekcja jest pusta, wysyłany jest jedynie noOfSpecificConditionRecords=0.
Signature	Podpis RSA wszystkich danych, począwszy od elementu TimeReal aż do ostatniego bajtu ostatniego rekordu dotyczącego stanu szczególnego.

Struktura danych 2. generacji:

Element danych	Uwagi
DateOfDayDownloadedRecordArray	data pobieranego dnia
OdometerValueMidnightRecordArray	stan licznika kilometrów na koniec pobieranego dnia
VuCardIWRecordArray	Dane dotyczące cykli wkładania wyjmowania kart. — Jeżeli ta sekcja nie zawiera dostępnych danych, wysyłany jest nagłówek tablicy z noOfRecords = 0. — Jeżeli VuCardIWRecord wykracza poza 00:00 (włożenie karty poprzedniego dnia) lub poza 24:00 (wyjęcie karty następnego dnia), musi pojawiać się w pełni w ciągu dwóch odpowiednich dni.
VuActivityDailyRecordArray	Stan szczelin o godzinie 00:00 i zmiany czynności zapisane dla pobieranego dnia.
VuPlaceDailyWorkPeriodRecordArray	Dane dotyczące miejsc zapisane dla pobieranego dnia. Jeżeli sekcja jest pusta, wysyłany jest nagłówek tablicy z noOfRecords = 0.
VuGNSSCDRecordArray	Pozycje GNSS dla pojazdu, jeżeli nieprzerwany czas prowadzenia pojazdu przez kierowcę osiągnie wielokrotność trzech godzin. Jeżeli sekcja jest pusta, wysyłany jest nagłówek tablicy z noOfRecords = 0.
VuSpecificConditionRecordArray	Dane dotyczące warunków szczególnych zapisane dla pobieranego dnia. Jeżeli sekcja jest pusta, wysyłany jest nagłówek tablicy z noOfRecords =0.
SignatureRecordArray	Podpis ECC wszystkich poprzednich danych.

2.2.6.3 Positive Response Transfer Data Events and Faults

DDP_031 Pole danych w komunikacie „Positive Response Transfer Data Events and Faults" zawiera następujące dane w określonej tu kolejności pod SID 76 Hex, TREP 03 Hex, z odpowiednim podziałem na podkomunikaty i z licznikami:

Struktura danych 1. generacji

Element danych	Uwagi
VuFaultData	Wszystkie usterki przechowywane lub trwające w VU. Jeżeli sekcja jest pusta, wysyłany jest jedynie noOfVuFaults = 0.
VuEventData	Wszystkie zdarzenia (z wyjątkiem przekroczenia prędkości) przechowywane lub trwające w VU. Jeżeli sekcja jest pusta, wysyłany jest jedynie noOfVuEvents = 0.
VuOverSpeedingControlData	Dane dotyczące ostatniej kontroli przekroczenia prędkości (wartość domyślna w przypadku braku danych).
VuOverSpeedingEventData	Wszystkie zdarzenia dotyczące przekroczenia prędkości przechowywane w VU. Jeżeli sekcja jest pusta, wysyłany jest jedynie noOfVuOverSpeedingEvents = 0.
VuTimeAdjustmentData	Wszystkie zdarzenia dotyczące korekty czasu przechowywane w VU (poza ramami pełnej kalibracji). Jeżeli sekcja jest pusta, wysyłany jest jedynie noOfVuTimeAdjRecords = 0.
Signature	Podpis RSA wszystkich danych, począwszy od noOfVuFaults aż do ostatniego bajtu ostatniego rekordu dotyczącego korekty czasu.

Struktura danych 2. generacji:

Element danych	Uwagi
VuFaultRecordArray	Wszystkie usterki przechowywane lub trwające w VU. Jeżeli sekcja jest pusta, wysyłany jest nagłówek tablicy z noOfRecords = 0.
VuEventRecordArray	Wszystkie zdarzenia (z wyjątkiem przekroczenia prędkości) przechowywane lub trwające w VU. Jeżeli sekcja jest pusta, wysyłany jest nagłówek tablicy z noOfRecords = 0.
VuOverSpeedingControlDataRecordArray	Dane dotyczące ostatniej kontroli przekroczenia prędkości (wartość domyślna w przypadku braku danych).
VuOverSpeedingEventRecordArray	Wszystkie zdarzenia dotyczące przekroczenia prędkości przechowywane w VU. Jeżeli sekcja jest pusta, wysyłany jest nagłówek tablicy z noOfRecords = 0.
VuTimeAdjustmentRecordArray	Wszystkie zdarzenia dotyczące korekty czasu przechowywane w VU (poza ramami pełnej kalibracji). Jeżeli sekcja jest pusta, wysyłany jest nagłówek tablicy z noOfRecords = 0.
VuTimeAdjustmentGNSSRecordArray	
SignatureRecordArray	Podpis ECC wszystkich poprzednich danych.

2.2.6.4 Positive Response Transfer Data Detailed Speed

DDP_032 Pole danych w komunikacie „Positive Response Transfer Data Detailed Speed" zawiera następujące dane w określonej tu kolejności pod SID 76 Hex, TREP 04 Hex z odpowiednim podziałem na podkomunikaty i licznikami:

Struktura danych 1. generacji

Element danych	Uwagi
VuDetailedSpeedData	Wszystkie szczegółowe dane dotyczące prędkości przechowywane w VU (jeden blok prędkości dla minuty, przez którą pojazd był w ruchu). 60 wartości prędkości na minutę (jedna na sekundę).
Signature	Podpis RSA wszystkich danych, począwszy od noOfSpeedBlocks aż do ostatniego bajtu ostatniego bloku prędkości.

Struktura danych 2. generacji:

Element danych	Uwagi
VuDetailedSpeedBlockRecordArray	Wszystkie szczegółowe dane dotyczące prędkości przechowywane w VU (jeden blok prędkości dla minuty, przez którą pojazd był w ruchu). 60 wartości prędkości na minutę (jedna na sekundę).
SignatureRecordArray	Podpis ECC wszystkich poprzednich danych.

2.2.6.5 Positive Response Transfer Data Technical Data

DDP_033 Pole danych w komunikacie „Positive Response Transfer Data Technical Data" zawiera następujące dane w określonej tu kolejności pod SID 76 Hex, TREP 05 Hex z odpowiednim podziałem na podkomunikaty i licznikami:

Struktura danych 1. generacji

Element danych	Uwagi
VuIdentification	
SensorPaired	
VuCalibrationData	Wszystkie rekordy dotyczące kalibracji przechowywane w VU.
Signature	Podpis RSA wszystkich danych, począwszy od vuManufacturerName aż do ostatniego bajtu ostatniego VuCalibrationRecord.

Struktura danych 2. generacji:

Element danych	Uwagi
VuIdentificationRecordArray	
VuSensorPairedRecordArray	Wszystkie sparowania państw członkowskich przechowywane w VU.
VuSensorExternalGNSSCoupledRecordArray	Wszystkie powiązania urządzenia zewnętrznego GNSS przechowywane w VU.
VuCalibrationRecordArray	Wszystkie rekordy dotyczące kalibracji przechowywane w VU.
VuCardRecordArray	Wszystkie dane dotyczące włożenia karty przechowywane w VU.
VuITSConsentRecordArray	
VuPowerSupplyInterruptionRecordArray	
SignatureRecordArray	Podpis ECC wszystkich poprzednich danych.

2.3. **Gromadzenie plików na ESM**

DDP_034 Jeżeli sesja pobierania obejmuje przesłanie danych z VU, IDE w jednym fizycznym pliku przechowuje wszystkie dane odebrane z VU w czasie tej sesji przesłane z komunikatami „Positive Response Transfer Data". Dane przechowuje się bez nagłówków komunikatów, liczników podkomunikatów, pustych podkomunikatów i sum kontrolnych, ale wraz z SID i TREP (tylko pierwszego podkomunikatu w przypadku kilku podkomunikatów).

3. PROTOKÓŁ POBIERANIA DANYCH Z KART DO TACHOGRAFÓW

3.1. **Zakres**

W tym punkcie opisano bezpośrednie pobieranie danych z karty do tachografu do IDE. IDE nie jest częścią bezpiecznego środowiska; dlatego też nie wykonuje się uwierzytelnienia między kartą a IDE.

3.2. **Definicje**

Sesja pobierania: Sesja pobierania ma miejsce za każdym razem, gdy pobiera się dane z karty ICC. Sesja obejmuje całą procedurę od zainicjowania karty ICC przez IFD do dezaktywowania karty ICC (wyjęcie karty lub następne zainicjowanie).

Podpisany plik danych: Plik z karty ICC. Plik przesyła się do IFD w formie odkrytego tekstu. Na karcie ICC skrót pliku jest obliczany i podpisywany, a podpis jest przesyłany do IFD.

3.3. **Pobieranie danych z karty**

DDP_035 Pobieranie danych z karty do tachografu obejmuje następujące kroki:

— Pobieranie wspólnych informacji zawartych na karcie w plikach EF ICC i IC. Dane te są nieobowiązkowe i nie są chronione podpisem cyfrowym.

— Pobranie plików EF Card_Certificate (lub CardSignCertificate) i CA_Certificate. Dane te nie są chronione podpisem cyfrowym.

Pobranie tych plików jest obowiązkowe dla każdej sesji pobierania.

— Pobranie plików EF zawierających inne dane aplikacyjne (w Tachograph DF i Tachograph_G2 DF, w stosownych przypadkach) z wyłączeniem EF Card_Download. Dane te są chronione podpisem cyfrowym.

— Pobranie przynajmniej plików EF Application_Identification i ID jest obowiązkowe dla każdej sesji pobierania.

— Przy pobieraniu danych z karty kierowcy obowiązkowe jest pobranie także następujących plików EF:

- `Events_Data`,
- `Faults_Data`,
- `Driver_Activity_Data`,
- `Vehicles_Used`,
- `Places`,
- `GNSS_Places (w odpowiednich przypadkach)`,
- `Control_Activity_Data`,
- `Specific_Conditions`.

— Przy pobieraniu danych z karty kierowcy, aktualizowana jest data `LastCardDownload` w EF `Card_Download`.

— Przy pobieraniu danych z karty warsztatowej, zerowany jest licznik kalibracji w EF `Card_Download`.

— Przy pobieraniu danych z karty warsztatowej plik `EF Sensor_Installation_Data` nie jest pobierany.

3.3.1 *Sekwencja inicjalizująca*

DDP_036 IDE inicjuje następującą sekwencję:

Karta	Kierunek	IDE/IFD	Znaczenie/Uwagi
	⇦	restart sprzętowy	
ATR	⇨		

Opcjonalnie można używać protokołu PPS do przełączania na większą szybkość transmisji, o ile ICC obsługuje tę funkcję.

3.3.2 *Sekwencja dla niepodpisanych plików danych*

DDP_037 Sekwencja pobierania plików elementarnych ICC, IC, Card_Certificate (lub CardSignCertificate) i CA_Certificate jest następująca:

Karta	Kierunek	IDE/IFD	Znaczenie/Uwagi
	⇦	**Select File**	wybierz poprzez identyfikator pliku
OK	⇨		
	⇦	**Read Binary**	Jeżeli wielkość danych w pliku jest większa od pojemności bufora czytnika lub karty, polecenie musi być powtarzane aż do odczytania całego pliku.
File Data **OK**	⇨	zapisz dane na ESM	zgodnie z pkt **3.4** Format gromadzenia danych

Uwaga 1: przed wybraniem Card_Certificate (lub CardSignCertificate) EF musi być wybrana aplikacja tachograficzna (wybór poprzez AID).

Uwaga 2: wybór i odczyt pliku może być również wykonany za jednym razem przy użyciu polecenia Read Binary z krótkim identyfikatorem EF.

3.3.3 *Sekwencja dla podpisanych plików danych*

DDP_038 Dla każdego pliku, który pobrany jest z podpisem, stosuje się następującą sekwencję operacji:

Karta	Kierunek	IDE/IFD	Znaczenie/Uwagi
	⇦	**Select File**	
OK	⇨		
	⇦	**Perform Hash of File**	Oblicza wartość skrótu dla danych wybranego pliku przy pomocy wymaganego algorytmu skrótu zgodnie z dodatkiem 11. Polecenie to nie jest poleceniem ISO.
oblicz skrót pliku i czasowo zachowaj wartość skrótu			
OK	⇨		
	⇦	**Read Binary**	Jeżeli wielkość danych w pliku jest większa od pojemności bufora czytnika lub karty, polecenie musi być powtarzane aż do odczytania całego pliku.
File Data **OK**	⇨	zapisz odebrane dane na ESM	zgodnie z pkt **3.4** Format gromadzenia danych
	⇦	**PSO: Compute Digital Signature**	
wykonaj operację zabezpieczającą „Compute Digital Signature", używając czasowo zachowaną wartość skrótu			
Signature **OK**	⇨	dołącz dane do poprzednio zapisanych danych na ESM	zgodnie z pkt **3.4** Format gromadzenia danych

Uwaga: wybór i odczyt pliku może być również wykonany za jednym razem przy użyciu polecenia Read Binary z krótkim identyfikatorem EF. W tym przypadku EF może być wybrany i odczytany przed zastosowaniem polecenia Perform Hash of File.

3.3.4 *Sekwencja zerowania licznika kalibracji*

DDP_039 Sekwencja zerowania licznika kalibracji `NoOfCalibrationsSinceDownload` w pliku EF `Card_Download` na karcie warsztatowej jest następująca:

Karta	Kierunek	IDE/IFD	Znaczenie/Uwagi
	⇦	**Select File** EF Card_Download	wybierz poprzez identyfikator pliku
OK	⇨		

Karta	Kierunek	IDE/IFD	Znaczenie/Uwagi
	⇦	**Update Binary** NoOfCalibrationsSinceDownload = '00 00'	
zeruje liczbę pobrań danych z karty			
OK	⇨		

Uwaga: wybór i odczyt pliku może być również wykonany za jednym razem przy użyciu polecenia Update Binary z krótkim identyfikatorem EF.

3.4. **Format gromadzenia danych**

3.4.1 *Wprowadzenie*

DDP_040 Pobrane dane należy przechowywać w sposób zgodny z następującymi wymaganiami:

— Dane przechowuje się transparentnie. Oznacza to, że przy gromadzeniu należy zachować kolejność bajtów, jak i kolejność bitów w bajcie taką jak przy przesyłaniu z karty.

— Wszystkie pliki pobrane z karty w ramach sesji pobierania przechowuje się w jednym pliku na ESM.

3.4.2 *Format pliku*

DDP_041 Format pliku jest konkatenacją kilku obiektów TLV.

DDP_042 Znacznikiem pliku EF jest jego identyfikator FID z dodatkiem „00".

DDP_043 Znacznikiem podpisu pliku EF jest identyfikator pliku FID z dodatkiem „01".

DDP_044 Długość podana jest w postaci dwubajtowej wartości. Wartość określa liczbę bajtów w polu wartości. Wartość „FF FF" w polu długości jest zastrzeżona do wykorzystania w przyszłości.

DDP_045 Gdy plik nie jest pobrany, nie zachowuje się żadnych danych dotyczących tego pliku (nie ma znacznika i nie ma zerowej długości).

DDP_046 Podpis zachowuje się w obiekcie TLV znajdującym się bezpośrednio za obiektem TLV zawierającym dane pliku.

Definicja	Znaczenie	Długość
FID (2 bajty) || „00"	Znacznik pliku EF (FID)	3 bajty
FID (2 bajty) || „01"	Znacznik podpisu pliku EF (FID)	3 bajty
xx xx	pole Wartość długości	2 bajty

Przykładowe dane w pliku pobranym na ESM:

Znacznik	Długość	Wartość
00 02 00	00 11	Dane pliku EF ICC
C1 00 00	00 C2	Dane pliku EF Card_Certificate
		…
05 05 00	0A 2E	Dane pliku EF Vehicles_Used
05 05 01	00 80	Podpis pliku EF Vehicles_Used

4. POBIERANIE DANYCH Z KARTY DO TACHOGRAFU ZA POŚREDNICTWEM PRZYRZĄDU REJESTRUJĄCEGO

DDP_047 VU musi umożliwiać pobieranie danych z włożonej karty kierowcy do przyłączonego IDE.

DDP_048 IDE wysyła do VU komunikat „Transfer Data Request Card Download" w celu zainicjowania tego trybu (zob. pkt 2.2.2.9).

DDP_049 Następnie VU pobiera wszystkie dane z karty, plik po pliku, zgodnie z protokołem pobierania danych z karty zdefiniowanym w pkt 3 oraz przekazuje wszystkie dane odebrane z karty do IDE w odpowiednim formacie pliku TLV (zob. 3.4.2) i zapakowane w komunikacie „Positive Response Transfer Data".

DDP_050 IDE odzyskuje dane z karty z komunikatu „Positive Response Transfer Data" (usuwając wszystkie nagłówki, SID, TREP, liczniki podkomunikatów i sumy kontrolne) i zachowuje te dane w jednym fizycznym pliku jak opisano w pkt 2.3.

DDP_051 Następnie VU, stosownie do przypadku, aktualizuje plik `Control_Activity_Data` lub `Card_Download` na karcie kierowcy.

Dodatek 8

PROTOKÓŁ KALIBRACJI

SPIS TREŚCI

1. WPROWADZENIE

Niniejszy dodatek opisuje wymianę danych między przyrządem rejestrującym a testerem poprzez łącze K-line, które stanowi część interfejsu kalibracyjnego opisanego w dodatku 6. Opisano tu także sterowanie linią sygnałową we/wy w złączu kalibracji.

Komunikaty zestawiające łącze K-line opisano w sekcji 4 „Usługi komunikacyjne".

W niniejszym dodatku wykorzystano koncepcję „sesji" diagnostycznych do ustalania zakresu kontroli K-line dla różnych warunków. Sesją domyślną jest „StandardDiagnosticSession", w której wszystkie dane można odczytać z przyrządu rejestrującego, ale żadnych danych nie można zapisać w przyrządzie rejestrującym.

Wybór sesji diagnostycznej opisano w sekcji 5 „Usługi zarządzania".

Niniejszy dodatek musi być uznany za odnoszący się do obu generacji VU i kart warsztatowych, zgodnie z wymaganiami w zakresie interoperacyjności określonymi w niniejszym rozporządzeniu.

CPR_001 Sesja „ECUProgrammingSession" umożliwia wprowadzanie danych do przyrządu rejestrującego. W przypadku wprowadzania danych kalibracyjnych przyrząd rejestrujący musi pracować w trybie KALIBRACYJNYM.

Przesyłanie danych poprzez K-line opisano w sekcji 6 „Usługi przesyłania danych". Formaty przesyłanych danych opisano szczegółowo w sekcji 8 „Formaty dataRecords".

CPR_002 Sesja „ECUAdjustmentSession" umożliwia wybranie trybu we/wy dla linii sygnałowej we/wy kalibracji poprzez interfejs K-line. Sterowanie linią sygnałową we/wy kalibracji opisano w sekcji 7„Sterowanie impulsami testującymi – jednostka funkcjonalna sterowania we/wy".

CPR_003 W niniejszym dokumencie adres testera określony jest jako „tt". Chociaż mogą być zalecane adresy dla testerów, VU odpowiada prawidłowo na dowolny adres testera. Fizycznym adresem VU jest 0xEE.

2. POJĘCIA, DEFINICJE I ODNIESIENIA

Protokoły, komunikaty i kody błędów oparte są zasadniczo na projekcie normy ISO 14229-1 (Pojazdy drogowe — Systemy diagnostyczne — część 1: Usługi diagnostyczne, wersja 6 z dnia 22 lutego 2001 r.).

Kodowania bajtowego i wartości heksadecymalnych używa się w identyfikatorach usług, żądaniach usług i odpowiedziach oraz parametrach standardowych.

Pojęcie „tester" oznacza urządzenie służące do wprowadzania do VU danych programistycznych/kalibracyjnych.

Pojęcia „klient" i „serwer" oznaczają odpowiednio tester i VU.

Pojęcie ECU oznacza „sterownik elektroniczny" i odnosi się do VU.

Odniesienia:

ISO 14230-2:

Pojazdy drogowe – Systemy diagnostyczne – Protokół słowa kluczowego 2000 – część 2: Warstwa łącza danych). Wydanie pierwsze: 1999.

Pojazdy – systemy diagnostyczne.

3. INFORMACJE OGÓLNE O USŁUGACH

3.1. **Dostępne usługi**

Tabela poniżej zawiera informacje ogólne o usługach, które są dostępne w tachografie i są zdefiniowane w niniejszym dokumencie.

CPR_004 Tabela wskazuje usługi dostępne przy włączonej sesji diagnostycznej.

— **Pierwsza kolumna** zawiera wykaz dostępnych usług.

— **Druga kolumna** zawiera numer sekcji w niniejszym dodatku, gdzie usługa jest dokładniej zdefiniowana.

— **Trzecia kolumna** przypisuje wartości identyfikatora usługi dla komunikatów żądań.

— **Czwarta kolumna** określa usługi **„StandardDiagnosticSession" (SD)**, których wdrożenie jest wymagane w każdym VU.

— **Piąta kolumna** określa usługi **„ECUAdjustmentSession" (ECUAS)**, które muszą być wdrożone w celu umożliwienia sterowania linią sygnałową we/wy w złączu kalibracji w panelu czołowym VU.

— **Szósta kolumna** określa usługi **„ECUProgrammingSession" (ECUPS)**, które muszą być wdrożone w celu umożliwienia programowania parametrów w VU.

Tabela 1

Zestawienie wartości identyfikatorów usług

			Sesje diagnostyczne		
Nazwa usługi diagnostycznej	Sekcja nr	Wartość SId Req.	SD	ECUAS	ECUPS
StartCommunication	4.1	81	■	■	■
StopCommunication	4.2	82	■		
TesterPresent	4.3	3E	■	■	■
StartDiagnosticSession	5.1	10	■	■	■
SecurityAccess	5.2	27	■	■	■
ReadDataByIdentifier	6.1	22	■	■	■
WriteDataByIdentifier	6.2	2E			■
InputOutputControlByIdentifier	7.1	2F		■	

■ Symbol ten oznacza, że usługa jest obowiązkowa w tej sesji diagnostycznej.

Brak symbolu oznacza, że usługa nie jest dozwolona w tej sesji diagnostycznej.

3.2. **Kody odpowiedzi**

Kody odpowiedzi są zdefiniowane dla każdej usługi.

4. USŁUGI KOMUNIKACYJNE

Niektóre usługi są niezbędne do ustanowienia i utrzymania komunikacji. Nie występują one w warstwie aplikacji. Dostępne usługi wyszczególniono w tabeli poniżej:

Tabela 2

Usługi komunikacyjne

Nazwa usługi	Wyszczególnienie
StartCommunication	Klient żąda rozpoczęcia sesji komunikacyjnej z serwerem(-ami).
StopCommunication	Klient żąda zaprzestania bieżącej sesji komunikacyjnej.
TesterPresent	Klient wskazuje serwerowi, że jest jeszcze obecny.

CPR_005 Usługa StartCommunication służy do rozpoczęcia komunikacji. W celu wykonania usługi konieczne jest zainicjowanie komunikacji i ustawienie parametrów odpowiednio dla pożądanego trybu.

4.1. **Usługa StartCommunication**

CPR_006 Po odebraniu prymitywu wskazania StartCommunication VU sprawdza, czy w obecnych warunkach można zainicjować żądane łącze komunikacyjne. Warunki zezwalające na zainicjowanie łącza komunikacyjnego opisano w normie ISO 14230-2.

CPR_007 Następnie VU wykonuje wszystkie działania niezbędne do zainicjowania łącza komunikacyjnego i wysyła prymityw odpowiedzi StartCommunication z wybranymi parametrami Positive Response.

CPR_008 Jeżeli VU, który jest już zainicjowany (ma otwartą dowolną sesję diagnostyczną), otrzymuje nowe żądanie StartCommunication (np. wskutek usuwania błędu w testerze), żądanie zostanie przyjęte, a VU ponownie zainicjowany.

CPR_009 Jeżeli z jakiejkolwiek przyczyny nie można zainicjować łącza komunikacyjnego, VU pracuje tak jak pracował bezpośrednio przed próbą zainicjowania łącza komunikacyjnego.

CPR_010 Komunikat żądania StartCommunication musi mieć fizyczny adres.

CPR_011 Inicjowanie usług w VU odbywa się metodą „szybkiej inicjalizacji”:

— Przed każdą czynnością występuje czas jałowy magistrali.

— Następnie tester wysyła kod inicjujący.

— Wszystkie informacje niezbędne do nawiązania komunikacji zawarte są w odpowiedzi VU.

CPR_012 Po zakończeniu inicjalizacji:

— Wszystkie parametry komunikacyjne zostają ustawione na wartości zdefiniowane w tabeli 4 zgodnie z bajtami kluczowymi.

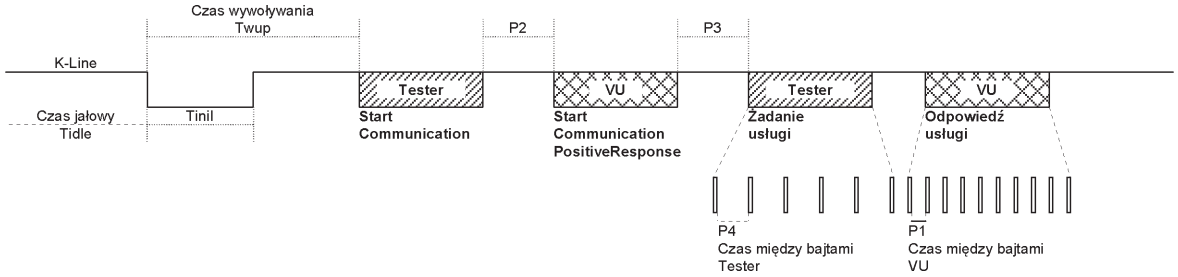
— VU czeka na pierwsze żądanie testera.

— VU znajduje się w domyślnym trybie diagnostycznym, tj. StandardDiagnosticSession.

— Linia sygnałowa we/wy kalibracji jest w stanie domyślnym, tj. w stanie „disabled" (wyłączona).

CPR_014 Szybkość transmisji K-line jest ustawiona na 10 400 bodów.

CPR_016 Szybką inicjalizację uruchamia tester, wysyłając kod wywoływania (Wup) przez K-line. Kod rozpoczyna się po czasie jałowym na K-line niskim stanem w czasie Tinil. Tester wysyła pierwszy bit usługi StartCommunication po czasie Twup następującym po pierwszej krawędzi opadającej.



CPR_017 Wartości czasów dla szybkiej inicjalizacji i ogólnie komunikatów podano w tabeli poniżej. Dla czasu jałowego są różne możliwości:

— pierwsza transmisja po włączeniu zasilania, Tidle = 300 ms;

— po zakończeniu usługi StopCommunication, Tidle = P3 min;

— po zatrzymaniu komunikacji wskutek upływu czasu oczekiwania P3 max, Tidle = 0.

Tabela 3

Wartości czasów dla szybkiej inicjalizacji

Parametr		Wartość min.	Wartość maks.
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

Tabela 4

Wartości czasów dla komunikacji

Parametr czasowy	Opis parametru	Dolna granica [ms]	Górna granica [ms]
		min.	maks.
P1	Czas między bajtami dla odpowiedzi VU	0	20
P2	Czas między żądaniem testera a odpowiedzią VU lub dwiema odpowiedziami VU	25	250
P3	Czas między końcem odpowiedzi VU a początkiem nowego żądania testera	55	5 000
P4	Czas między bajtami dla żądania testera	5	20

CPR_018 Format komunikatu dla szybkiej inicjalizacji opisano szczegółowo w poniższych tabelach.

Tabela 5

Komunikat StartCommunication Request

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne	81	FMT
#2	Bajt adresu docelowego	EE	TGT
#3	Bajt adresu źródłowego	tt	SRC
#4	**StartCommunication Request Service Id**	**81**	**SCR**
#5	Suma kontrolna	00-FF	CS

Tabela 6

Komunikat StartCommunication Positive Reponse

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	03	LEN
#5	**StartCommunication Positive Response Service Id**	**C1**	**SCRPR**
#6	Bajt kluczowy 1	EA	KB1
#7	Bajt kluczowy 2	8F	KB2
#8	Suma kontrolna	00-FF	CS

CPR_019 Nie ma negatywnej odpowiedzi na komunikat StartCommunication Request, gdy nie zostanie wysłana pozytywna odpowiedź, VU nie zostaje zainicjowany, nic nie jest przesyłane i VU pozostaje w stanie normalnej pracy.

4.2. **Usługa StopCommunication**

4.2.1 *Opis komunikatu*

Celem tej usługi warstwy komunikacji jest zakończenie sesji komunikacyjnej.

CPR_020 Po odebraniu prymitywu wskazania StopCommunication VU sprawdza, czy bieżące warunki pozwalają na zakończenie tej komunikacji. W tym przypadku VU wykonuje wszystkie działania niezbędne do zakończenia sesji komunikacyjnej.

CPR_021 Jeżeli zakończenie sesji komunikacyjnej jest możliwe, VU – przed zakończeniem komunikacji – wysyła prymityw odpowiedzi StopCommunication z wybranymi parametrami Positive Response.

CPR_022 Jeżeli zakończenie sesji komunikacyjnej nie jest możliwe z jakiejkolwiek przyczyny, VU wysyła prymityw odpowiedzi StopCommunication z wybranym parametrem Negative Response.

CPR_023 Jeżeli VU wykryje przekroczenie czasu P3 max, komunikacja zostaje zakończona bez wysyłania żadnego prymitywu odpowiedzi.

4.2.2 *Format komunikatu*

CPR_024 Formaty komunikatu dla prymitywów StopCommunication opisano szczegółowo w poniższych tabelach.

Tabela 7

Komunikat StopCommunication Request

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	EE	TGT
#3	Bajt adresu źródłowego	tt	SRC
#4	Dodatkowy bajt długości	01	LEN
#5	**StopCommunication Request Service Id**	**82**	**SPR**
#6	Suma kontrolna	00-FF	CS

Tabela 8

Komunikat StopCommunication Positive Response

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	01	LEN
#5	**StopCommunication Positive Response Service Id**	**C2**	**SPRPR**
#6	Suma kontrolna	00-FF	CS

Tabela 9

Komunikat StopCommunication Negative Response

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	03	LEN
#5	**negative Response Service Id**	**7F**	**NR**
#6	StopCommunication Request Service Identification	82	SPR
#7	responseCode = generalReject	10	RC_GR
#8	Suma kontrolna	00-FF	CS

4.2.3 *Definicja parametru*

Ta usługa nie wymaga żadnych definicji parametrów.

4.3. **Usługa TesterPresent**

4.3.1 *Opis komunikatu*

Tester używa usługi TesterPresent do wskazania serwerowi, że jeszcze jest obecny, w celu zapobieżenia automatycznemu powrotowi serwera do normalnego trybu pracy i zerwania komunikacji. Usługa ta, wysyłana okresowo, utrzymuje sesję diagnostyczną/komunikacyjną w stanie aktywnym, zerując timer P3 za każdym razem po odebraniu żądania tej usługi.

4.3.2 *Format komunikatu*

CPR_079 Formaty komunikatu dla prymitywów TesterPresent opisano szczegółowo w poniższych tabelach.

Tabela 10

Komunikat TesterPresent Request

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	EE	TGT
#3	Bajt adresu źródłowego	tt	SRC
#4	Dodatkowy bajt długości	02	LEN
#5	**TesterPresent Request Service Id**	**3E**	**TP**

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#6	podfunkcja = responseRequired = [tak	01	RESPREQ_Y
	nie]	02	RESPREQ_NO
#7	Suma kontrolna	00-FF	CS

CPR_080 Jeżeli parametr responseRequired jest ustawiony na „tak”, to serwer odpowie niżej przedstawionym komunikatem pozytywnej odpowiedzi. Jeżeli jest ustawiony na „nie”, serwer nie wysyła żadnej odpowiedzi.

Tabela 11

Komunikat TesterPresent Positive Response

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	01	LEN
#5	**TesterPresent Positive Response Service Id**	**7E**	**TPPR**
#6	Suma kontrolna	00-FF	CS

CPR_081 Usługa używa następujących kodów negatywnej odpowiedzi:

Tabela 12

Komunikat TesterPresent Negative Response

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	03	LEN
#5	**negative Response Service Id**	**7F**	**NR**
#6	TesterPresent Request Service Identification	3E	TP

# bajtu	Nazwa parametru		Wartość heksadecymalna	Mnemonik
#7	responseCode =	[SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
		incorrectMessageLength]	13	RC_IML
#8	Suma kontrolna		00-FF	CS

5. USŁUGI ZARZĄDZANIA

Dostępne usługi wyszczególniono w tabeli poniżej:

Tabela 13

Usługi zarządzania

Nazwa usługi	Wyszczególnienie
StartDiagnosticSession	Klient żąda rozpoczęcia sesji diagnostycznej z VU.
SecurityAccess	Klient żąda dostępu do funkcji zastrzeżonych dla uprawnionych użytkowników.

5.1. **Usługa StartDiagnosticSession**

5.1.1 *Opis komunikatu*

CPR_025 Usługa StartDiagnosticSession służy do włączania różnych sesji diagnostycznych w serwerze. Sesja diagnostyczna udostępnia swoisty zestaw usług zgodnie z opisem w Tabeli 17. Sesja może udostępnić producentowi pojazdu usługi swoiste nieobjęte tym dokumentem. Zasady wdrożenia muszą spełniać następujące wymagania:

— W VU aktywna jest zawsze dokładnie jedna sesja diagnostyczna.

— Po włączeniu zasilania VU zawsze uruchamia StandardDiagnosticSession. Jeżeli żadna inna sesja diagnostyczna nie zostanie uruchomiona, wówczas StandardDiagnosticSession pozostaje uruchomiona tak długo, jak włączone jest zasilanie VU.

— Jeżeli jest już uruchomiona sesja diagnostyczna zażądana przez tester, VU wysyła komunikat pozytywnej odpowiedzi.

— Za każdym razem kiedy tester żąda nowej sesji diagnostycznej, VU najpierw wysyła komunikat pozytywnej odpowiedzi StartDiagnosticSession, zanim nowa sesja stanie się aktywna w VU. Jeżeli VU nie może uruchomić żądanej nowej sesji diagnostycznej, to odpowiada komunikatem negatywnej odpowiedzi StartDiagnosticSession i bieżąca sesja jest kontynuowana.

CPR_026 Sesja diagnostyczna może zostać uruchomiona tylko wtedy, gdy nawiązana jest komunikacja między klientem a VU.

CPR_027 Parametry czasowe zdefiniowane w tabeli 4 są aktywne po pomyślnym uruchomieniu sesji StartDiagnosticSession z parametrem diagnosticSession ustawionym na „StandardDiagnosticSession" w komunikacie żądania, jeżeli poprzednio aktywna była inna sesja diagnostyczna.

5.1.2 *Format komunikatu*

CPR_028 Formaty komunikatu dla prymitywów StartDiagnosticSession opisano szczegółowo w poniższych tabelach.

Tabela 14

Komunikat StartDiagnosticSession Request

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	EE	TGT
#3	Bajt adresu źródłowego	tt	SRC
#4	Dodatkowy bajt długości	02	LEN
#5	**StartDiagnosticSession Request Service Id**	**10**	**STDS**
#6	diagnosticSession = [jedna wartość z tabeli 17]	xx	DS_…
#7	Suma kontrolna	00-FF	CS

Tabela 15

Komunikat StartDiagnosticSession Positive Response

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	02	LEN
#5	**StartDiagnosticSession Positive Response Service Id**	**50**	**STDSPR**
#6	diagnosticSession = [ta sama wartość jak dla bajtu #6 w tabeli 14]	xx	DS_…
#7	Suma kontrolna	00-FF	CS

Tabela 16

Komunikat StartDiagnosticSession Negative Response

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT

# bajtu	Nazwa parametru		Wartość heksadecymalna	Mnemonik
#3	Bajt adresu źródłowego		EE	SRC
#4	Dodatkowy bajt długości		03	LEN
#5	**Negative Response Service Id**		**7F**	**NR**
#6	StartDiagnosticSession Request Service Id		10	STDS
#7	ResponseCode =	[subFunctionNotSupported [a]	12	RC_SFNS
		incorrectMessageLength [b]	13	RC_IML
		conditionsNotCorrect [c]	22	RC_CNC
#8	Suma kontrolna		00-FF	CS

[a] – wartość wstawiona w bajcie #6 komunikatu żądania nie jest obsługiwana, tzn. nie ma jej w tabeli 17;
[b] – długość komunikatu jest nieprawidłowa;
[c] – kryteria żądania StartDiagnosticSession nie są spełnione.

5.1.3 *Definicja parametru*

CPR_029 Parametr ***diagnosticSession (DS_)*** używany jest w usłudze StartDiagnosticSession do wybierania szczególnego zachowania serwera(-ów). W niniejszym dokumencie określone są następujące sesje diagnostyczne:

Tabela 17

Definicja wartości diagnosticSession

Heks	Wyszczególnienie	Mnemonik
81	**StandardDiagnosticSession** Ta sesja diagnostyczna udostępnia wszystkie usługi wyszczególnione w **tabeli 1 w kolumnie 4 „SD”**. Usługi te umożliwiają odczyt danych z serwera (VU). Ta sesja diagnostyczna jest aktywna po pomyślnym zakończeniu inicjacji między klientem (tester) a serwerem (VU). Tę sesję diagnostyczną można zastąpić każdą inną sesją diagnostyczną wyszczególnioną w tej sekcji.	**SD**
85	**ECUProgrammingSession** Ta sesja diagnostyczna udostępnia wszystkie usługi wyszczególnione w **tabeli 1 w kolumnie 6 „ECUPS”**. Usługi te wspomagają programowanie pamięci serwera (VU). Tę sesję diagnostyczną można zastąpić każdą inną sesją diagnostyczną wyszczególnioną w tej sekcji.	**ECUPS**
87	**ECUAdjustmentSession** Ta sesja diagnostyczna udostępnia wszystkie usługi wyszczególnione w **tabeli 1 w kolumnie 5 „ECUAS”.** Usługi te wspomagają sterowania we/wy serwera (VU). Tę sesję diagnostyczną można zastąpić każdą inną sesją diagnostyczną wyszczególnioną w tej sekcji.	**ECUAS**

5.2. **Usługa SecurityAccess**

Zapis danych kalibracyjnych nie jest możliwy w trybie KALIBRACYJNYM. Dodatkowo, oprócz włożenia do VU ważnej karty warsztatowej, niezbędne jest wprowadzenie numeru PIN do VU przed uzyskaniem dostępu do trybu KALIBRACYJNEGO.

Jeżeli VU jest w trybie KALIBRACYJNYM lub KONTROLNYM, dostęp do linii we/wy kalibracji jest również możliwy.

Usługa SecurityAccess umożliwia wprowadzenie numeru PIN i przekazanie testerowi, czy VU jest w trybie KALIBRACYJNYM.

Dopuszcza się wprowadzanie numeru PIN alternatywnymi metodami.

5.2.1 *Opis komunikatu*

Usługa SecurityAccess zawiera komunikat SecurityAccess „requestSeed", po którym może nastąpić komunikat SecurityAccess „sendKey". Usługa SecurityAccess musi być przeprowadzona po usłudze StartDiagnosticSession.

CPR_033 Tester używa komunikatu SecurityAccess „requestSeed" do sprawdzenia, czy przyrząd rejestrujący jest gotowy do przyjęcia numeru PIN.

CPR_034 Jeżeli przyrząd rejestrujący jest już w trybie KALIBRACYJNYM, odpowiada na żądanie wysyłając „seed" równy 0x0000 przy pomocy usługi SecurityAccess Positive Response.

CPR_035 Jeżeli przyrząd rejestrujący jest gotowy do przyjęcia numeru PIN w celu zweryfikowania go przez kartę warsztatową, odpowiada na żądanie wysyłając „seed" większy niż 0x0000 przy pomocy usługi SecurityAccess Positive Response.

CPR_036 Jeżeli przyrząd rejestrujący nie jest gotowy do przyjęcia numeru PIN z testera, albo z tego powodu, że włożona karta warsztatowa nie jest ważna lub nie włożono żadnej karty warsztatowej lub przyrząd rejestrujący oczekuje na wprowadzenie numeru PIN inną metodą, odpowiada na żądanie wysyłając negatywną odpowiedź (Negative Reponse) z kodem odpowiedzi ustawionym na conditionsNotCorrectOrRequestSequenceError.

CPR_037 Następnie tester używa ostatecznie komunikatu SecurityAccess „sendKey" do przesłania numeru PIN do przyrządu rejestrującego. Aby karta miała wystarczający czas na przeprowadzenie uwierzytelnienia, VU w celu przedłużenia czasu oczekiwania na odpowiedź używa kodu negatywnej odpowiedzi requestCorrectlyReceived-ResponsePending. Maksymalny czas oczekiwania na odpowiedź nie może jednak przekraczać 5 minut. Gdy tylko żądana usługa zostaje zakończona, VU wysyła komunikat pozytywnej odpowiedzi lub komunikat negatywnej odpowiedzi z kodem odpowiedzi różnym od tego pierwszego kodu. VU może powtarzać kod negatywnej odpowiedzi requestCorrectlyReceived-ResponsePending aż do zakończenia żądanej usługi i wysłania komunikatu ostatecznej odpowiedzi.

CPR_038 Przyrząd rejestrujący odpowiada na to żądanie przy pomocy usługi SecurityAccess Positive Response jedynie wtedy, gdy jest w trybie KALIBRACYJNYM.

CPR_039 W następujących przypadkach przyrząd rejestrujący odpowiada na to żądanie negatywną odpowiedzią (Negative Reponse) z następującą wartością kodu odpowiedzi:

— subFunctionNot supported: niedozwolony format dla parametru podfunkcji (accessType);

— conditionsNotCorrectOrRequestSequenceError: przyrząd rejestrujący nie jest gotowy do przyjęcia numeru PIN;

— invalidKey: nieprawidłowy numer PIN i nieprzekroczona dozwolona liczba prób sprawdzania numeru PIN;

— exceededNumberOfAttempts: nieprawidłowy numer PIN i przekroczona dozwolona liczba prób sprawdzania numeru PIN;

— generalReject: prawidłowy numer PIN, ale nieudane wzajemne uwierzytelnienie z kartą warsztatową.

5.2.2 *Format komunikatu – SecurityAccess – requestSeed*

CPR_040 Formaty komunikatu dla prymitywów SecurityAccess „requestSeed" opisano szczegółowo w poniższych tabelach.

Tabela 18

Komunikat SecurityAccess Request- requestSeed

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	EE	TGT
#3	Bajt adresu źródłowego	tt	SRC
#4	Dodatkowy bajt długości	02	LEN
#5	**SecurityAccess Request Service Id**	**27**	**SA**
#6	accessType – requestSeed	7D	AT_RSD
#7	Suma kontrolna	00-FF	CS

Tabela 19

Komunikat SecurityAccess – requestSeed Positive Response

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	04	LEN
#5	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
#6	accessType – requestSeed	7D	AT_RSD
#7	Seed High	00-FF	SEEDH
#8	Seed Low	00-FF	SEEDL
#9	Suma kontrolna	00-FF	CS

Tabela 20

Komunikat SecurityAccess Negative Response

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#4	Dodatkowy bajt długości	03	LEN
#5	**negativeResponse Service Id**	**7F**	**NR**
#6	SecurityAccess Request Service Id	27	SA
#7	responseCode = [conditionsNotCorrectOrRequestSequenceError incorrectMessageLength]	22 13	RC_CNC RC_IML
#8	Suma kontrolna	00-FF	CS

5.2.3 *Format komunikatu – SecurityAccess – sendKey*

CPR_041 Formaty komunikatu dla prymitywów SecurityAccess „sendKey" opisano szczegółowo w poniższych tabelach.

Tabela 21

Komunikat SecurityAccess Request – sendKey

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	EE	TGT
#3	Bajt adresu źródłowego	tt	SRC
#4	Dodatkowy bajt długości	m+2	LEN
#5	**SecurityAccess Request Service Id**	**27**	**SA**
#6	accessType – sendKey	7E	AT_SK
#7 do #m +6	Klucz#1 (najwyższy) … Klucz #m (niższy, m musi być minimum 4 i maksimum 8)	xx … xx	KEY
#m+7	Suma kontrolna	00-FF	CS

Tabela 22

Komunikat SecurityAccess – sendKey Positive Response

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#4	Dodatkowy bajt długości	02	LEN
#5	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
#6	accessType – sendKey	7E	AT_SK
#7	Suma kontrolna	00-FF	CS

Tabela 23

Komunikat SecurityAccess Negative Response

# bajtu	Nazwa parametru		Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne		80	FMT
#2	Bajt adresu docelowego		tt	TGT
#3	Bajt adresu źródłowego		EE	SRC
#4	Dodatkowy bajt długości		03	LEN
#5	**NegativeResponse Service Id**		**7F**	**NR**
#6	SecurityAccess Request Service Id		27	SA
#7	ResponseCode =	[generalReject	10	RC_GR
		subFunctionNotSupported	12	RC_SFNS
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
		invalidKey	35	RC_IK
		exceededNumberOfAttempts	36	RC_ENA
		requestCorrectlyReceived-ResponsePending]	78	RC_RCR_RP
#8	Suma kontrolna		00-FF	CS

6. USŁUGI PRZESYŁANIA DANYCH

Dostępne usługi wyszczególniono w tabeli poniżej:

Tabela 24

Usługi przesyłania danych

Nazwa usługi	Wyszczególnienie
ReadDataByIdentifier	Klient żąda przesłania bieżącej wartości rekordu z dostępem poprzez recordDataIdentifier.
WriteDataByIdentifier	Klient żąda zapisu rekordu z dostępem poprzez recordDataIdentifier.

6.1. **Usługa ReadDataByIdentifier**

6.1.1 *Opis komunikatu*

CPR_050 Klient używa usługi ReadDataByIdentifier do żądania wartości rekordów danych z serwera. Dane są identyfikowane przez recordDataIdentifier. Producent VU odpowiada za spełnienie warunków serwera przy wykonywaniu tej usługi.

6.1.2 *Format komunikatu*

CPR_051 Formaty komunikatu dla prymitywów ReadDataByIdentifier opisano szczegółowo w poniższych tabelach.

Tabela 25

Komunikat ReadDataByIdentifier Request

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	EE	TGT
#3	Bajt adresu źródłowego	tt	SRC
#4	Dodatkowy bajt długości	03	LEN
#5	**ReadDataByIdentifier Request Service Id**	**22**	**RDBI**
#6 do #7	recordDataIdentifier = [wartość z tabeli 28]	xxxx	RDI_…
#8	Suma kontrolna	00-FF	CS

Tabela 26

Komunikat ReadDataByIdentifier Positive Response

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	m + 3	LEN
#5	**ReadDataByIdentifier Positive Response Service Id**	**62**	**RDBIPR**
#6 i #7	recordDataIdentifier = [ta sama wartość jak dla bajtów #6 i #7 w tabeli 25]	xxxx	RDI_…
#8 do #m + 7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Suma kontrolna	00-FF	CS

Tabela 27

Komunikat ReadDataByIdentifier Negative Response

# bajtu	Nazwa parametru		Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne		80	FMT
#2	Bajt adresu docelowego		tt	TGT
#3	Bajt adresu źródłowego		EE	SRC
#4	Dodatkowy bajt długości		03	LEN
#5	**NegativeResponse Service Id**		**7F**	**NR**
#6	ReadDataByIdentifier Request Service Id		22	RDBI
#7	ResponseCode=	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
#8	Suma kontrolna		00-FF	CS

6.1.3 *Definicja parametru*

CPR_052 Parametr ***recordDataIdentifier (RDI_)*** w komunikacie żądania ReadDataByIdentifier wskazuje rekord danych.

CPR_053 Wartości recordDataIdentifier zdefiniowane w tym dokumencie pokazano w tabeli poniżej.

Tabela recordDataIdentifier składa się z czterech kolumn i wielu rzędów.

— **Pierwsza kolumna (Heks)** zawiera „wartość heksadecymalną" przypisaną identyfikatorowi recordDataIdentifier z trzeciej kolumny.

— **Druga kolumna (Element danych)** określa element danych z dodatku 1, na którym oparty jest identyfikator recordDataIdentifier (czasami niezbędne jest przekodowanie).

— **Trzecia kolumna (Opis)** podaje nazwę odpowiadającego identyfikatora recordDataIdentifier.

— **Czwarta kolumna (Mnemonik)** podaje mnemonik tego identyfikatora recordDataIdentifier.

Tabela 28

Definicja wartości recordDataIdentifier

Heks	Element danych	Nazwa recordDataIdentifier (zob. format w sekcji 8.2)	Mnemonik
F90B	`CurrentDateTime`	TimeDate	RDI_TD
F912	`HighResOdometer`	HighResolutionTotalVehicleDistance	RDI_HRTVD
F918	`K-ConstantOfRecordingEquipment`	Kfactor	RDI_KF

Heks	Element danych	Nazwa recordDataIdentifier (zob. format w sekcji 8.2)	Mnemonik
F91C	L-TyreCircumference	LfactorTyreCircumference	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize	TyreSize	RDI_TS
F922	nextCalibrationDate	NextCalibrationDate	RDI_NCD
F92C	SpeedAuthorised	SpeedAuthorised	RDI_SA
F97D	vehicleRegistrationNation	RegisteringMemberState	RDI_RMS
F97E	VehicleRegistrationNumber	VehicleRegistrationNumber	RDI_ VRN
F190	VehicleIdentificationNumber	VIN	RDI_ VIN

CPR_054 Parametr ***dataRecord (DREC_)*** używany jest w komunikacie pozytywnej odpowiedzi ReadDataByIdentifier do dostarczania wartości rekordu danych wskazanego klientowi (testerowi) identyfikatorem recordDataIdentifier. Formaty danych określono w sekcji 8. Można wprowadzić dodatkowe opcjonalne dataRecords użytkownika obejmujące szczególne dane wejściowe, wewnętrzne i wyjściowe VU, ale nie są one zdefiniowane w tym dokumencie.

6.2. **UsługaWriteDataByIdentifier**

6.2.1 *Opis komunikatu*

CPR_056 Usługa WriteDataByIdentifier używana jest przez klienta do zapisania wartości rekordu danych w serwerze. Dane są identyfikowane przez recordDataIdentifier. Producent VU odpowiada za spełnienie warunków serwera przy wykonywaniu tej usługi. Aby aktualizować parametry wymienione w tabeli 28, VU musi być w trybie KALIBRACYJNYM.

6.2.2 *Format komunikatu*

CPR_057 Formaty komunikatu dla prymitywów WriteDataByIdentifier opisano szczegółowo w poniższych tabelach.

Tabela 29

Komunikat WriteDataByIdentifier Request

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	EE	TGT
#3	Bajt adresu źródłowego	tt	SRC
#4	Dodatkowy bajt długości	m+3	LEN
#5	**WriteDataByIdentifier Request Service Id**	**2E**	**WDBI**
#6 do #7	recordDataIdentifier = [wartość z tabeli 28]	xxxx	RDI_…

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#8 do m +7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Suma kontrolna	00-FF	CS

Tabela 30

Komunikat WriteDataByIdentifier Positive Response

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	03	LEN
#5	**WriteDataByIdentifier Positive Response Service Id**	**6E**	**WDBIPR**
#6 do #7	recordDataIdentifier = [ta sama wartość jak dla bajtów #6 i #7 w tabeli 29]	xxxx	RDI_…
#8	Suma kontrolna	00-FF	CS

Tabela 31

Komunikat WriteDataByIdentifier Negative Response

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	03	LEN
#5	**NegativeResponse Service Id**	**7F**	**NR**
#6	WriteDataByIdentifier Request Service Id	2E	WDBI

# bajtu	Nazwa parametru		Wartość heksadecymalna	Mnemonik
#7	ResponseCode=	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
#8	Suma kontrolna		00-FF	CS

6.2.3 *Definicja parametru*

Parametr ***recordDataIdentifier (RDI_)*** zdefiniowano w tabeli 28.

Parametr ***dataRecord (DREC_)*** używany jest w komunikacie żądania WriteDataByIdentifier do dostarczenia wartości rekordu danych wskazanego serwerowi (VU) przez recordDataIdentifier. Formaty danych określono w sekcji 8.

7. STEROWANIE IMPULSAMI TESTUJĄCYMI – JEDNOSTKA FUNKCJONALNA STEROWANIA WE/WY

Dostępne usługi wyszczególniono w tabeli poniżej:

Tabela 32

Jednostka funkcjonalna sterowania we/wy

Nazwa usługi	Wyszczególnienie
InputOutputControlByIdentifier	Klient żąda sterowania we/wy specyficznego dla serwera.

7.1. **Usługa InputOutputControlByIdentifier**

7.1.1 *Opis komunikatu*

Przez przednie gniazdo zestawione jest połączenie, które umożliwia sterowanie lub monitorowanie impulsów testowych przy pomocy odpowiedniego testera.

CPR_058 Tę linię sygnałową we/wy kalibracji można skonfigurować poleceniem K-line, posługując się usługą InputOutputControlByIdentifier w celu wybrania dla linii wymaganej funkcji wejścia lub wyjścia. Linia może przyjmować następujące stany:

— disabled (wyłączona);

— speedSignalInput, w którym linia sygnałowa we/wy kalibracji używana jest do wprowadzenia sygnału prędkości (sygnał testowy) zastępującego sygnał prędkości z czujnika ruchu; ta funkcja nie jest dostępna w trybie KONTROLNYM;

— realTimeSpeedSignalOutputSensor, w którym linia sygnałowa we/wy kalibracji używana jest do wyprowadzenia sygnału prędkości z czujnika ruchu;

— RTCOutput, w którym linia sygnałowa we/wy kalibracji używana jest do wyprowadzenia sygnału zegarowego UTC; ta funkcja nie jest dostępna w trybie KONTROLNYM.

CPR_059 Przyrząd rejestrujący musi być wprowadzony do sesji regulacji i być w trybie KALIBRACYJNYM lub KONTROLNYM w celu skonfigurowania stanu linii. Jeżeli VU jest w trybie KALIBRACYJNYM, można wybrać cztery stany linii (disabled, speedSignalInput, realTimeSpeedSignalOutputSensor, RTCOutput). Jeżeli VU jest w trybie KONTROLNYM, można wybrać tylko dwa stany linii (disabled, realTimeSpeedOutputSensor). Na zakończenie sesji regulacji lub trybu KALIBRACYJNEGO lub KONTROLNEGO przyrząd rejestrujący musi zapewnić, aby linia sygnałowa we/wy kalibracji powróciła do stanu „disabled" (wyłączona – stan domyślny).

CPR_060 Jeżeli impulsy prędkości odbierane są w czasie rzeczywistym z linii sygnału wejściowego prędkości w VU, natomiast linia sygnałowa we/wy kalibracji jest ustawiona na wejście, to linia sygnałowa we/wy kalibracji zostanie ustawiona na wyjście lub powróci do stanu „disabled" (wyłączona).

CPR_061 Kolejność czynności jest następująca:

— uruchomienie komunikacji usługą StartCommunication;

— otworzenie sesji regulacji usługą StartDiagnosticSession i wejście do trybu KALIBRACYJNEGO lub KONTROLNEGO (kolejność tych dwóch czynności nie ma znaczenia);

— zmiana stanu wyjścia usługą InputOutputControlByIdentifier.

7.1.2 *Format komunikatu*

CPR_062 Formaty komunikatu dla prymitywów InputOutputControlByIdentifier opisano szczegółowo w poniższych tabelach.

Tabela 33

Komunikat InputOutputControlByIdentifier Request

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	EE	TGT
#3	Bajt adresu źródłowego	tt	SRC
#4	Dodatkowy bajt długości	xx	LEN
#5	**InputOutputControlByIdentifier Request Sid**	**2F**	**IOCBI**
#6 i #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 lub	ControlOptionRecord = [		COR_…
#8 do #9	inputOutputControlParameter – jedna wartość z tabeli 36	xx	IOCP_…
	controlState – jedna wartość z tabeli 37 (zob. uwaga poniżej)]	xx	CS_…
#9 lub #10	Suma kontrolna	00-FF	CS

Uwaga: Parametr controlState występuje tylko w określonych przypadkach (zob. 7.1.3).

Tabela 34

Komunikat InputOutputControlByIdentifier Positive Response

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	xx	LEN
#5	**inputOutputControlByIdentifier Positive Response SId**	**6F**	**IOCBIPR**
#6 i #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 lub	controlStatusRecord = [		CSR_
#8 do #9	inputOutputControlParameter (ta sama wartość jak dla bajtu #8 w tabeli 33)	xx	IOCP_…
	controlState (ta sama wartość jak dla bajtu #9 w tabeli 33)] (jeżeli dotyczy)	xx	CS_…
#9 lub #10	Suma kontrolna	00-FF	CS

Tabela 35

Komunikat InputOutputControlByIdentifier Negative Response

# bajtu	Nazwa parametru	Wartość heksadecymalna	Mnemonik
#1	Bajt formatu – adresowanie fizyczne	80	FMT
#2	Bajt adresu docelowego	tt	TGT
#3	Bajt adresu źródłowego	EE	SRC
#4	Dodatkowy bajt długości	03	LEN
#5	**negativeResponse Service Id**	**7F**	**NR**
#6	inputOutputControlByIdentifier Request SId	2F	IOCBI
#7	responseCode=[		
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded]	7A	RC_DCLE
#8	Suma kontrolna	00-FF	CS

7.1.3 *Definicja parametru*

CPR_064 Parametr ***inputOutputControlParameter (IOCP_)*** zdefiniowano w poniższej tabeli.

Tabela 36

Definicja wartości inputOutputControlParameter

Heks	Wyszczególnienie	Mnemonik
00	**ReturnControlToECU** Wartość ta wskazuje serwerowi (VU), że tester już nie steruje linią sygnałową we/wy kalibracji.	RCTECU
01	**ResetToDefault** Wartość ta wskazuje serwerowi (VU), że wymagane jest przełączenie linii sygnałowej we/wy kalibracji do stanu domyślnego.	RTD
03	**ShortTermAdjustment** Wartość ta wskazuje serwerowi (VU), że wymagane jest przełączenie linii sygnałowej we/wy kalibracji do żądanej wartości w celu wyregulowania parametru controlState.	STA

CPR_065 Parametr ***controlState*** występuje jedynie wtedy, gdy parametr inputOutputControlParameter jest ustawiony na ShortTermAdjustment i przyjmuje wartości zdefiniowane w poniższej tabeli.

Tabela 37

Definicja wartości controlState

Tryb	Wartość heksadecymalna	Wyszczególnienie
wyłączony	00	linia we/wy wyłączona (stan domyślny)
włączony	01	włącz linię sygnałową we/wy kalibracji jako speedSignalInput
włączony	02	włącz linię sygnałową we/wy kalibracji jako realTimeSpeedSignalOutputSensor
włączony	03	włącz linię sygnałową we/wy kalibracji jako RTCOutput

8. FORMATY DATARECORDS

W tej sekcji opisano szczegółowo:

— ogólne zasady odnoszące się do szeregu parametrów wysyłanych przez przyrząd rejestrujący do testera;

— formaty, które należy stosować dla danych przesyłanych poprzez usługi przesyłania danych opisane w sekcji 6.

CPR_067 VU obsługuje wszystkie wyszczególnione parametry.

CPR_068 Dane wysyłane przez przyrząd rejestrujący do testera w odpowiedzi na komunikat żądania są typu pomiarowego (tj. bieżąca wartość żądanego parametru pomierzona lub stwierdzona przez VU).

8.1. **Zakresy przesyłanych parametrów**

CPR_069 W tabeli 38 podano wartości zakresów używane do sprawdzania poprawności przesłanego parametru.

CPR_070 Wartości w zakresie „wskaźnik błędu" umożliwiają przyrządowi rejestrującemu niezwłoczne wskazanie, że poprawne dane parametryczne nie są dostępne w bieżącym czasie wskutek pewnego typu błędu w tachografie.

CPR_071 Wartości w zakresie „niedostępne" umożliwiają przyrządowi rejestrującemu wysłanie komunikatu zawierającego parametr, który nie jest dostępny bądź nie jest obsługiwany w tym module. Wartości w zakresie „nieżądane" umożliwiają urządzeniu wysłanie komunikatu polecenia i wskazanie tych parametrów, w przypadku gdy od urządzenia odbierającego oczekiwany jest brak odpowiedzi.

CPR_072 Jeżeli usterka elementu składowego uniemożliwia wysłanie prawidłowych danych dla parametru, zamiast danych parametru używa się wskaźnika błędu opisanego w tabeli 38. Jednak jeżeli dane pomierzone lub obliczone dają wartość, która jest poprawna, ale wychodzi poza zdefiniowany zakres parametru, nie należy używać wskaźnika błędu. Dane przesyłane są przy użyciu odpowiednio wartości minimalnej lub maksymalnej parametru.

Tabela 38

Zakresy dataRecords

Nazwa zakresu	1 bajt (wartość heksadecymalna)	2 bajty (wartość heksadecymalna)	4 bajty (wartość heksadecymalna)	ASCII
Prawidłowy sygnał	00 do FA	0000 do FAFF	00000000 do FAFFFFFF	1 do 254
Szczególny wskaźnik parametru	FB	FB00 do FBFF	FB000000 do FBFFFFFF	brak
Zastrzeżony zakres do wykorzystania w przyszłości	FC do FD	FC00 do FDFF	FC000000 do FDFFFFFF	brak
Wskaźnik błędu	FE	FE00 do FEFF	FE000000 do FEFFFFFF	0
Niedostępne lub nieżądane	FF	FF00 do FFFF	FF000000 do FFFFFFFF	FF

CPR_073 Dla parametrów kodowanych w ASCII znak ASCII „*" jest zastrzeżony jako ogranicznik.

8.2. **Formaty dataRecords**

W tabelach od 39 do 42 poniżej opisano szczegółowo formaty używane przez usługi ReadDataByIdentifier i WriteDataByIdentifier.

CPR_074 W tabeli 39 podano długość, rozdzielczość i zakres roboczy dla każdego parametru identyfikowanego przez recordDataIdentifier:

Tabela 39

Format dataRecords

Nazwa parametru	Długość danych (w bajtach)	Rozdzielczość	Zakres roboczy
TimeDate	8	Zob. szczegółowy opis w tabeli 40	
HighResolutionTotalVehicleDistance	4	wzmocnienie 5 m/bit, offset 0 m	0 do +21 055 406 km
Kfactor	2	wzmocnienie 0,001 impulsu/m/bit, offset 0	0 do 64,255 impulsu/m
LfactorTyreCircumference	2	wzmocnienie $0{,}125\ 10^{-3}$ m/bit, offset 0	0 do 8,031 m
WvehicleCharacteristicFactor	2	wzmocnienie 0,001 impulsu/m/bit, offset 0	0 do 64,255 impulsu/m
TyreSize	15	ASCII	ASCII

Nazwa parametru	Długość danych (w bajtach)	Rozdzielczość	Zakres roboczy
NextCalibrationDate	3	Zob. szczegółowy opis w tabeli 41	
SpeedAuthorised	2	wzmocnienie 1/256 km/h/bit, offset 0	0 do 250,996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Zob. szczegółowy opis w tabeli 42	
VIN	17	ASCII	ASCII

CPR_075 W tabeli 40 zamieszczono szczegółowy opis formatów poszczególnych bajtów parametru TimeDate:

Tabela 40

Szczegółowy opis formatu TimeDate (wartość recordDataIdentifier # F90B)

Bajt	Definicja parametru	Rozdzielczość	Zakres roboczy
1	Sekundy	wzmocnienie 0,25 s/bit, offset 0 s	0 do 59,75s
2	Minuty	wzmocnienie 1 minuta/bit, offset 0 minut	0 do 59 minut
3	Godziny	wzmocnienie 1 h/bit, offset 0 h	0 do 23 h
4	Miesiąc	wzmocnienie 1 miesiąc/bit, offset 0 miesięcy	1 do 12 miesięcy
5	Dzień	wzmocnienie 0,25 dzień/bit, offset 0 dni (zob. UWAGA pod tabelą 41)	0,25 do 31,75 dnia
6	Rok	wzmocnienie 1 rok/bit, offset rok + 1985 (zob. UWAGA pod tabelą 41)	lata od 1985 do 2235
7	lokalne przesunięcie dla minut	wzmocnienie 1 minuta/bit, offset – 125 minut	– 59 do + 59 minut
8	lokalne przesunięcie dla godzin	wzmocnienie 1 h/bit, offset – 125 h	– 23 do + 23 h

CPR_076 W tabeli 41 zamieszczono szczegółowy opis formatów poszczególnych bajtów parametru NextCalibrationDate.

Tabela 41

Szczegółowy opis formatu NextCalibrationDate (wartość recordDataIdentifier # F922)

Bajt	Definicja parametru	Rozdzielczość	Zakres roboczy
1	Miesiąc	wzmocnienie 1 miesiąc/bit, offset 0 miesięcy	1 do 12 miesięcy
2	Dzień	0,25 dnia/bit, offset 0 dni (zob. UWAGA poniżej)	0,25 do 31,75 dnia
3	Rok	wzmocnienie 1 rok/bit, offset rok + 1985 (zob. UWAGA poniżej)	lata od 1985 do 2235

UWAGA dotycząca zastosowania parametru „dzień”:

1) Wartość 0 dla daty nie istnieje. Wartości 1, 2, 3 i 4 są stosowane do oznaczenia pierwszego dnia miesiąca; 5, 6, 7 i 8 – do oznaczenia drugiego dnia miesiąca, itd.

2) Ten parametr nie ma wpływu na parametr „godzina” ani go nie zmienia.

UWAGA dotycząca zastosowania parametru „rok”:

Wartość 0 dla roku oznacza rok 1985, wartość 1 oznacza rok 1986, itd.

CPR_078 W tabeli 42 zamieszczono szczegółowy opis formatów poszczególnych bajtów parametru VehicleRegistrationNumber.

Tabela 42

Szczegółowy opis formatu VehicleRegistrationNumber (wartość recordDataIdentifier # F97E)

Bajt	Definicja parametru	Rozdzielczość	Zakres roboczy
1	Strona kodowa (zdefiniowana w dodatku 1)	ASCII	01 do 0A
2 – 14	Numer rejestracyjny pojazdu (zdefiniowany w dodatku 1)	ASCII	ASCII

Dodatek 9

HOMOLOGACJA TYPU WYKAZ MINIMUM WYMAGANYCH BADAŃ

SPIS TREŚCI

1. WPROWADZENIE

1.1. **Homologacja typu**

Homologacja typu WE urządzenia rejestrującego (lub elementu składowego) lub karty do tachografu opiera się na następujących dokumentach:

— **świadectwie bezpieczeństwa**, opartym na specyfikacjach normy „Common Criteria", w odniesieniu do celu bezpieczeństwa w pełni zgodnego z celami przedstawionymi w dodatku 10 do niniejszego załącznika (do uzupełnienia/zmiany),

— **świadectwie funkcjonalności** wystawionym przez organ państwa członkowskiego i zaświadczającym, że badany element spełnia wymogi określone w niniejszym załączniku pod względem wykonywanych funkcji, dokładności pomiarów i charakterystyki środowiskowej,

— **świadectwie interoperacyjności** wystawionym przez właściwy organ i zaświadczającym, że urządzenie rejestrujące (lub karta do tachografu) jest w pełni interoperacyjne z wymaganymi typami kart do tachografu (lub urządzenia rejestrującego) (zob. rozdział 8 niniejszego załącznika).

W niniejszym dodatku określa się, które badania, jako minimum, musi przeprowadzić organ państwa członkowskiego w ramach badań funkcjonalności, i które badania, jako minimum, musi przeprowadzić właściwy organ w ramach badań interoperacyjności. Nie określa się dokładnie procedur przeprowadzania tych badań ani ich rodzajów.

Niniejszy dodatek nie obejmuje aspektów świadectwa bezpieczeństwa. Jeżeli niektóre badania wymagane na potrzeby homologacji typu przeprowadza się przy ocenie bezpieczeństwa i w ramach procesu certyfikacji, to nie trzeba ich przeprowadzać ponownie. W takim przypadku można poddać kontroli tylko wyniki takich badań bezpieczeństwa. Do celów informacyjnych wymogi, które mają zostać poddane badaniom (lub ściśle wiążą się z badaniami, które mają zostać przeprowadzone) w ramach certyfikacji bezpieczeństwa, są w niniejszym dodatku oznaczone symbolem „*".

Ponumerowane wymogi odnoszą się do tekstu głównego załącznika, natomiast pozostałe wymogi odnoszą się do innych dodatków (np. PIC_001 odnosi się do wymogu PIC_001 zawartego w dodatku 3 Piktogramy).

W niniejszym dodatku oddzielnie przedstawiono informacje na temat homologacji typu czujnika ruchu, przyrządu rejestrującego oraz urządzenia zewnętrznego GNSS jako elementów składowych urządzenia rejestrującego. Każdy element składowy uzyska oddzielne świadectwo homologacji typu, w którym wskazane zostaną pozostałe kompatybilne elementy składowe. Badanie funkcjonalności czujnika ruchu (lub urządzenia zewnętrznego GNSS) wykonuje się wraz z badaniem funkcjonalności przyrządu rejestrującego i odwrotnie.

Nie wymaga się zapewnienia interoperacyjności między każdym modelem czujnika ruchu (lub urządzenia zewnętrznego GNSS) i każdym modelem przyrządu rejestrującego. W takim przypadku homologacja typu czujnika ruchu (lub odpowiednio urządzenia zewnętrznego GNSS) może być wydana tylko w połączeniu z homologacją typu właściwego przyrządu rejestrującego i odwrotnie.

1.2. **Odniesienia**

W niniejszym dodatku używa się następujących odniesień:

IEC 60068-2-1: Badania środowiskowe – Część 2-1: Próby – Próba A: Zimno

IEC 60068-2-2: Podstawowe procedury badań środowiskowych – Część 2: Próby – Próba B: Suche gorąco (harmoniczne).

IEC 60068-2-6: Badania środowiskowe – Część 2: Próby – Próba Fc: Wibracje

IEC 60068-2-14: Badania środowiskowe – Część 2-14: Próby – Próba N: Zmiany temperatury

IEC 60068-2-27: Badania środowiskowe – Część 2: Próby – Próba Ea i wytyczne: Udary

IEC 60068-2-30: Badania środowiskowe – Część 2-30: Próby – Próba Db: Wilgotne gorąco, cykliczne (cykl 12 +12 h)

IEC 60068-2-64: Badania środowiskowe – Część 2-64: Próby – Próba Fh: Wibracje szerokopasmowe losowe i wytyczne

IEC 60068-2-78: Badania środowiskowe – Część 2-78: Próby – Próba Cab: Wilgotne gorąco stałe

ISO 16750-3 – Obciążenia mechaniczne (2012-12)

ISO 16750-4 – Obciążenia klimatyczne (2010-04)

ISO 20653: Pojazdy drogowe – Stopień ochrony (kod IP) – Ochrona urządzeń elektrycznych przed ciałami obcymi, wodą i dostępem

ISO 10605:2008 + Sprostowanie techniczne:2010 + AMD1:2014 Pojazdy drogowe – Metody badań zakłóceń elektrycznych powodowanych przez wyładowania elektrostatyczne

ISO 7637-1:2002 + AMD1:2008 Pojazdy drogowe – Zakłócenia elektryczne przenoszone przez przewodzenie i przez sprzężenie – Część 1: Definicje i postanowienia ogólne

ISO 7637-2 Pojazdy drogowe – Zakłócenia elektryczne przenoszone przez przewodzenie i przez sprzężenie – Część 2: Przewodzenie przebiegów przejściowych wyłącznie wzdłuż przewodów zasilających

ISO 7637-3 Pojazdy drogowe – Zakłócenia elektryczne przenoszone przez przewodzenie i przez sprzężenie – Część 3: Przenoszenie elektrycznych przebiegów przejściowych przez sprzężenia pojemnościowe i indukcyjne przez linie inne niż linie zasilające

ISO/IEC 7816-1 Karty identyfikacyjne – Karty elektroniczne – Część 1: Karty stykowe – Charakterystyki fizyczne

ISO/IEC 7816-2 Technologia informacyjna – Karty identyfikacyjne – Karty elektroniczne – Część 2: Karty stykowe – Wymiary i rozmieszczenie styków

ISO/IEC 7816-3 Technologia informacyjna – Karty identyfikacyjne – Karty elektroniczne – Część 3: Karty Stykowe – Sygnały elektryczne i protokoły transmisji

ISO/IEC 10373-1:2006 + AMD1:2012 Karty identyfikacyjne – Metody badań – Część 1: Charakterystyki ogólne

ISO/IEC 10373-3:2010 + Sprostowanie techniczne: 2013 Karty identyfikacyjne – Metody badań – Część 3: Karty elektroniczne i powiązane z nimi urządzenia interfejsowe

ISO 16844-3:2004, Sprostowanie 1: 2006 Pojazdy drogowe – Systemy tachograficzne – Część 3: Interfejs czujnika ruchu (z przyrządami rejestrującymi)

ISO 16844-4 Pojazdy drogowe – Systemy tachograficzne – Część 4: Interfejs CAN

ISO 16844-6 Pojazdy drogowe – Systemy tachograficzne – Część 6: Diagnostyka

ISO 16844-7 Pojazdy drogowe – Systemy tachograficzne – Część 7: Parametry

ISO 534 Papier i tektura – Oznaczanie grubości, gęstości pozornej i objętości właściwej

EKG ONZ R10 Jednolite przepisy dotyczące homologacji pojazdów w odniesieniu do kompatybilności elektromagnetycznej (Europejska Komisja Gospodarcza ONZ)

2. BADANIA FUNKCJONALNOŚCI PRZYRZĄDU REJESTRUJĄCEGO

Nr	Badanie	Opis	Powiązane wymogi
1	**Badanie administracyjne**		
1.1	Dokumentacja	Prawidłowość dokumentacji	
1.2	Wyniki badań producenta	Wyniki badań producenta przeprowadzonych podczas integracji. Przedstawienie dokumentów papierowych.	88, 89, 91
2	**Kontrola wizualna**		
2.1	Zgodność z dokumentacją		
2.2	Identyfikacja/oznakowanie		224–226
2.3	Materiały		219–223
2.4	Plombowanie		398, 401–405
2.5	Interfejsy zewnętrzne		
3	**Badania funkcjonalności**		
3.1	Obsługiwane funkcje		03, 04, 05, 07, 382,
3.2	Tryby pracy		09–11*, 132, 133
3.3	Prawa dostępu do funkcji i danych		12* 13*,, 382, 383, 386–389
3.4	Monitorowanie wkładania i wyjmowania kart		15, 16, 17, 18, 19*, 20*, 132
3.5	Pomiar prędkości i odległości		21–31
3.6	Pomiar czasu (badanie przeprowadzone w temperaturze 20 °C)		38–43
3.7	Monitorowanie czynności kierowcy		44–53, 132
3.8	Monitorowanie stanu prowadzenia pojazdu		54, 55, 132

Nr	Badanie	Opis	Powiązane wymogi
3.9	Pozycje wprowadzane ręcznie		56–62
3.10	Zarządzanie blokadami firmowymi		63–68
3.11	Monitorowanie czynności kontrolnych		69, 70
3.12	Wykrywanie zdarzeń lub usterek		71 – 88 132
3.13	Dane identyfikujące urządzenie		93*, 94*, 97, 100
3.14	Dane dotyczące wkładania i wyjmowania karty kierowcy		102*–104*
3.15	Dane dotyczące czynności kierowcy		105*–107*
3.16	Dane dotyczące miejsc i położenia		108*–112*
3.17	Dane dotyczące licznika kilometrów		113*–115*
3.18	Szczegółowe dane dotyczące prędkości		116*
3.19	Dane dotyczące zdarzeń		117*
3.20	Dane dotyczące usterek		118*
3.21	Dane dotyczące kalibracji		119*–121*
3.22	Dane dotyczące korekty czasu		124*, 125*
3.23	Dane dotyczące czynności kontrolnej		126*, 127*
3.24	Dane dotyczące blokad firmowych		128*
3.25	Dane dotyczące czynności pobierania		129*
3.26	Dane dotyczące warunków szczególnych		130*, 131*
3.27	Rejestrowanie i przechowywanie danych na kartach do tachografu		134, 135,, 136*, 137*, 139*, 140, 141 142, 143, 144*, 145*, 146*, 147, 148
3.28	Wyświetlanie		90, 132, 149–166, PIC_001, DIS_001
3.29	Drukowanie		90, 132, 167–179, PIC_001, PRT_001–PRT_014
3.30	Ostrzeganie		132, 180–189, PIC_001

Nr	Badanie	Opis	Powiązane wymogi
3.31	Pobieranie danych na nośnik zewnętrzny		90, 132, 190–194
3.32	Łączność na odległość na potrzeby ukierunkowanych kontroli drogowych		195–197
3.33	Wyprowadzanie danych do dodatkowych urządzeń zewnętrznych		198, 199
3.34	Kalibracja		202–206*, 383, 384, 386–391
3.35	Drogowe kontrole kalibracji		207–209
3.36	Korekta czasu		210–212*
3.37	Niezakłócanie funkcji dodatkowych		06, 425
3.38	Interfejs czujnika ruchu		02, 122
3.39	Urządzenie zewnętrzne GNSS		03, 123
3.40	Sprawdzenie, czy VU wykrywa, rejestruje i zapisuje zdarzenie (zdarzenia) lub usterkę (usterki) określone przez producenta VU, gdy sparowany czujnik ruchu reaguje na pola magnetyczne zaburzające wykrywanie ruchu pojazdu.		217
3.41	Pakiet szyfrów i standardowe parametry domeny		CSM_48, CSM_50
4	**Badania środowiskowe**		
4.1	Temperatura	Sprawdzenie funkcjonalności za pomocą: badania zgodnie z normą ISO 16750-4, Rozdział 5.1.1.2: Próba eksploatacyjna w niskiej temperaturze (72 h w temperaturze – 20 °C). Badanie to odnosi się do normy IEC 60068-2-1: Badania środowiskowe – Część 2-1: Próby – Próba A: Zimno; badania zgodnie z normą ISO 16750-4, Rozdział 5.1.2.2: Próba eksploatacyjna w wysokiej temperaturze (72 h w temperaturze 70 °C). Badanie to odnosi się do normy IEC 60068-2-2: Podstawowe procedury badań środowiskowych – Część 2: Próby – Próba B: Suche gorąco; badania zgodnie z normą ISO 16750-4: Rozdział 5.3.2: Nagła zmiana temperatury z określonym okresem przejściowym (– 20 °C/70 °C, 20 cykli, czas przebywania: 2 h w każdej temperaturze). Można przeprowadzić skrócony zestaw badań (spośród tych zdefiniowanych w sekcji 3 niniejszej tabeli) w niższej temperaturze, wyższej temperaturze i w czasie cykli temperaturowych.	213

Nr	Badanie	Opis	Powiązane wymogi
4.2	Wilgotność	Sprawdzenie odporności przyrządu rejestrującego na cykliczne zmiany wilgotności (próba gorąca) za pomocą próby Db wg normy IEC 60068-2-30, w sześciu 24-godzinnych cyklach, w każdym ze zmieniającą się temperaturą od + 25 °C do + 55 °C i wilgotnością względną 97 % w + 25 °C i 93 % w + 55 °C	214
4.3	Mechanika	1. Drgania harmoniczne: sprawdzenie odporności przyrządu rejestrującego na drgania harmoniczne o następujących właściwościach: stałe przemieszczenie przy częstotliwości 5–11 Hz: 10-milimetrowa amplituda; stałe przyspieszenie przy częstotliwości 11–300 Hz: 5g. Wymóg ten sprawdza się za pomocą próby Fc wg normy IEC 60068-2-6, z minimalnym czasem trwania próby 3 × 12 h (12 h na oś). ISO 16750-3 nie wymaga przeprowadzenia badania drgań harmonicznych w przypadku urządzeń znajdujących się w oddzielnej kabinie pojazdu. 2. Drgania swobodne: Próba zgodnie z ISO 16750-3: Rozdział 4.1.2.8: Próba VIII: Pojazd użytkowy, oddzielna kabina pojazdu. Próba drgań swobodnych: 10 … 2 000 Hz, wertykalna średnia kwadratowa 21,3 m/s^2, wzdłużna średnia kwadratowa 11,8 m/s^2, poprzeczna średnia kwadratowa 13,1 m/s^2, 3 osie, 32 h na oś, w tym cykl temperaturowy – 20…70 °C. Badanie to odnosi się do normy IEC 60068-2-64: Badania środowiskowe – Część 2-64: Próby – Próba Fh: Wibracje szerokopasmowe losowe i wytyczne. 3. Udary: udar mechaniczny przy impulsie półsinusoidalnym 3 g wg normy ISO 16750. Opisane powyżej badania przeprowadza się na różnych próbkach urządzeń poddawanych badaniom.	219
4.4	Ochrona przed wodą i ciałami obcymi	Badanie zgodnie z normą ISO 20653: Pojazdy drogowe – Stopień ochrony (kod IP) – Ochrona urządzeń elektrycznych przed ciałami obcymi, wodą i dostępem (bez zmian parametrów); minimalna wartość IP – 40	220, 221
4.5	Zabezpieczenie nadnapięciowe	Sprawdzenie odporności przyrządu rejestrującego na napięcie zasilania: wersje 24 V: 34 V przy + 40 °C przez 1 godzinę wersje 12 V: 17 V przy + 40 °C przez 1 godzinę (ISO 16750-2)	216
4.6	Zabezpieczenie przed odwróceniem polaryzacji	Sprawdzenie odporności przyrządu rejestrującego na odwrócenie biegunów napięcia zasilającego. (ISO 16750-2)	216

Nr	Badanie	Opis	Powiązane wymogi
4.7	Zabezpieczenie zwarciowe	Sprawdzenie, czy sygnały wyjściowe są zabezpieczone przed zwarciem do napięcia zasilającego i do masy. (ISO 16750-2)	216
5	**Badania EMC**		
5.1	Emisje radiacyjne i wrażliwość na radiację	Zgodność z regulaminem nr 10 EKG ONZ	218
5.2	Wyładowania elektrostatyczne	Zgodność z normą ISO 10605:2008 + Sprostowanie techniczne:2010 + AMD1:2014: +/– 4 kV w przypadku styku i +/– 8 kV w przypadku rozładowania do powietrza	218
5.3	Wrażliwość na stany nieustalone w zasilaniu	W przypadku wersji 24 V: zgodność z normą ISO 7637-2 i wersją 3 regulaminu nr 10 EKG ONZ: impuls 1a: Vs = – 450 V, Ri = 50 omów impuls 2a: Vs = + 37 V, Ri = 2 omy impuls 2b: Vs = + 20 V, Ri = 0,05 oma impuls 3a: Vs = – 150 V, Ri = 50 omów impuls 3b: Vs = + 150 V, Ri = 50 omów impuls 4: Vs = – 16 V Va = – 12V, t6 = 100ms impuls 5: Vs = + 120 V, Ri = 2,2 oma, td = 250 ms W przypadku wersji 12 V: zgodność z normą ISO 7637-1 i wersją 3 regulaminu nr 10 EKG ONZ: impuls 1: Vs = – 75 V, Ri = 10 omów impuls 2a: Vs = + 37 V, Ri = 2 omy impuls 2b: Vs = + 10 V, Ri = 0,05 oma impuls 3a: Vs = – 112 V, Ri = 50 omów impuls 3b: Vs = + 75 V, Ri = 50 omów impuls 4: Vs = – 6 V, Va = – 5 V, t6 = 15 ms impuls 5: Vs = + 65 V, Ri = 3 omy, td = 100 ms Impuls 5 należy testować tylko w przypadku przyrządów rejestrujących przeznaczonych do zainstalowania w pojazdach, w których nie zainstalowano zewnętrznego, wspólnego zabezpieczenia przed spadkiem obciążenia. Aby uzyskać informacje na temat propozycji zabezpieczenia przed spadkiem obciążenia, zob. norma ISO 16750-2 wydanie 4. rozdział 4.6.4.	218

3. BADANIA FUNKCJONALNOŚCI CZUJNIKA RUCHU

Nr	Badanie	Opis	Powiązane wymogi
1.	**Badanie administracyjne**		
1.1	Dokumentacja	Prawidłowość dokumentacji	

Nr	Badanie	Opis	Powiązane wymogi
2.	**Kontrola wizualna**		
2.1	Zgodność z dokumentacją		
2.2	Identyfikacja/oznakowanie		225, 226,
2.3	Materiały		219–223
2.4	Plombowanie		398, 401–405
3.	**Badania funkcjonalności**		
3.1	Dane identyfikacyjne czujnika		95–97*
3.2	Parowanie czujnik ruchu — przyrząd rejestrujący		122*, 204
3.3	Wykrywanie ruchu Dokładność pomiaru ruchu		30–35
3.4	Interfejs przyrządu rejestrującego		02
3.5	Sprawdzenie, czy działanie stałego pola magnetycznego nie wpływa na czujnik ruchu. Ewentualnie sprawdzenie, czy czujnik ruchu reaguje na działanie stałych pól magnetycznych zaburzających wykrywanie ruchu pojazdu, tak aby podłączony VU mógł wykrywać, rejestrować i zapisywać usterki czujnika.		217
4.	**Badania środowiskowe**		
4.1	Temperatura pracy	Sprawdzenie funkcjonalności (zdefiniowanej w ramach badania nr 3.3) w zakresie temperatur [– 40 – + 135 °C] za pomocą: próby Ad wg normy IEC 60068-2-1, z czasem trwania badania 96 h w najniższej temperaturze To_{min}, próby Bd wg normy IEC 60068-2-2, z czasem trwania badania 96 h w najwyższej temperaturze To_{max}, badania zgodnie z normą ISO 16750-4: Rozdział 5.1.1.2: Próba eksploatacyjna w niskiej temperaturze (24 h w temperaturze – 40 °C). Badanie to odnosi się do normy IEC 60068-2-1: Badania środowiskowe – Część 2-1: Próby – Próba A: Zimno, wg próby Bd w ramach normy IEC 68-2-2, z czasem trwania 96 h w najniższej temperaturze – 40 °C badania zgodnie z normą ISO 16750-4: Rozdział 5.1.2.2: Próba eksploatacyjna w niskiej temperaturze (96 h w temperaturze 135 °C). Badanie to odnosi się do normy IEC 60068-2-2: Podstawowe procedury badań środowiskowych – Część 2: Próby – Próba B: Suche gorąco;	213

Nr	Badanie	Opis	Powiązane wymogi
4.2	Cykle temperaturowe	Badanie zgodnie z normą ISO 16750-4: Rozdział 5.3.2: Nagła zmiana temperatury z określonym okresem przejściowym (– 40 °C/135 °C, 20 cykli, czas przebywania: 30 min w każdej temperaturze). IEC 60068-2-14: Badania środowiskowe – Część 2-14: Próby – Próba N: Zmiany temperatury	213
4.3	Cykle wilgotności	Sprawdzenie funkcjonalności (zdefiniowanej w ramach badania nr 3.3) za pomocą próby Db wg normy IEC 60068-2-30, w sześciu 24-godzinnych cyklach, w każdym ze zmieniającą się temperaturą od + 25 °C do + 55 °C i wilgotnością względną 97 % w + 25 °C i 93 % w + 55 °C	214
4.4	Drgania	ISO 16750-3: Rozdział 4.1.2.6: Próba IV: Pojazd użytkowy, silnik, skrzynia biegów Badanie drgań w trybie mieszanym obejmujące: a) badanie drgań harmonicznych, 20…520 Hz, 11,4 … 120 m/s², <= 0,5 oct/min b) badanie drgań swobodnych, 10 … 2 000 Hz, średnia kwadratowa 177 m/s², 94 h na oś, z cyklem temperaturowym -20…70 °C). Badanie to odnosi się do normy IEC 60068-2-80: Badania środowiskowe – Część 2-80: Próby – Próba Fi: Wibracje – tryb mieszany	219
4.5	Udar mechaniczny	ISO 16750-3: Rozdział 4.2.3: Próba IV: Próba dla urządzeń znajdujących się w skrzyni biegów lub na skrzyni biegów Udar o impulsie półsinusoidalnym, przyspieszenie do uzgodnienia w zakresie 3 000 … 15 000 m/s², czas trwania impulsu do uzgodnienia, ale < 1 ms, liczba wstrząsów: do uzgodnienia. Badanie to odnosi się do normy IEC 60068-2-27: Badania środowiskowe – Część 2: Próby – Próba Ea i wytyczne: Udary	219
4.6	Ochrona przed wodą i ciałami obcymi	Badanie zgodnie z normą ISO 20653: Pojazdy drogowe – Stopień ochrony (kod IP) – Ochrona urządzeń elektrycznych przed ciałami obcymi, wodą i dostępem (docelowa wartość IP – 64)	220, 221
4.7	Zabezpieczenie przed odwróceniem polaryzacji	Sprawdzenie odporności czujnika ruchu na odwrócenie biegunów napięcia zasilającego.	216
4.8	Zabezpieczenie zwarciowe	Sprawdzenie, czy sygnały wyjściowe są zabezpieczone przed zwarciem do napięcia zasilającego i do masy.	216

Nr	Badanie	Opis	Powiązane wymogi
5.	**Badania kompatybilności elektromagnetycznej**		
5.1	Emisje radiacyjne i wrażliwość na radiację	Sprawdzenie zgodności z regulaminem nr 10 EKG ONZ	218
5.2	Wyładowania elektrostatyczne	Zgodność z normą ISO 10605:2008 + Sprostowanie techniczne:2010 + AMD1:2014: +/– 4kV w przypadku styku i +/– 8kV w przypadku rozładowania do powietrza	218
5.3	Wrażliwość na stany nieustalone na liniach danych	W przypadku wersji 24 V: zgodność z normą ISO 7637-2 i wersją 3 regulaminu nr 10 EKG ONZ: impuls 1a: Vs = – 450 V, Ri = 50 omów impuls 2a: Vs = + 37 V, Ri = 2 omy impuls 2b: Vs = + 20 V, Ri = 0,05 oma impuls 3a: Vs = – 150 V, Ri = 50 omów impuls 3b: Vs = + 150 V, Ri = 50 omów impuls 4: Vs = – 16 V Va = – 12V, t6 = 100ms impuls 5: Vs = + 120 V, Ri = 2,2 oma, td = 250 ms W przypadku wersji 12 V: zgodność z normą ISO 7637-1 i wersją 3 regulaminu nr 10 EKG ONZ: impuls 1: Vs = – 75 V, Ri = 10 omów impuls 2a: Vs = + 37 V, Ri = 2 omy impuls 2b: Vs = + 10 V, Ri = 0,05 oma impuls 3a: Vs = – 112 V, Ri = 50 omów impuls 3b: Vs = + 75 V, Ri = 50 omów impuls 4: Vs = – 6 V, Va = – 5 V, t6 = 15 ms impuls 5: Vs = + 65 V, Ri = 3 omy, td = 100 ms Impuls 5 należy testować tylko w przypadku przyrządów rejestrujących przeznaczonych do zainstalowania w pojazdach, w których nie zainstalowano zewnętrznego, wspólnego zabezpieczenia przed spadkiem obciążenia. Aby uzyskać informacje na temat propozycji zabezpieczenia przed spadkiem obciążenia, zob. norma ISO 16750-2 wydanie 4. rozdział 4.6.4.	218

4. BADANIA FUNKCJONALNOŚCI KART DO TACHOGRAFU

Badania zgodnie z niniejszą sekcją 4

nr 5 „Testy protokołów”,

nr 6 „Struktura karty” i

nr 7 „Badania funkcjonalności”

może przeprowadzić jednostka dokonująca oceny lub jednostka certyfikująca w trakcie procesu wydawania świadectwa bezpieczeństwa dla modułu chipowego zgodnie z normą „Common Criteria” (CC).

Badania nr 2.3 i 4.2 są identyczne. Są to próby mechaniczne kombinacji karty i modułu chipowego. Jeżeli jeden z tych elementów (karta, moduł chipowy) zostanie zmieniony, wówczas przeprowadzenie tych badań jest konieczne.

Nr	Badanie	Opis	Powiązane wymogi
1.	**Badanie administracyjne**		
1.1	Dokumentacja	Prawidłowość dokumentacji	
2	**Karta**		
2.1	Nadruk	Sprawdzenie, czy wszystkie zabezpieczenia i widoczne dane są prawidłowo nadrukowane i zgodne z wymogami. [Oznaczenie] (Załącznik 1C rozdział 4.1 „Dane widzialne”, 227) Na awersie znajdują się: wyrażenia „Karta kierowcy”, „Karta kontrolna”, „Karta warsztatowa”, lub „Karta firmowa” nadrukowane wielkimi literami w języku urzędowym lub językach urzędowych państwa członkowskiego wydającego kartę, zgodnie z typem karty. [Nazwa państwa członkowskiego] (Załącznik 1C rozdział 4.1 „Dane widzialne”, 228) Na awersie znajdują się: nazwa państwa członkowskiego wydającego kartę (nieobowiązkowo). [Znak] (Załącznik 1C rozdział 4.1 „Dane widzialne”, 229) Na awersie znajdują się: wyróżniający znak państwa członkowskiego wydającego kartę, drukowany w negatywie w niebieskim prostokącie i otoczony 12 żółtymi gwiazdkami. [Oznaczenie liczby] (Załącznik 1C rozdział 4.1 „Dane widzialne”, 232) Na awersie znajdują się: objaśnienia numerowanych pozycji znajdujących się na awersie karty. [Kolor] (Załącznik 1C rozdział 4.1 „Dane widzialne”, 234) Karty do tachografu drukuje się w następujących dominujących kolorach tła: — karta kierowcy: biały, — karta warsztatowa: czerwony, — karta kontrolna: niebieski, — karta firmowa: żółty.	227–229, 232, 234–236

Nr	Badanie	Opis	Powiązane wymogi
		[Zabezpieczenie] (Załącznik 1C rozdział 4.1 „Dane widzialne", 235) Karty do tachografu mają przynajmniej następujące zabezpieczenia przed fałszowaniem i manipulowaniem: — zabezpieczający wzór tła z drukowanym drobnym giloszem i tęczą, — przynajmniej dwubarwną linię wykonaną techniką mikrodruku.	
		[Oznakowania] (Załącznik 1C rozdział 4.1 „Dane widzialne", 236) Państwa członkowskie mogą dodawać kolory lub oznakowania, takie jak symbole państwowe i zabezpieczenia.	
		[Znak homologacji] Karta do tachografu jest opatrzona znakiem homologacji. Znak homologacji składa się z: — prostokąta, wewnątrz którego jest umieszczona litera „e", po której następuje liczba lub litera oznaczająca państwo, które wydało homologację, — numeru homologacji typu odpowiadającego numerowi świadectwa homologacji typu karty do tachografu, umieszczonego bezpośrednio obok wspomnianego wyżej prostokąta.	
2.2	Próby mechaniczne	[Wielkość karty] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7810: Karty identyfikacyjne – Charakterystyki fizyczne, [5] Wymiary karty [5.1] Wielkość karty [5.1.1] Wymiary i tolerancje karty Typ karty ID-1 Karta nieużywana	240, 243 ISO/IEC 7810
		[Krawędzie karty] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7810: Karty identyfikacyjne – Charakterystyki fizyczne, [5] Wymiary karty [5.1] Wielkość karty [5.1.2] Krawędzie karty	

Nr	Badanie	Opis	Powiązane wymogi
		[Struktura karty] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7810: Karty identyfikacyjne – Charakterystyki fizyczne, [6] Struktura karty	
		[Materiały, z których wykonane są karty] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7810: Karty identyfikacyjne – Charakterystyki fizyczne, [7] Materiały, z których wykonane są karty	
		[Odporność na zginanie] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7810: Karty identyfikacyjne – Charakterystyki fizyczne, [8] Charakterystyki kart [8.1] Odporność na zginanie	
		[Toksyczność] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7810: Karty identyfikacyjne – Charakterystyki fizyczne, [8] Charakterystyki kart [8.3] Toksyczność	
		[Odporność na działanie czynników chemicznych] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7810: Karty identyfikacyjne – Charakterystyki fizyczne, [8] Charakterystyki kart [8.4] Odporność na działanie czynników chemicznych	
		[Stabilność kart] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7810: Karty identyfikacyjne – Charakterystyki fizyczne, [8] Charakterystyki kart [8.5] Stabilność wymiarowa kart i odkształcenie wywołane przez temperaturę i wilgotność	

Nr	Badanie	Opis	Powiązane wymogi
		[Światło] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7810: Karty identyfikacyjne – Charakterystyki fizyczne, [8] Charakterystyki kart [8.6.] Światło	
		[Trwałość] Załącznik 1C rozdział 4.4 „Wymagania środowiskowe i elektryczne”, 241) Karty do tachografu prawidłowo pracują przez okres pięciu lat, jeżeli są używane w określonych warunkach środowiskowych i elektrycznych.	
		[Wytrzymałość na rozwarstwienie] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7810: Karty identyfikacyjne – Charakterystyki fizyczne, [8] Charakterystyki kart [8.8] Wytrzymałość na rozwarstwienie	
		[Przyczepność lub blokowanie] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7810: Karty identyfikacyjne – Charakterystyki fizyczne, [8] Charakterystyki kart [8.9] Przyczepność lub blokowanie	
		[Odkształcenie] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7810: Karty identyfikacyjne – Charakterystyki fizyczne, [8] Charakterystyki kart [8.11] Ogólne odkształcenie kart	
		[Odporność na działanie wysokich temperatur] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7810: Karty identyfikacyjne – Charakterystyki fizyczne, [8] Charakterystyki kart [8.12] Odporność na działanie wysokich temperatur	

Nr	Badanie	Opis	Powiązane wymogi
		[Zniekształcenia powierzchni] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7810: Karty identyfikacyjne – Charakterystyki fizyczne, [8] Charakterystyki kart [8.13] Zniekształcenia powierzchni	
		[Zanieczyszczenie] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7810: Karty identyfikacyjne – Charakterystyki fizyczne, [8] Charakterystyki kart [8.14] Zanieczyszczenie i interakcje komponentów kart	
2.3	Próby mechaniczne z wbudowanym modułem chipowym	[Zginanie] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7810:2003/zmiana 1:2009, Karty identyfikacyjne – Charakterystyki fizyczne, zmiana 1: Kryteria dotyczące kart elektronicznych [9.2] Dynamiczne naprężenie zginające Łączna liczba cykli zginania: 4 000.	ISO/IEC 7810
		[Skręcanie] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7810:2003/zmiana 1:2009, Karty identyfikacyjne – Charakterystyki fizyczne, zmiana 1: Kryteria dotyczące kart elektronicznych [9.3] Dynamiczne naprężenie skręcające Łączna liczba cykli skręcania: 4 000.	
3	**Moduł**		
3.1	Moduł	Moduł to obudowa chipu i płyta stykowa. [Profil powierzchni] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7816-1:2011, Karty identyfikacyjne – Karty elektroniczne – Część 1: Karty stykowe – Charakterystyki fizyczne [4.2] Profil powierzchni styków	ISO/IEC 7816

Nr	Badanie	Opis	Powiązane wymogi
		[Wytrzymałość mechaniczna] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7816-1:2011, Karty identyfikacyjne – Karty elektroniczne – Część 1: Karty stykowe – Charakterystyki fizyczne [4.3] Wytrzymałość mechaniczna (karty i styków)	
		[Rezystancja] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7816-1:2011, Karty identyfikacyjne – Karty elektroniczne – Część 1: Karty stykowe – Charakterystyki fizyczne [4.4] Rezystancja (styków)	
		[Wymiary] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7816-2:2007, Karty identyfikacyjne – Karty elektroniczne – Część 2: Karty stykowe – Wymiary i rozmieszczenie styków [3] Wymiary styków	
		[Rozmieszczenie] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7816-2:2007, Karty identyfikacyjne – Karty elektroniczne – Część 2: Karty stykowe – Wymiary i rozmieszczenie styków [4] Liczba i rozmieszczenie styków W przypadku modułów z sześcioma stykami styki „C4” i „C8” nie są objęte tym wymogiem dotyczącym próby.	
4	**Chip**		
4.1	Chip	[Temperatura pracy] Chip karty do tachografu pracuje w temperaturze otoczenia wynoszącej od – 25 °C do + 85 °C.	241–244 Regulamin nr 10 EKG ONZ ISO/IEC 7810 ISO/IEC 10373

Nr	Badanie	Opis	Powiązane wymogi
		[Temperatura i wilgotność] Załącznik 1C rozdział 4.4 „Wymagania środowiskowe i elektryczne”, 241) Karty do tachografu prawidłowo pracują we wszystkich warunkach klimatycznych normalnie występujących na terytorium Wspólnoty, przynajmniej w zakresie temperatur od – 25 do + 70 °C ze sporadycznymi temperaturami szczytowymi do +85 °C, przy czym „sporadyczny” oznacza nie dłużej niż 4 godziny jednorazowo i nie więcej niż 100 razy w okresie eksploatacji karty. Karty do tachografu naraża się kolejno na następujące temperatury i wilgotność przez określony czas. Po każdym etapie kartę do tachografu bada się pod kątem funkcjonalności elektrycznej. 1. Temperatura – 20 °C przez 2 h. 2. Temperatura +/– 0 °C przez 2 h. 3. Temperatura + 20 °C, wilgotność względna 50 %, przez 2 h. 4. Temperatura + 50 °C, wilgotność względna 50 %, przez 2 h 5. Temperatura + 70 °C, wilgotność względna 50 %, przez 2 h. Temperatura jest zwiększana sporadycznie do + 85 °C, wilgotność względna wynosi 50 %, przez 60 min. 6. Temperatura + 70 °C, wilgotność względna 85 %, przez 2 h. Temperatura jest zwiększana sporadycznie do + 85 °C, wilgotność względna wynosi 85 %, przez 30 min.	
		[Wilgotność] Załącznik 1C rozdział 4.4 „Wymagania środowiskowe i elektryczne”, 242) Karty do tachografu prawidłowo pracują w zakresie wilgotności od 10 % do 90 %.	
		[Kompatybilność elektromagnetyczna – EMC] Załącznik 1C rozdział 4.4 „Wymagania środowiskowe i elektryczne”, 244) W trakcie pracy karty do tachografu zachowują zgodność z regulaminem nr 10 EKG ONZ pod względem kompatybilności elektromagnetycznej.	

Nr	Badanie	Opis	Powiązane wymogi
		[Elektryczność statyczna] Załącznik 1C rozdział 4.4 „Wymagania środowiskowe i elektryczne", 244) W trakcie pracy karty do tachografu muszą być zabezpieczone przed wyładowaniami elektrostatycznymi. Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7810:2003/zmiana 1:2009, Karty identyfikacyjne – Charakterystyki fizyczne, zmiana 1: Kryteria dotyczące kart elektronicznych [9.4] Elektryczność statyczna [9.4.1] Karty elektroniczne ze stykami Napięcie próbne: 4 000 V.	
		[Urządzenia rentgenowskie] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7810:2003/zmiana 1:2009, Karty identyfikacyjne – Charakterystyki fizyczne, zmiana 1: Kryteria dotyczące kart elektronicznych [9.1.] Urządzenia rentgenowskie	
		[Promieniowanie ultrafioletowe] ISO/IEC 10373-1:2006, Karty identyfikacyjne – Metody badań – Część 1: Charakterystyki ogólne [5.11] Promieniowanie ultrafioletowe	
		[trzykołowe] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 10373-1:2006/zmiana 1:2012, Karty identyfikacyjne – Metody badań – Część 1: Charakterystyki ogólne, zmiana 1 [5.22] Karta elektroniczna – Wytrzymałość mechaniczna: trzykołowy test kart elektronicznych ze stykami	
		[Nawijanie] Karty do tachografu muszą być zgodne z wymogami normy MasterCard CQM V2.03:2013 [11.1.3] R-L3-14-8: Próba trwałości nawijania [13.2.1.32] TM-422: Niezawodność mechaniczna: próba nawijania	

Nr	Badanie	Opis	Powiązane wymogi
4.2	Próby mechaniczne modułu chipowego wbudowanego w kartę -> takie same jak w sekcji 2.3	[Zginanie] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7810:2003/zmiana 1:2009, Karty identyfikacyjne – Charakterystyki fizyczne, zmiana 1: Kryteria dotyczące kart elektronicznych [9.2] Dynamiczne naprężenie zginające Łączna liczba cykli zginania: 4 000. [Skręcanie] Karty do tachografu muszą być zgodne z wymogami normy ISO/IEC 7810:2003/zmiana 1:2009, Karty identyfikacyjne – Charakterystyki fizyczne, zmiana 1: Kryteria dotyczące kart elektronicznych [9.3] Dynamiczne naprężenie skręcające Łączna liczba cykli skręcania: 4 000.	ISO/IEC 7810
5	**Testy protokołów**		
5.1	Ciąg ATR	Sprawdzenie zgodności ciągu ATR.	ISO/IEC 7816-3 TCS_14, TCS_17, TCS_18
5.2	T=0	Sprawdzenie zgodności protokołu T=0.	ISO/IEC 7816-3 TCS_11, TCS_12, TCS_13, TCS_15
5.3	PTS	Sprawdzenie zgodności polecenia PTS przez ustawienie T = 1 z T = 0.	ISO/IEC 7816-3 TCS_12, TCS_19, TCS_20, TCS_21
5.4	T=1	Sprawdzenie zgodności protokołu T = 1.	ISO/IEC 7816-3 TCS_11, TCS_13, TCS_16
6	**Struktura karty**		
6.1		Sprawdzenie zgodności struktury plików na karcie przez sprawdzenie, czy na karcie są wymagane pliki oraz sprawdzenie warunków dostępu do plików.	TCS_22–TCS_28 TCS_140–TCS_179
7	**Badania funkcjonalności**		
7.1	Normalne przetwarzanie	Sprawdzenie co najmniej raz każdego, dozwolonego użycia każdego polecenia (np.: sprawdzenie polecenia UPDATE BINARY z CLA = '00', CLA = '0C' i z różnymi parametrami P1, P2 i Lc). Sprawdzenie, czy karta rzeczywiście wykonuje czynności (np.: odczytując plik poleceniem wykonywanym na tym pliku).	TCS_29–TCS_139

Nr	Badanie	Opis	Powiązane wymogi
7.2	Komunikaty błędu	Sprawdzenie co najmniej raz każdego komunikatu błędu (określonego w dodatku 2) dla każdego polecenia. Sprawdzenie co najmniej raz każdego błędu ogólnego (z wyjątkiem błędów integralności '**6400**' sprawdzanych w trakcie certyfikacji bezpieczeństwa).	
7.3	Pakiet szyfrów i standardowe parametry domeny		CSM_48, CSM_50
8	**Personalizacja**		
8.1	Personalizacja optyczna	(Załącznik 1C rozdział 4.1 „Dane widzialne", 230) Na awersie znajdują się: informacje szczególne dla wydanej karty. (Załącznik 1C rozdział 4.1 „Dane widzialne", 231) Na awersie znajdują się: daty podaje się w formacie „dd/mm/rrrr" lub „dd.mm.rrrr" (dzień, miesiąc, rok). (Załącznik 1C rozdział 4.1 „Dane widzialne", 235) Karty do tachografu mają przynajmniej następujące zabezpieczenia przed fałszowaniem i manipulowaniem: — w obszarze zdjęcia zabezpieczający wzór tła i zdjęcie zachodzą na siebie.	230, 231, 235

5. BADANIA URZĄDZENIA ZEWNĘTRZNEGO GNSS

Nr	Badanie	Opis	Powiązane wymogi
1.	**Badanie administracyjne**		
1.1	Dokumentacja	Prawidłowość dokumentacji	
2.	**Kontrola wizualna urządzenia zewnętrznego GNSS**		
2.1	Zgodność z dokumentacją		
2.2	Identyfikacja/oznakowanie		224–226
2.3	Materiały		219–223
3.	**Badania funkcjonalności**		
3.1	Dane identyfikacyjne czujnika		98, 99
3.2	Połączenie między zewnętrznym modułem GNSS a przyrządem rejestrującym		123, 205

Nr	Badanie	Opis	Powiązane wymogi
3.3	Położenie GNSS		36, 37
3.4	Interfejs przyrządu rejestrującego, gdy odbiornik GNSS znajduje się na zewnątrz przyrządu rejestrującego		03
3.5	Pakiet szyfrów i standardowe parametry domeny		CSM_48, CSM_50
4.	**Badania środowiskowe**		
4.1	Temperatura	Sprawdzenie funkcjonalności za pomocą: badania zgodnie z normą ISO 16750-4, Rozdział 5.1.1.2: Próba eksploatacyjna w niskiej temperaturze (72 h w temperaturze – 20 °C). Badanie to odnosi się do normy IEC 60068-2-1: Badania środowiskowe – Część 2-1: Próby – Próba A: Zimno. badania zgodnie z normą ISO 16750-4, Rozdział 5.1.2.2: Próba eksploatacyjna w wysokiej temperaturze (72 h w temperaturze 70 °C). Badanie to odnosi się do normy IEC 60068-2-2: Podstawowe procedury badań środowiskowych – Część 2: Próby – Próba B: Suche gorąco; Badanie zgodnie z normą ISO 16750-4: Rozdział 5.3.2: Nagła zmiana temperatury z określonym okresem przejściowym (20 °C/70 °C, 20 cykli, czas przebywania: 1 h w każdej temperaturze). Można przeprowadzić skrócony zestaw badań (spośród tych zdefiniowanych w sekcji 3 niniejszej tabeli) w niższej temperaturze, wyższej temperaturze i w czasie cykli temperaturowych.	213
4.2	Wilgotność	Sprawdzenie odporności przyrządu rejestrującego na cykliczne zmiany wilgotności (próba gorąca) za pomocą próby Db wg normy IEC 60068-2-30, w sześciu 24-godzinnych cyklach, w każdym ze zmieniającą się temperaturą od + 25 °C do + 55 °C i wilgotnością względną 97 % w + 25 °C i 93 % w + 55 °C	214
4.3	Mechanika	1. Drgania harmoniczne: sprawdzenie odporności przyrządu rejestrującego na drgania harmoniczne o następujących właściwościach: stałe przemieszczenie przy częstotliwości 5–11 Hz: 10-milimetrowa amplituda; stałe przyspieszenie przy częstotliwości 11–300 Hz: 5g. Wymóg ten sprawdza się za pomocą próby Fc wg normy IEC 60068-2-6, z minimalnym czasem trwania próby 3 × 12 h (12 h na oś). ISO 16750-3 nie wymaga przeprowadzenia testu drgań harmonicznych w przypadku urządzeń znajdujących się w oddzielnej kabinie pojazdu.	219

Nr	Badanie	Opis	Powiązane wymogi
		2. Drgania swobodne: Próba zgodnie z ISO 16750-3: Rozdział 4.1.2.8: Próba VIII: Pojazd użytkowy, oddzielna kabina pojazdu. Próba drgań swobodnych: 10 … 2 000 Hz, wertykalna średnia kwadratowa 21,3 m/s^2, wzdłużna średnia kwadratowa 11,8 m/s^2, poprzeczna średnia kwadratowa 13,1 m/s^2, 3 osie, 32 h na oś, w tym cykl temperaturowy – 20 … 70°C. Badanie to odnosi się do normy IEC 60068-2-64: Badania środowiskowe – Część 2-64: Próby – Próba Fh: Wibracje szerokopasmowe losowe i wytyczne. 3. Udary: udar mechaniczny przy impulsie półsinusoidalnym 3 g wg normy ISO 16750. Opisane powyżej badania przeprowadza się na różnych próbkach urządzeń poddawanych badaniom.	
4.4	Ochrona przed wodą i ciałami obcymi	Badanie zgodnie z normą ISO 20653: Pojazdy drogowe – Stopień ochrony (kod IP) – Ochrona urządzeń elektrycznych przed ciałami obcymi, wodą i dostępem (bez zmian parametrów)	220, 221
4.5	Zabezpieczenie nadnapięciowe	Sprawdzenie odporności przyrządu rejestrującego na napięcie zasilania: wersje 24 V: 34 V przy + 40 °C przez 1 godzinę wersje 12 V: 17 V przy + 40 °C przez 1 godzinę (ISO 16750-2 rozdział 4.3)	216
4.6	Zabezpieczenie przed odwróceniem polaryzacji	Sprawdzenie odporności przyrządu rejestrującego na odwrócenie biegunów napięcia zasilającego. (ISO 16750-2 rozdział 4.7)	216
4.7	Zabezpieczenie zwarciowe	Sprawdzenie, czy sygnały wyjściowe są zabezpieczone przed zwarciem do napięcia zasilającego i do masy. (ISO 16750-2 rozdział 4.10)	216
5	**Badania EMC**		
5.1	Emisje radiacyjne i wrażliwość na radiację	Zgodność z regulaminem nr 10 EKG ONZ	218

Nr	Badanie	Opis	Powiązane wymogi
5.2	Wyładowania elektrostatyczne	Zgodność z normą ISO 10605:2008 + Sprostowanie techniczne: 2010 + AMD1: 2014: +/– 4 kV w przypadku styku i +/– 8 kV w przypadku rozładowania do powietrza	218
5.3	Wrażliwość na stany nieustalone w zasilaniu	W przypadku wersji 24 V: zgodność z normą ISO 7637-2 i wersją 3 regulaminu nr 10 EKG ONZ: impuls 1a: Vs = – 450 V, Ri = 50 omów impuls 2a: Vs = + 37 V, Ri = 2 omy impuls 2b: Vs = + 20 V, Ri = 0,05 oma impuls 3a: Vs = – 150 V, Ri = 50 omów impuls 3b: Vs = + 150 V, Ri = 50 omów impuls 4: Vs = – 16 V Va = – 12V, t6 = 100 ms impuls 5: Vs = + 120 V, Ri = 2,2 oma, td = 250 ms W przypadku wersji 12 V: zgodność z normą ISO 7637-1 i wersją 3 regulaminu nr 10 EKG ONZ: impuls 1: Vs = – 75 V, Ri = 10 omów impuls 2a: Vs = + 37 V, Ri = 2 omy impuls 2b: Vs = + 10 V, Ri = 0,05 oma impuls 3a: Vs = – 112 V, Ri = 50 omów impuls 3b: Vs = + 75 V, Ri = 50 omów impuls 4: Vs = – 6 V, Va = – 5 V, t6 = 15 ms impuls 5: Vs = + 65 V, Ri = 3 omy, td = 100 ms Impuls 5 należy testować tylko w przypadku przyrządów rejestrujących przeznaczonych do zainstalowania w pojazdach, w których nie zainstalowano zewnętrznego, wspólnego zabezpieczenia przed spadkiem obciążenia. Aby uzyskać informacje na temat propozycji zabezpieczenia przed spadkiem obciążenia, zob. norma ISO 16750-2 wydanie 4. rozdział 4.6.4.	218

6. BADANIA URZĄDZENIA DO ŁĄCZNOŚCI NA ODLEGŁOŚĆ

Nr	Badanie	Opis	Powiązane wymogi
1.	**Badanie administracyjne**		
1.1	Dokumentacja	Prawidłowość dokumentacji	
2.	**Kontrola wizualna**		
2.1	Zgodność z dokumentacją		
2.2	Identyfikacja/oznakowanie		225, 226
2.3	Materiały		219 to 223

Nr	Badanie	Opis	Powiązane wymogi
4.	**Badania środowiskowe**		
4.1	Temperatura	Sprawdzenie funkcjonalności za pomocą: badania zgodnie z normą ISO 16750-4, Rozdział 5.1.1.2: Próba eksploatacyjna w niskiej temperaturze (72 h w temperaturze – 20 °C). Badanie to odnosi się do normy IEC 60068-2-1: Badania środowiskowe – Część 2-1: Próby – Próba A: Zimno. badania zgodnie z normą ISO 16750-4, Rozdział 5.1.2.2: Próba eksploatacyjna w wysokiej temperaturze (72 h w temperaturze 70 °C). Badanie to odnosi się do normy IEC 60068-2-2: Podstawowe procedury badań środowiskowych – Część 2: Próby – Próba B: Suche gorąco; Badanie zgodnie z normą ISO 16750-4: Rozdział 5.3.2: Nagła zmiana temperatury z określonym okresem przejściowym (20 °C/70 °C, 20 cykli, czas przebywania: 1 h (?) w każdej temperaturze). Można przeprowadzić skrócony zestaw badań (spośród tych zdefiniowanych w sekcji 3 niniejszej tabeli) w niższej temperaturze, wyższej temperaturze i w czasie cykli temperaturowych.	213
4.4	Ochrona przed wodą i ciałami obcymi	Badanie zgodnie z normą ISO 20653: Pojazdy drogowe – Stopień ochrony (kod IP) – Ochrona urządzeń elektrycznych przed ciałami obcymi, wodą i dostępem (wartość docelowa IP40)	220, 221
5	**Badania EMC**		
5.1	Emisje radiacyjne i wrażliwość na radiację	Zgodność z regulaminem nr 10 EKG ONZ	218
5.2	Wyładowania elektrostatyczne	Zgodność z normą ISO 10605:2008 + Sprostowanie techniczne:2010 + AMD1:2014: +/– 4kV w przypadku styku i +/– 8kV w przypadku rozładowania do powietrza	218
5.3	Wrażliwość na stany nieustalone w zasilaniu	W przypadku wersji 24 V: zgodność z normą ISO 7637-2 i wersją 3 regulaminu nr 10 EKG ONZ: impuls 1a: Vs = – 450 V, Ri = 50 omów impuls 2a: Vs = + 37 V, Ri = 2 omy impuls 2b: Vs = + 20 V, Ri = 0,05 oma impuls 3a: Vs = – 150 V, Ri = 50 omów impuls 3b: Vs = + 150 V, Ri = 50 omów impuls 4: Vs = – 16 V Va = – 12V, t6 = 100 ms impuls 5: Vs = + 120 V, Ri = 2,2 oma, td = 250 ms	218

Nr	Badanie	Opis	Powiązane wymogi
		W przypadku wersji 12 V: zgodność z normą ISO 7637-1 i wersją 3 regulaminu nr 10 EKG ONZ: impuls 1: Vs = – 75 V, Ri = 10 omów impuls 2a: Vs = + 37 V, Ri = 2 omy impuls 2b: Vs = + 10 V, Ri = 0,05 oma impuls 3a: Vs = – 112 V, Ri = 50 omów impuls 3b: Vs = + 75 V, Ri = 50 omów impuls 4: Vs = – 6 V, Va = – 5 V, t6 = 15 ms impuls 5: Vs = + 65 V, Ri = 3 omy, td = 100 ms Impuls 5 należy testować tylko w przypadku przyrządów rejestrujących przeznaczonych do zainstalowania w pojazdach, w których nie zainstalowano zewnętrznego, wspólnego zabezpieczenia przed spadkiem obciążenia. Aby uzyskać informacje na temat propozycji zabezpieczenia przed spadkiem obciążenia, zob. norma ISO 16750-2 wydanie 4. rozdział 4.6.4.	

7. BADANIA FUNKCJONALNOŚCI PAPIERU

Nr	Badanie	Opis	Powiązane wymogi
1.	**Badanie administracyjne**		
1.1	Dokumentacja	Prawidłowość dokumentacji	
2	**Badania ogólne**		
2.1	Liczba znaków w wierszu	Kontrola wizualna wydruków	172
2.2	Minimalna wielkość czcionki	Kontrola wizualna wydruków i kontrola znaków	173
2.3	Obsługiwane zestawy znaków	Drukarka umożliwia drukowanie znaków określonych w dodatku 1 rozdział 4 „Zestawy znaków”.	174
2.4	Definicja wydruków	Sprawdzenie homologacji typu tachografu i przeprowadzenie kontroli wizualnej wydruków	174
2.5	Czytelność i identyfikacja wydruków	Kontrola wydruków Potwierdzona sprawozdaniami z badań i protokołami badań przez producenta. Wszystkie numery homologacyjne tachografów, z którymi można używać danego papieru do drukarek, wydrukowano na papierze.	175, 177, 178
2.6	Dodawanie uwag odręcznych	Kontrola wizualna: dostępne jest miejsce na podpis kierowcy. Dostępne jest miejsce na inne dodatkowe wpisy odręczne.	180

Nr	Badanie	Opis	Powiązane wymogi
2.7	Dodatkowe informacje szczegółowe na pierwszej stronie kartki papieru	Pierwsza i druga strona kartki papieru mogą zawierać dodatkowe szczegółowe dane i informacje. Tego rodzaju dodatkowe szczegółowe dane i informacje nie mogą ograniczać czytelności wydruków. Kontrola wizualna	177, 178
3	**Badania przechowywania**		
3.1	Suche gorąco	Kondycjonowanie wstępne: 16 h w temperaturze + 23 °C ± 2 °C/przy wilgotności względnej 55 % ± 3 %. Środowisko testowe: 72 h w temperaturze + 70 °C ± 2 °C. Odzyskanie: 16 h w temperaturze + 23 °C ± 2 °C/przy wilgotności względnej 55 % ± 3 %.	176, 178 IEC 60068-2-2-Bb
2.2	Wilgotne gorąco	Kondycjonowanie wstępne: 16 h w temperaturze + 23 °C ± 2 °C/przy wilgotności względnej 55 % ± 3 %. Środowisko testowe: 144 h w temperaturze + 55 °C ± 2 ° C/przy wilgotności względnej 93 % ± 3 %. Odzyskanie: 16 h w temperaturze + 23 °C ± 2 °C/przy wilgotności względnej 55 % ± 3 %.	176, 178 IEC 60068-2-78-Cab
4	**Badania papieru w użyciu**		
4.1	Podstawowa odporność na działanie wilgoci (papier niezadrukowany)	Kondycjonowanie wstępne: 16 h w temperaturze + 23 °C ± 2 °C/przy wilgotności względnej 55 % ± 3 %. Środowisko testowe: 144 h w temperaturze + 55 °C ± 2 ° C/przy wilgotności względnej 93 % ± 3 %. Odzyskanie: 16 h w temperaturze + 23 °C ± 2 °C/przy wilgotności względnej 55 % ± 3 %.	176, 178 IEC 60068-2-78-Cab
4.2	Drukowność	Kondycjonowanie wstępne: 24 h w temperaturze + 40 °C ± 2 °C/przy wilgotności względnej 93 % ± 3 %. Środowisko testowe: wydruk sporządzony w temperaturze + 23 °C ± 2 °C Odzyskanie: 16 h w temperaturze + 23 °C ± 2 °C/przy wilgotności względnej 55 % ± 3 %.	176, 178
4.3	Odporność na działanie wysokich temperatur	Kondycjonowanie wstępne: 16 h w temperaturze + 23 °C ± 2 °C/przy wilgotności względnej 55 % ± 3 %. Środowisko testowe: 2 h w temperaturze + 70 °C ± 2 °C, suche gorąco Odzyskanie: 16 h w temperaturze + 23 °C ± 2 °C/przy wilgotności względnej 55 % ± 3 %.	176, 178 IEC 60068-2-2-Bb
4.4	Odporność na działanie niskich temperatur	Kondycjonowanie wstępne: 16 h w temperaturze + 23 °C ± 2 °C/przy wilgotności względnej 55 % ± 3 %. Środowisko testowe: 24 h w temperaturze – 20 °C ± 3 °C, suche zimno Odzyskanie: 16 h w temperaturze + 23 °C ± 2 °C/przy wilgotności względnej 55 % ± 3 %.	176, 178 ISO 60068-2-1-Ab

Nr	Badanie	Opis	Powiązane wymogi
4.5	Światłoodporność	Kondycjonowanie wstępne: 16 h w temperaturze + 23 °C ± 2 °C/przy wilgotności względnej 55 % ± 3 %. Środowisko testowe: 100 h pod oświetleniem o natężeniu 5 000 luksów w temperaturze + 23 °C ± 2 °C przy wilgotności względnej 55 % ± 3 % Odzyskanie: 16 h w temperaturze + 23 °C ± 2 °C/przy wilgotności względnej 55 % ± 3 %.	176, 178

Kryteria czytelności w odniesieniu do badań 3.x i 4.x:

Czytelność wydruku jest zapewniona, jeżeli gęstości optyczne są zgodne z następującymi ograniczeniami:

Wielkość drukowanych znaków: min. 1,0

Tło (papier niezadrukowany): maks. 0,2

Gęstości optyczne otrzymanych wydruków mierzy się według DIN EN ISO 534.

Wydruki muszą przedstawiać niezmienione wymiary i być wyraźnie czytelne.

8. BADANIA INTEROPERACYJNOŚCI

Nr	Badanie	Opis
9.1 Badania interoperacyjności między przyrządami rejestrującymi a kartami do tachografu		
1	Wzajemne uwierzytelnienie	Sprawdzenie, czy wzajemne uwierzytelnienie między przyrządem rejestrującym a kartą do tachografu przebiega normalnie.
2	Próby zapisu/odczytu	Wykonanie scenariusza typowej czynności na przyrządzie rejestrującym. Scenariusz dostosowany jest do typu badanej karty i obejmuje zapis na karcie tak wielu EF, jak to możliwe. Sprawdzenie poprzez pobieranie danych z przyrządu rejestrującego, czy wszystkie odpowiednie zapisy zostały wykonane prawidłowo. Sprawdzenie poprzez pobieranie danych z karty, czy wszystkie odpowiednie zapisy zostały wykonane prawidłowo. Sprawdzenie poprzez dzienny wydruk z karty, czy wszystkie odpowiednie zapisy mogą być odczytane prawidłowo.
9.2 Badania interoperacyjności między przyrządami rejestrującymi a czujnikami ruchu		
1	Parowanie	Sprawdzenie, czy parowanie przyrządu rejestrującego z czujnikami ruchu przebiega normalnie.
2	Badania czynności	Wykonanie scenariusza typowej czynności na czujniku ruchu. Scenariusz obejmuje normalną czynność i wygenerowanie jak największej liczby zdarzeń lub usterek. Sprawdzenie poprzez pobieranie danych z przyrządu rejestrującego, czy wszystkie odpowiednie zapisy zostały wykonane prawidłowo. Sprawdzenie poprzez pobieranie danych z karty, czy wszystkie odpowiednie zapisy zostały wykonane prawidłowo. Sprawdzenie poprzez dzienny wydruk, czy wszystkie odpowiednie zapisy mogą być odczytane prawidłowo.

Nr	Badanie	Opis
9.3 Badania interoperacyjności między przyrządami rejestrującymi a urządzeniem zewnętrznym GNSS (w stosownych przypadkach)		
1	Wzajemne uwierzytelnienie	Sprawdzenie, czy wzajemne uwierzytelnienie (połączenie) między przyrządem rejestrującym a zewnętrznym modułem GNSS przebiega normalnie.
2	Badania czynności	Wykonanie scenariusza typowej czynności na zewnętrznym urządzeniu GNSS. Scenariusz obejmuje normalną czynność i wygenerowanie jak największej liczby zdarzeń lub usterek. Sprawdzenie poprzez pobieranie danych z przyrządu rejestrującego, czy wszystkie odpowiednie zapisy zostały wykonane prawidłowo. Sprawdzenie poprzez pobieranie danych z karty, czy wszystkie odpowiednie zapisy zostały wykonane prawidłowo. Sprawdzenie poprzez dzienny wydruk, czy wszystkie odpowiednie zapisy mogą być odczytane prawidłowo

Dodatek 10

WYMOGI BEZPIECZEŃSTWA

W niniejszym dodatku określono wymogi bezpieczeństwa informatycznego dotyczące elementów składowych systemu tachografu inteligentnego (tachografu drugiej generacji).

SEC_001 Następujące elementy składowe systemu tachografu inteligentnego muszą posiadać certyfikacje bezpieczeństwa zgodnie z systemem wspólnych kryteriów:

— przyrząd rejestrujący;

— karta do tachografu;

— czujnik ruchu;

— urządzenie zewnętrzne GNSS.

SEC_002 Minimalne wymogi bezpieczeństwa informatycznego, jakie ma spełnić każdy element składowy, który musi posiadać certyfikację bezpieczeństwa, określa się w profilu zabezpieczenia dla elementu składowego, zgodnie z systemem wspólnych kryteriów.

SEC_003 Komisja Europejska upewnia się, że cztery profile zabezpieczenia zgodne z niniejszym załącznikiem są finansowane, opracowywane, zatwierdzane przez rządowe jednostki certyfikujące ds. bezpieczeństwa informatycznego, skupione w grupie roboczej ds. wspólnej interpretacji (JIWG), która wspiera wzajemne uznawanie certyfikatów pod egidą SOGIS-MRA (Umowa o wzajemnym uznawaniu świadectw z oceny bezpieczeństwa informatycznego), oraz rejestrowane:

— profil zabezpieczenia dla przyrządu rejestrującego;

— profil zabezpieczenia dla karty do tachografu;

— profil zabezpieczenia dla czujnika ruchu;

— profil zabezpieczenia dla urządzenia zewnętrznego GNSS.

Profil zabezpieczenia dla przyrządu rejestrującego uwzględnia przypadki, gdy przyrząd rejestrujący jest przeznaczony do użytkowania z urządzeniem zewnętrznym GNSS, jak i gdy nie jest do tego przeznaczony. W tym pierwszym przypadku wymogi bezpieczeństwa dotyczące urządzenia zewnętrznego GNSS zostają podane w specjalnym profilu zabezpieczenia.

SEC_004 Aby nadać kształt celowi zabezpieczenia, który stanowi podstawę do uzyskania certyfikacji bezpieczeństwa elementu składowego, producenci elementów składowych przygotowują i kompletują niezbędny profil zabezpieczenia dla odpowiedniego elementu składowego bez poprawiania i usuwania istniejących zagrożeń, celów, środków proceduralnych i specyfikacji funkcji realizujących zabezpieczenia.

SEC_005 Ścisła zgodność takiego konkretnego celu zabezpieczenia z odpowiednim profilem zabezpieczenia musi zostać stwierdzona w procesie oceny.

SEC_006 Poziomem gwarancji dla każdego profilu zabezpieczenia jest poziom EAL4 wzmocniony elementami gwarancji ATE_DPT.2 i AVA_VAN.5.

Dodatek 11

WSPÓLNE MECHANIZMY ZABEZPIECZENIA

SPIS TREŚCI

INFORMACJE OGÓLNE

W niniejszym dodatku określa się mechanizmy zabezpieczenia zapewniające:

— wzajemne uwierzytelnienie między różnymi elementami składowymi systemu tachografu;

— poufność, integralność, autentyczność lub niezaprzeczalność danych przekazywanych między różnymi elementami składowymi systemu tachografu lub pobieranych na zewnętrzne nośniki danych.

Niniejszy dodatek składa się z dwóch części. W części A opisano mechanizmy zabezpieczenia stosowane w systemie tachografu pierwszej generacji (tachograf cyfrowy). W części B opisano mechanizmy zabezpieczenia stosowane w systemie tachografu drugiej generacji (tachograf inteligentny).

Mechanizmy opisane w części A niniejszego dodatku stosuje się, jeżeli przynajmniej jeden element składowy systemu tachografu wykorzystywany w procesie wzajemnego uwierzytelniania lub przesyłania danych jest urządzeniem pierwszej generacji.

Mechanizmy opisane w części B niniejszego dodatku stosuje się, jeżeli obydwa elementy składowe systemu tachografu wykorzystywane w procesie wzajemnego uwierzytelniania lub przesyłania danych są urządzeniami drugiej generacji.

Dodatek 15 zawiera dodatkowe informacje na temat korzystania z elementów składowych pierwszej generacji w połączeniu z elementami składowymi drugiej generacji.

CZĘŚĆ A

SYSTEM TACHOGRAFU PIERWSZEJ GENERACJI

1. WPROWADZENIE

1.1. **Odniesienia**

W niniejszym dodatku używa się następujących odniesień:

SHA-1	Narodowy Instytut Standaryzacji i Technologii (NIST). *FIPS Publikacja 180-1: Bezpieczny standard skrótu*. Kwiecień 1995 r.
PKCS1	RSA Laboratories. PCKS # 1: *Standard szyfrowania RSA*. Wersja 2.0. Październik 1998 r.
TDES	Narodowy Instytut Standaryzacji i Technologii (NIST). *FIPS Publikacja 46-3: Symetryczny algorytm kryptograficzny*. Projekt 1999 r.
TDES-OP	ANSI X9.52, Tryby pracy algorytmu trzyetapowego szyfrowania danych. 1998 r.
ISO/IEC 7816-4	Technologia informacyjna – Karty identyfikacyjne – Elektroniczne karty stykowe – Część 4: Międzybranżowe polecenia wymiany informacji. Wydanie pierwsze: 1995 r. + zmiana 1: 1997 r.
ISO/IEC 7816-6	Technologia informacyjna – Karty identyfikacyjne – Elektroniczne karty stykowe – Część 6: Międzybranżowe elementy danych. Wydanie pierwsze: 1996 r. + zmiana 1: 1998 r.
ISO/IEC 7816-8	Technologia informacyjna – Karty identyfikacyjne – Elektroniczne karty stykowe – Część 8: Międzybranżowe polecenia związane z bezpieczeństwem. Wydanie pierwsze: 1999 r.
ISO/IEC 9796-2	Technologia informacyjna – Techniki zabezpieczeń – Schematy podpisu cyfrowego z odtwarzaniem wiadomości – Część 2: Mechanizmy oparte na faktoryzacji liczb całkowitych. Wydanie pierwsze: 1997 r.
ISO/IEC 9798-3	Technologia informacyjna – Techniki zabezpieczeń – Mechanizmy uwierzytelnienia jednostki – Część 3: Uwierzytelnienie jednostki przy użyciu algorytmu klucza publicznego. Wydanie drugie: 1998 r.
ISO 16844-3	Pojazdy drogowe – Systemy tachograficzne – Część 3: Interfejs czujnika ruchu.

1.2. **Oznaczenia i skróty**

W niniejszym dodatku używa się następujących oznaczeń i skrótów:

(K_a, K_b, K_c)	wiązka kluczy używanych w algorytmie trzyetapowego szyfrowania danych,
CA	organ certyfikacji
CAR	odniesienie do organu certyfikacji
CC	kryptograficzna suma kontrolna
CG	kryptogram
CH	nagłówek polecenia
CHA	upoważnienie posiadacza certyfikatu
CHR	odniesienie do posiadacza certyfikatu
D()	deszyfracja DES

DE	element danych
DO	obiekt danych
d	klucz prywatny RSA, wykładnik prywatny
e	klucz publiczny RSA, wykładnik publiczny
E()	szyfrowanie DES
EQT	urządzenie
Hash()	skrót, wartość wyjściowa funkcji skrótu
Hash	funkcja skrótu
KID	identyfikator klucza
Km	klucz TDES, klucz główny wg normy ISO 16844-3
Km_{VU}	klucz TDES umieszczony w przyrządzie rejestrującym
Km_{WC}	klucz TDES umieszczony w kartach warsztatowych
m	reprezentacja komunikatu, liczba całkowita z przedziału od 0 do n-1
n	klucze RSA, moduły
PB	bajty wypełnienia
PI	bajt wskaźnik wypełnienia (do zastosowania w kryptogramie dla poufności DO)
PV	wartość odkryta
s	reprezentacja podpisu, liczba całkowita z przedziału od 0 do n-1
SSC	licznik sekwencji wysyłania
SM	bezpieczna wymiana komunikatów
TCBC	tryb wiązania bloków zaszyfrowanych TDEA
TDEA	algorytm trzyetapowego szyfrowania danych
TLV	obiekt TLV
VU	przyrząd rejestrujący
X.C	certyfikat użytkownika X wydany przez organ certyfikacji
X.CA	organ certyfikacji użytkownika X
X.CA.PK $_{o}$ X.C	Operacja rozpakowania certyfikatu w celu wyodrębnienia klucza publicznego. Jest to operator wrostkowy, którego argumentem lewostronnym jest klucz publiczny organu certyfikacji, a argumentem prawostronnym jest certyfikat wydany przez ten organ certyfikacji. Wynikiem jest klucz publiczny użytkownika X, którego certyfikat jest argumentem prawostronnym.
X.PK	klucz publiczny użytkownika X
X.PK[I]	szyfrowanie RSA pewnych informacji kluczem publicznym I użytkownika X
X.SK	klucz prywatny RSA użytkownika X
X.SK[I]	szyfrowanie RSA pewnych informacji kluczem prywatnym I użytkownika X
‘xx’	wartość heksadecymalna
||	operator konkatenacji

2. SYSTEMY I ALGORYTMY KRYPTOGRAFICZNE

2.1. **Systemy kryptograficzne**

CSM_001 Przyrządy rejestrujące i karty do tachografu używają klasycznego systemu kryptograficznego RSA z kluczem publicznym do realizowania następujących mechanizmów zabezpieczenia:

— uwierzytelnienie między przyrządami rejestrującymi a kartami,

— transport kluczy sesji Triple-DES między przyrządami rejestrującymi a kartami do tachografu,

— podpis cyfrowy danych pobieranych z przyrządów rejestrujących lub kart do tachografu do zewnętrznych nośników.

CSM_002 Przyrządy rejestrujące i karty do tachografu używają symetrycznego systemu kryptograficznego Triple-DES do zrealizowania mechanizmu zapewniającego integralność danych w czasie wymiany danych użytkownika między przyrządami rejestrującymi a kartami do tachografu i zapewnienia, w stosownych przypadkach, poufności wymiany danych między przyrządami rejestrującymi a kartami do tachografu.

2.2. **Algorytmy kryptograficzne**

2.2.1 *Algorytm RSA*

CSM_003 Algorytm RSA w pełni definiują następujące relacje:

$$X.SK[m] = s = m^d \bmod n$$
$$X.PK[s] = m = s^e \bmod n$$

Bardziej wyczerpujący opis funkcji RSA można znaleźć w odniesieniu [PKCS1]. Wykładnik publiczny, e, dla obliczeń RSA jest liczbą całkowitą pomiędzy 3 i n-1 spełniającą gcd(e, lcm(p-1, q-1))=1.

2.2.2 *Algorytm skrótu*

CSM_004 Mechanizmy podpisu cyfrowego używają algorytmu skrótu SHA-1 zdefiniowanego w odniesieniu [SHA-1].

2.2.3 *Algorytm szyfrowania danych*

CSM_005 Algorytmy oparte na algorytmie DES są używane w trybie wiązania bloków zaszyfrowanych.

3. KLUCZE I CERTYFIKATY

3.1. **Generowanie i dystrybucja kluczy**

3.1.1 *Generowanie i dystrybucja kluczy RSA*

CSM_006 Klucze RSA są generowane na trzech hierarchicznych poziomach funkcjonalnych:

— poziomie europejskim,

— poziomie państwa członkowskiego,

— poziomie urządzenia.

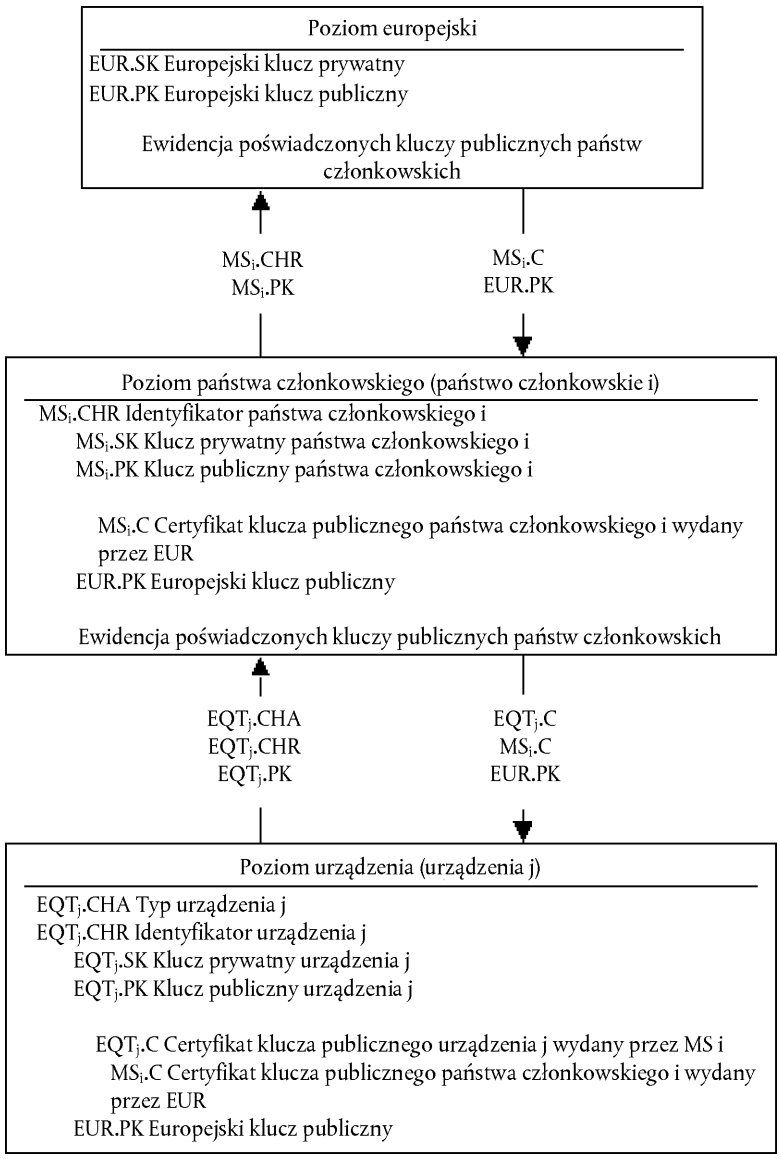
CSM_007 Na poziomie europejskim generuje się jedną parę kluczy europejskich (EUR.SK i EUR.PK). Do poświadczania kluczy publicznych państw członkowskich służy europejski klucz prywatny. Należy prowadzić rejestry wszystkich certyfikowanych kluczy. Organem odpowiedzialnym za realizację tych zadań jest europejski organ certyfikacji, działający z upoważnienia i na odpowiedzialność Komisji Europejskiej.

CSM_008 Na poziomie państwa członkowskiego generuje się parę kluczy państwa członkowskiego (MS.SK i MS.PK). Klucze publiczne państwa członkowskiego certyfikuje europejski organ certyfikacji. Klucza prywatnego państwa członkowskiego używa się do certyfikowania kluczy publicznych umieszczanych w urządzeniach (w przyrządzie rejestrującym lub karcie do tachografu). Należy prowadzić rejestry wszystkich certyfikowanych kluczy publicznych wraz z identyfikacją urządzeń, dla których są przewidziane. Organem realizującym te zadania jest organ certyfikacji państwa członkowskiego. Państwo członkowskie może okresowo zmieniać swoją parę kluczy.

CSM_009 Na poziomie urządzenia generuje się jedną parę kluczy (EQT.SK i EQT.PK), którą umieszcza się w każdym urządzeniu. Klucze publiczne urządzenia certyfikuje organ certyfikacji państwa członkowskiego. Zadania te mogą realizować producenci urządzeń, jednostki personalizujące urządzenia lub organy państwa członkowskiego. Wspomnianej pary kluczy używa się do uwierzytelniania, składania podpisu cyfrowego oraz świadczenia usług w zakresie szyfrowania.

CSM_010 W czasie generowania, ewentualnego transportu i przechowywania należy zachować poufność kluczy prywatnych.

Na poniższym rysunku zobrazowano przepływ danych w tym procesie:



3.1.2 *Klucze testowe RSA*

CSM_011 Do celów testowania urządzeń (włącznie z badaniami interoperacyjności) europejski organ certyfikacji generuje różniące się pary kluczy, jedną europejską parę kluczy testowych i przynajmniej dwie pary kluczy testowych państwa członkowskiego, których klucze publiczne są certyfikowane europejskim prywatnym kluczem testowym. Producenci umieszczają w urządzeniach przechodzących testy homologacji typu klucze testowe certyfikowane jednym z tych kluczy testowych państwa członkowskiego.

3.1.3 *Klucze czujnika ruchu*

W czasie generowania, ewentualnego transportu i przechowywania w należyty sposób zachowuje się poufność trzech kluczy Triple DES opisanych poniżej.

W celu obsługi elementów składowych tachografu zgodnych z normą ISO 16844 europejski organ certyfikacji i organ certyfikacji państwa członkowskiego dodatkowo zapewniają, co następuje:

CSM_036 europejski organ certyfikacji generuje KmVU i KmWC, dwa niezależne i unikatowe klucze Triple DES, oraz generuje Km jako: $Km = Km_{VU}$ XOR KM_{WC} . Europejski organ certyfikacji przesyła te klucze, z zachowaniem stosownych procedur bezpieczeństwa, organom certyfikacji państw członkowskich na ich wniosek.

CSM_037 Organy certyfikacji państw członkowskich:

— używają Km do szyfrowania danych czujnika ruchu wymaganych przez producentów czujników ruchu (dane, które mają być zaszyfrowane kluczem Km, są określone w normie ISO 16844-3),

— przesyłają klucz Km_{VU} producentom przyrządów rejestrujących z zachowaniem należytych procedur bezpieczeństwa w celu umieszczenia w przyrządach rejestrujących,

— zapewniają umieszczenie klucza Km_{WC} we wszystkich kartach warsztatowych `SensorInstallationSecData` w pliku elementarnym `Sensor_Installation_Data` w czasie personalizacji kart.

3.1.4 *Generowanie i dystrybucja kluczy sesji T-DES*

CSM_012 W ramach procesu wzajemnego uwierzytelnienia przyrządy rejestrujące i karty do tachografu generują i wymieniają niezbędne dane w celu uzyskania wspólnego klucza sesji Triple DES. Poufność tej wymiany informacji jest chroniona mechanizmem kryptograficznym RSA.

CSM_013 Klucz ten stosuje się we wszystkich późniejszych czynnościach kryptograficznych, używając bezpiecznej wymiany komunikatów. Ważność tego klucza wygasa z końcem sesji (wyjęcie karty lub wyzerowanie karty) lub po 240 użyciach (jedno użycie klucza = jedno polecenie używające bezpiecznej wymiany komunikatów wysłane do karty i związana z nim odpowiedź).

3.2. **Klucze**

CSM_014 Długości kluczy RSA (niezależnie od poziomu) są następujące: moduł *n* 1 024 bity, wykładnik publiczny *e* maksymalnie 64 bity, wykładnik prywatny *d* 1 024 bity.

CSM_015 Klucze Triple DES mają postać (K_a, K_b, K_a), gdzie K_a i K_b są niezależnymi 64-bitowymi kluczami. Nie dopuszcza się możliwości ustawiania jakichkolwiek bitów wykrywania błędu parzystości.

3.3. **Certyfikaty**

CSM_016 Certyfikaty klucza publicznego RSA są certyfikatami „niesamoopisującymi", weryfikowalnymi przez kartę (CVC) (zob. norma ISO/IEC 7816-8).

3.3.1 *Treść certyfikatów*

CSM_017 Certyfikaty klucza publicznego RSA zawierają następujące dane w określonym poniżej porządku:

Dane	Format	Bajty	Opis
CPI	INTEGER	1	Identyfikator profilu certyfikatu („01” dla tej wersji)
CAR	OCTET STRING	8	Odniesienie do organu certyfikacji
CHA	OCTET STRING	7	upoważnienie posiadacza certyfikatu
EOV	TimeReal	4	Koniec terminu ważności certyfikatu. Opcjonalny, gdy nieużywany, wypełniony „FF”.
CHR	OCTET STRING	8	odniesienie do posiadacza certyfikatu
n	OCTET STRING	128	Klucz publiczny (moduł)
e	OCTET STRING	8	Klucz publiczny (wykładnik publiczny)
		164	

Uwagi:

1. „Identyfikator profilu certyfikatu” (CPI) wyznacza dokładną strukturę certyfikatu uwierzytelniania. Można go używać jako wewnętrznego identyfikatora urządzenia w odpowiednim wykazie nagłówków, który opisuje konkatenację elementów danych w certyfikacie.

   Wykaz nagłówków związanych z treścią certyfikatu jest następujący:

‘4D’	‘16’	‘5F 29’	‘01’	‘42’	‘08’	‘5F 4B’	‘07’	‘5F 24’	‘04’	‘5F 20’	‘08’	‘7F 49’	‘05’	‘81’	‘81 80’	‘82’	‘08’
Znacznik rozszerzonego wykazu nagłówków	Długość wykazu nagłówków	Znacznik CPI	Długość CPI	Znacznik CAR	Długość CAR	Znacznik CHA	Długość CHA	Znacznik EOV	Długość EOV	Znacznik CHR	Długość CHR	Znacznik klucza publicznego (zbudowany)	Długość następnych DO	Znacznik modułu	Długość modułu	Znacznik wykładnika publicznego	Długość wykładnika publicznego

2. „Odniesienie do organu certyfikacji” (CAR) ma na celu identyfikację organu certyfikacji wydającego certyfikat, w taki sposób, że ten element danych może być użyty jednocześnie jako identyfikator klucza organu w celu odniesienia do klucza publicznego organu certyfikacji (kodowanie — patrz Identyfikator klucza poniżej).

3. „Upoważnienie posiadacza certyfikatu" (CHA) służy do identyfikowania praw posiadacza certyfikatu. Składa się ono z ID aplikacji tachograficznej i typu urządzenia, dla którego certyfikat jest przeznaczony (zgodnie z elementem danych `EquipmentType`, „00" dla państwa członkowskiego).

4. „Odniesienie do posiadacza certyfikatu" (CHR) ma na celu jednoznaczną identyfikację posiadacza certyfikatu, w taki sposób, że ten element danych może być użyty jednocześnie jako identyfikator klucza podmiotu w celu odniesienia do posiadacza certyfikatu klucza publicznego.

5. Identyfikatory kluczy jednoznacznie identyfikują posiadacza certyfikatu lub organy certyfikacji. Są one kodowane w następujący sposób:

5.1. Urządzenie (VU lub karta):

Dane	Numer seryjny urządzenia	Data	Typ	Producent
Długość	4 bajty	2 bajty	1 bajt	1 bajt
Wartość	liczba całkowita	kodowanie BCD mm rr	specyficzny dla producenta	kod producenta

W przypadku VU producent, gdy wnioskuje o certyfikaty, może, ale nie musi, znać identyfikację urządzenia, w którym mają być umieszczone klucze.

W pierwszym przypadku producent wysyła identyfikację urządzenia z kluczem publicznym do organu swojego państwa członkowskiego w celu certyfikacji. W tym przypadku certyfikat będzie zawierał identyfikację urządzenia i producent musi zapewnić umieszczenie kluczy i certyfikatu w przewidzianym urządzeniu. Identyfikator klucza ma przedstawioną powyżej postać.

W drugim przypadku producent musi tylko jednoznacznie zidentyfikować każdy wniosek o certyfikat i wysłać tę identyfikację z kluczem publicznym do organu swojego państwa członkowskiego w celu certyfikacji. W tym przypadku certyfikat będzie zawierał wnioskowaną identyfikację. Po zainstalowaniu klucza w urządzeniu producent musi zawiadomić zwrotnie organ swojego państwa członkowskiego o przyporządkowaniu klucza do urządzenia (tj. podać identyfikację wniosku o certyfikat, identyfikację urządzenia). Identyfikator klucza ma następującą postać:

Dane	Numer seryjny wniosku o certyfikat	Data	Typ	Producent
Długość	4 bajty	2 bajty	1 bajt	1 bajt
Wartość	liczba całkowita	kodowanie BCD mm rr	'FF'	kod producenta

5.2. Organ certyfikacji:

Dane	Identyfikacja organu	Numer seryjny klucza	Dodatkowe informacje	Identyfikator
Długość	4 bajty	1 bajt	2 bajty	1 bajt

Wartość	1-bajtowy kod numeryczny państwa 3-bajtowy kod alfanumeryczny państwa	liczba całkowita	dodatkowe kodowanie (specyficzne dla CA) 'FF FF', gdy nie jest używany	'01'

Numer seryjny klucza służy do rozróżniania różnych kluczy państwa członkowskiego w przypadku zmiany klucza.

6. Weryfikatory certyfikatów wiedzą niejawnie o tym, iż certyfikowany klucz publiczny jest kluczem RSA właściwym do uwierzytelnienia, weryfikacji podpisu cyfrowego i szyfrowania dla poufnych usług (certyfikat nie zawiera identyfikatora obiektu, który by to określał).

3.3.2 *Wydane certyfikaty*

CSM_018 Wydany certyfikat jest podpisem cyfrowym z częściowym odzyskiwaniem treści certyfikatu zgodnie z normą ISO/IEC 9796-2 (z wyjątkiem jego załącznika A4) z dołączonym „odniesieniem do organu certyfikacji".

$$X.C = X.CA.SK['6A' \,||\, C_r \,||\, \mathit{Hash}(Cc) \,||\, 'BC'] \,||\, C_n \,||\, X.CAR$$

z treścią certyfikatu = Cc = C_r || C_n

106 bajtów 58 bajtów

Uwagi:

1. Ten certyfikat zawiera 194 bajty.

2. CAR, utajniony podpisem, jest również dołączony do podpisu, w związku z czym do weryfikacji certyfikatu można wybrać klucz publiczny organu certyfikacji.

3. Weryfikator certyfikatu zna niejawnie algorytm użyty przez organ certyfikacji do podpisania certyfikatu.

4. Wykaz nagłówków związanych z wydanym certyfikatem jest następujący:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Znacznik certyfikatu CV (zbudowany)	Długość następnych DO	Znacznik podpisu	Długość podpisu	Znacznik reszty	Długość reszty	Znacznik CAR	Długość CAR

3.3.3 *Weryfikacja i rozpakowanie certyfikatu*

Weryfikacja i rozpakowanie certyfikatu obejmuje sprawdzenie podpisu zgodnie z normą ISO/IEC 9796-2, odzyskanie treści certyfikatu i klucza publicznego: X.PK = X.CA.PK ₒ X.C. oraz sprawdzenie ważności certyfikatu.

CSM_019 Procedura ta składa się z następujących etapów:

weryfikacja podpisu i odzyskanie treści:

— z X.C odzyskaj Sign, C_n‘ i CAR’:

X.C =	Sign	||	C_n‘	||	CAR’
	128 bajtów		58 bajtów		8 bajtów

— z CAR’ wybierz odpowiednio klucz publiczny organu certyfikacji (jeżeli nie uzyskano go wcześniej innymi środkami)

— odtwórz Sign z klucza publicznego CA: Sr’= X.CA.PK [Sign]

— sprawdź, czy Sr’ zaczyna się od ‘6A’ i kończy na ‘BC’

— oblicz C_r’ i H’ z: Sr’ =

‘6A’	||	C_r’	||	H’	||	‘BC’
		106 bajtów		20 bajtów		

— odzyskaj treść certyfikatu C’ = C_r‘ || C_n’

— sprawdź, czy *Hash*(C’) = H’

Jeżeli rezultat kontroli będzie prawidłowy, certyfikat jest prawdziwy, a jego treść to C’.

Sprawdzenie ważności z C’:

— w stosownych przypadkach sprawdź koniec daty ważności,

odzyskaj i zachowaj klucz publiczny, identyfikator klucza, upoważnienie posiadacza certyfikatu i koniec ważności certyfikatu z C’:

— X.PK = *n* || *e*

— X.KID = CHR

— X.CHA = CHA

— X.EOV = EOV

4. MECHANIZM WZAJEMNEGO UWIERZYTELNIENIA

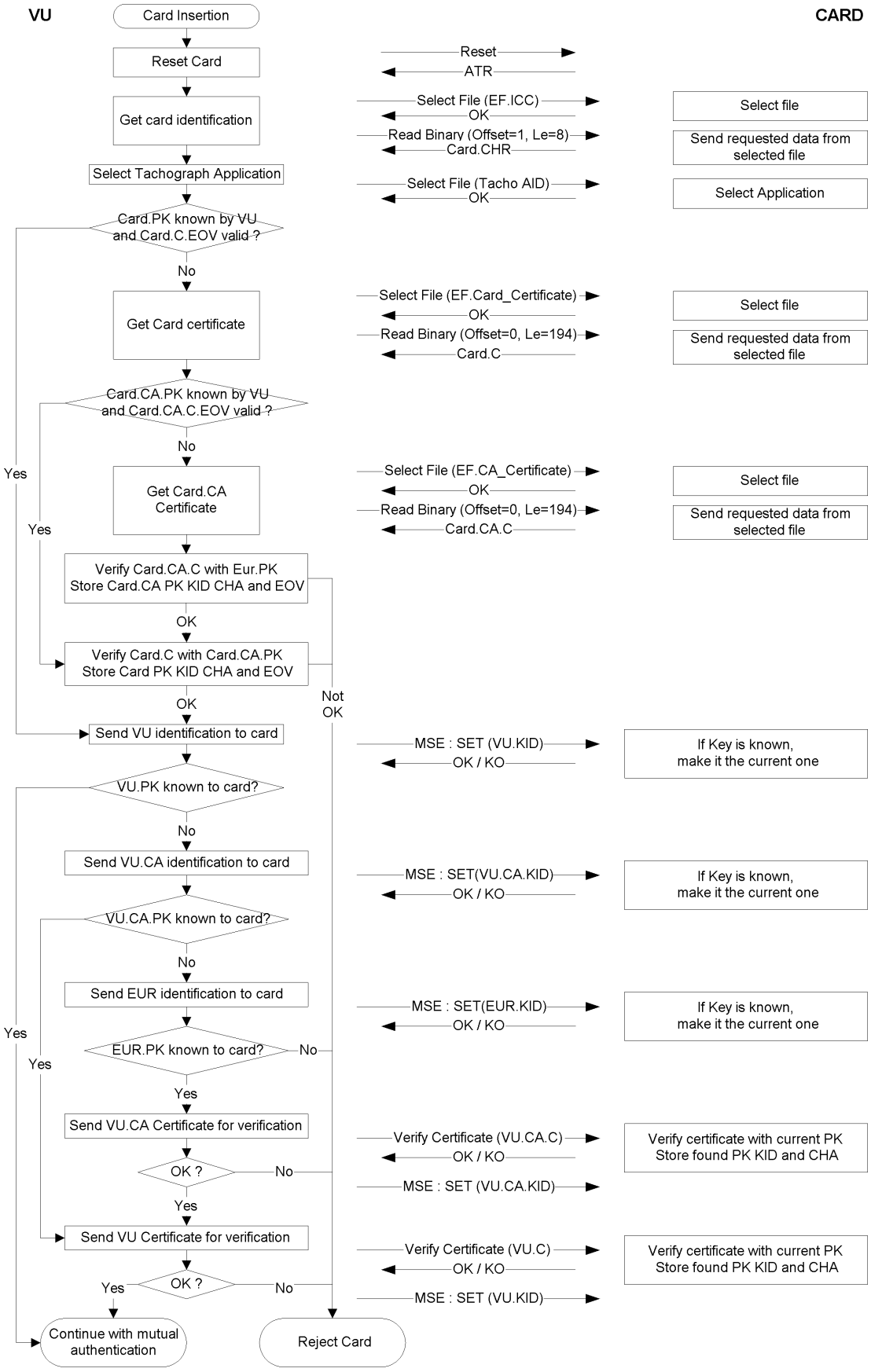
Wzajemne uwierzytelnienie między kartami a VU odbywa się według opisanej poniżej zasady.

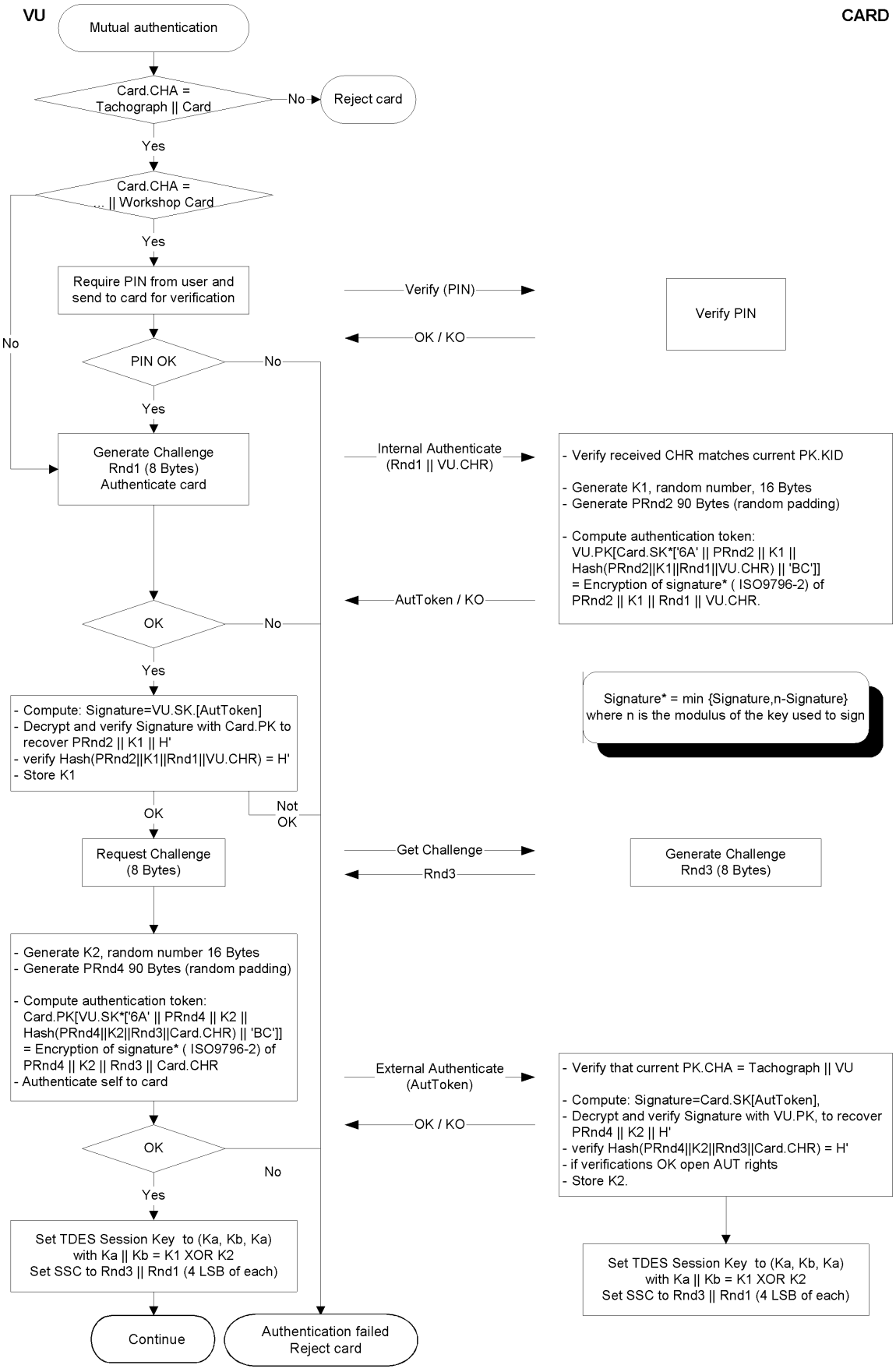
Każda strona wykazuje drugiej, że posiada ważną parę kluczy, z której klucz publiczny jest certyfikowany przez organ certyfikacji państwa członkowskiego, który uzyskał certyfikat wydany przez europejski organ certyfikacji.

Wykazanie polega na podpisaniu kluczem prywatnym losowej liczby przysłanej przez drugą stronę, która musi odzyskać tę liczbę przy sprawdzaniu tego podpisu.

Mechanizm zostaje uruchomiony przez VU w chwili włożenia karty. Procedura rozpoczyna się od wymiany certyfikatów i rozpakowania kluczy, a kończy ustaleniem klucza sesji.

CSM_020 W procesie tym stosuje się następujący protokół (strzałki oznaczają polecenia i wymianę danych (zob. dodatek 2)):




VU
CARD
Mutual authentication
Card.CHA = Tachograph || Card
No
Reject card
Yes
Card.CHA = ... || Workshop Card
Yes
Require PIN from user and send to card for verification
Verify (PIN)
Verify PIN
OK / KO
No
PIN OK
No
Yes
Generate Challenge Rnd1 (8 Bytes) Authenticate card
Internal Authenticate (Rnd1 || VU.CHR)
- Verify received CHR matches current PK.KID
- Generate K1, random number, 16 Bytes
- Generate PRnd2 90 Bytes (random padding)
- Compute authentication token: VU.PK[Card.SK*['6A' || PRnd2 || K1 || Hash(PRnd2||K1||Rnd1||VU.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd2 || K1 || Rnd1 || VU.CHR.
AutToken / KO
OK
No
Yes
Signature* = min {Signature,n-Signature} where n is the modulus of the key used to sign
- Compute: Signature=VU.SK.[AutToken]
- Decrypt and verify Signature with Card.PK to recover PRnd2 || K1 || H'
- verify Hash(PRnd2||K1||Rnd1||VU.CHR) = H'
- Store K1
Not OK
OK
Request Challenge (8 Bytes)
Get Challenge
Rnd3
Generate Challenge Rnd3 (8 Bytes)
- Generate K2, random number 16 Bytes
- Generate PRnd4 90 Bytes (random padding)
- Compute authentication token: Card.PK[VU.SK*['6A' || PRnd4 || K2 || Hash(PRnd4||K2||Rnd3||Card.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd4 || K2 || Rnd3 || Card.CHR
- Authenticate self to card
External Authenticate (AutToken)
- Verify that current PK.CHA = Tachograph || VU
- Compute: Signature=Card.SK[AutToken],
- Decrypt and verify Signature with VU.PK, to recover PRnd4 || K2 || H'
- verify Hash(PRnd4||K2||Rnd3||Card.CHR) = H'
- if verifications OK open AUT rights
- Store K2.
OK / KO
OK
No
Yes
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Continue
Authentication failed Reject card

5. POUFNOŚĆ, INTEGRALNOŚĆ I MECHANIZMY UWIERZYTELNIANIA PRZESYŁANIA DANYCH MIĘDZY VU A KARTAMI

5.1. **Bezpieczna wymiana komunikatów**

CSM_021 Bezpieczna wymiana komunikatów chroni integralność przesyłania danych między VU a kartami zgodnie z odniesieniami [ISO/IEC 7816-4] i [ISO/IEC 7816-8].

CSM_022 W przypadku konieczności zapewnienia ochrony przesyłanych danych do obiektów danych wysyłanych w poleceniu lub odpowiedzi dołącza się obiekt danych z kryptograficzną sumą kontrolną. Kryptograficzną sumę kontrolną weryfikuje odbiorca.

CSM_023 Kryptograficzna suma kontrolna danych wysyłanych w poleceniu integruje nagłówek polecenia i wszystkie wysyłane obiekty danych (=>CLA = '0C', a wszystkie obiekty danych są ograniczone znacznikami, w których b1=1).

CSM_024 Bajty stanu odpowiedzi-informacji są chronione kryptograficzną sumą kontrolną, jeżeli odpowiedź nie zawiera żadnego pola danych.

CSM_025 Kryptograficzne sumy kontrolne składają się z 4 bajtów.

W związku z tym struktura poleceń i odpowiedzi w ramach bezpiecznej wymiany komunikatów przedstawia się w następujący sposób:

Wykorzystywane DO stanowią częściowy zbiór DO stosowanych w ramach bezpiecznej wymiany komunikatów, o których mowa w normie ISO/IEC 7816-4:

Znacznik	Mnemonik	Znaczenie
'81'	T_{PV}	Odkryta wartość danych niekodowanych w BER-TLV (chroniona przez kryptograficzną sumę kontrolną)
'97'	**T_{LE}**	Wartość Le w niezabezpieczonym poleceniu (chroniona przez kryptograficzną sumę kontrolną)
'99'	T_{SW}	Stan-Info (chronione przez kryptograficzną sumę kontrolną)
'8E'	T_{CC}	Kryptograficzna suma kontrolna
'87'	$T_{PI\ CG}$	Bajt wskaźnika wypełnienia || Kryptogram (odkryta wartość niekodowana w BER-TLV)

Dla danej pary niezabezpieczone polecenie – odpowiedź:

Nagłówek polecenia				Treść polecenia		
CLA	INS	P1	P2	[Pole L_c]	[Pole danych]	[Pole L_e]
cztery bajty				Bajty L, oznaczone od B_1 do B_L		

Treść odpowiedzi	Stopka odpowiedzi	
[Pole danych]	SW1	SW2
Bajty danych L_r	dwa bajty	

Odpowiadająca para zabezpieczone polecenie – odpowiedź jest następująca:

Zabezpieczone polecenie:

Nagłówek polecenia (CH)				Treść polecenia										
CLA	INS	P1	P2	[Nowe pole L_c]	[Nowe pole danych]									[Nowe pole L_e]
'OC'				Długość nowego pola danych	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	'00'
					'81'	L_c	pole danych	'97'	'01'	L_e	'8E'	'04'	CC	

Dane zintegrowane w sumie kontrolnej = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = bajty wypełnienia (80 .. 00) zgodnie z normami ISO-IEC 7816-4 i ISO 9797 metoda 2.

Obiekty DO PV i LE występują tylko wtedy, gdy są pewne odpowiadające im dane w niezabezpieczonym poleceniu.

Zabezpieczona odpowiedź:

1. Przypadek, gdy pole danych odpowiedzi nie jest puste i nie wymaga ochrony poufności:

Treść odpowiedzi						Stopka odpowiedzi
[Nowe pole danych]						nowe SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
'81'	L_r	pole danych	'8E'	'04'	CC	

Dane zintegrowane w sumie kontrolnej = T_{PV} || L_{PV} || PV || PB

2. Przypadek, gdy pole danych odpowiedzi nie jest puste i wymaga ochrony poufności:

Treść odpowiedzi						Stopka odpowiedzi
[Nowe pole danych]						nowe SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
'87'		PI || CG	'8E'	'04'	CC	

Dane przenoszone przez CG: dane niekodowane w BER-TLV i bajty wypełnienia.

Dane zintegrowane w sumie kontrolnej = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Przypadek, gdy pole danych odpowiedzi jest puste:

Treść odpowiedzi						Stopka odpowiedzi
[Nowe pole danych]						nowe SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
'99'	'02'	nowe SW1 SW2	'8E'	'04'	CC	

Dane zintegrowane w sumie kontrolnej = T_{SW} || L_{SW} || SW || PB

5.2. **Obsługa błędów w bezpiecznej wymianie komunikatów**

CSM_026 Gdy karta do tachografu wykryje błąd SM podczas interpretowania polecenia, w odpowiedzi musi zwrócić bajty stanu bez SM. Zgodnie z normą ISO/IEC 7816-4 błędy SM wskazuje się następującymi bajtami stanu:

'66 88': błąd weryfikacji kryptograficznej sumy kontrolnej,

'69 87': brak oczekiwanych obiektów danych SM,

'69 88': nieprawidłowe obiekty danych SM.

CSM_027 W przypadku gdy karta do tachografu zwraca bajty stanu bez obiektów danych SM lub z błędnym obiektem danych SM, VU musi przerwać sesję.

5.3. **Algorytm obliczania kryptograficznych sum kontrolnych**

CSM_028 Kryptograficzne sumy kontrolne tworzy się za pomocą jednokierunkowej funkcji skrótu MAC zgodnie z normą ANSI X9.19 z DES:

— etap początkowy: początkowy blok kontrolny y0 jest E(Ka, SSC),

— etap sekwencyjny: bloki kontrolne y1,…, yn oblicza się za pomocą Ka,

— etap końcowy: kryptograficzną sumę kontrolną oblicza się z ostatniego bloku yn jako: E(Ka, D (Kb, yn)),

gdzie E() oznacza szyfrowanie z DES, a D() oznacza deszyfrowanie z DES.

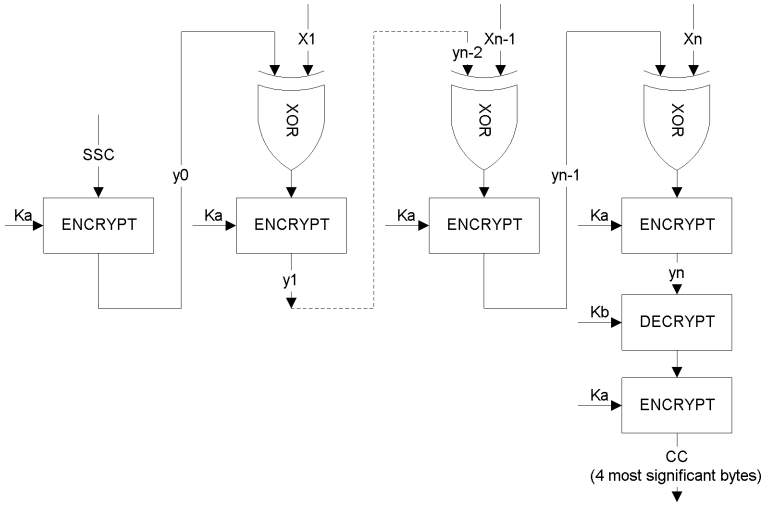
Cztery najbardziej znaczące bajty kryptograficznej sumy kontrolnej są przesyłane.

CSM_029 Licznik sekwencji wysyłania (SSC) jest inicjowany podczas procedury uzgadniania klucza:

początkowy SSC: Rnd3 (4 najmniej znaczące bajty) || Rnd1 (4 najmniej znaczące bajty).

CSM_030 Licznik SSC zwiększa się za każdym razem o 1 przed obliczeniem MAC (tj. SSC dla pierwszego polecenia będzie początkowy SSC + 1, SSC dla pierwszej odpowiedzi będzie początkowy SSC + 2).

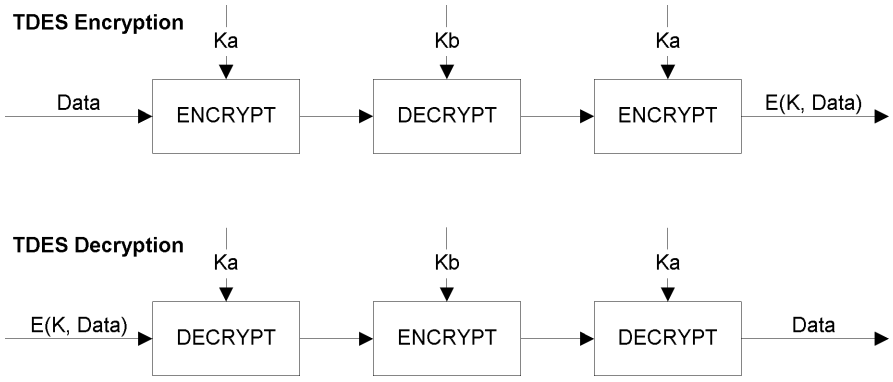
Na poniższym rysunku pokazano obliczenie skrótu MAC:



5.4. **Algorytm obliczania kryptogramów dla poufnych obiektów danych**

CSM_031 Kryptogramy oblicza się za pomocą TDEA w trybie pracy TCBC zgodnie z odniesieniami (TDES) i (TDES-OP) i wektorem zerowym jako blokiem wartości początkowych.

Na poniższym rysunku pokazano zastosowanie kluczy w TDES:



6. MECHANIZMY CYFROWEGO PODPISU DLA POBIERANIA DANYCH

CSM_032 Inteligentne urządzenie dedykowane (IDE) przechowuje dane otrzymane z urządzenia (VU lub karty) podczas jednej sesji pobierania w jednym fizycznym pliku danych. Plik ten musi zawierać certyfikaty MSi.C i EQT.C. Plik zawiera podpisy cyfrowe bloków danych zgodnie z opisem znajdującym się w dodatku 7 Protokoły pobierania danych.

CSM_033 Podpisy cyfrowe pobranych danych korzystają ze schematu podpisu cyfrowego z dodatkiem, przy czym, w razie potrzeby, pobrane dane można odczytać bez deszyfrowania.

6.1. **Generowanie podpisu**

CSM_034 Urządzenie generuje podpis danych zgodnie ze schematem podpisu z dodatkiem zdefiniowanym w odniesieniu [PKCS1] z funkcją skrótu SHA-1:

Podpis = EQT.SK[‘00’ || ‘01’ || *PS* || ‘00’ || DER(SHA-1(Data))]

PS = Wypełnienie ciągiem oktetów o wartości 'FF' do długości 128.

DER(SHA-1(*M*)) to kodowanie identyfikatora algorytmu dla funkcji skrótu, a wartość skrótu jest wartością w ASN.1 typu DigestInfo (wyróżnione reguły kodowania):

'30'||'21'||'30'||'09'||'06'||'05'||'2B'||'0E'||'03'||'02'||'1A'||'05'||'00'||'04'||'14'||wartość skrótu.

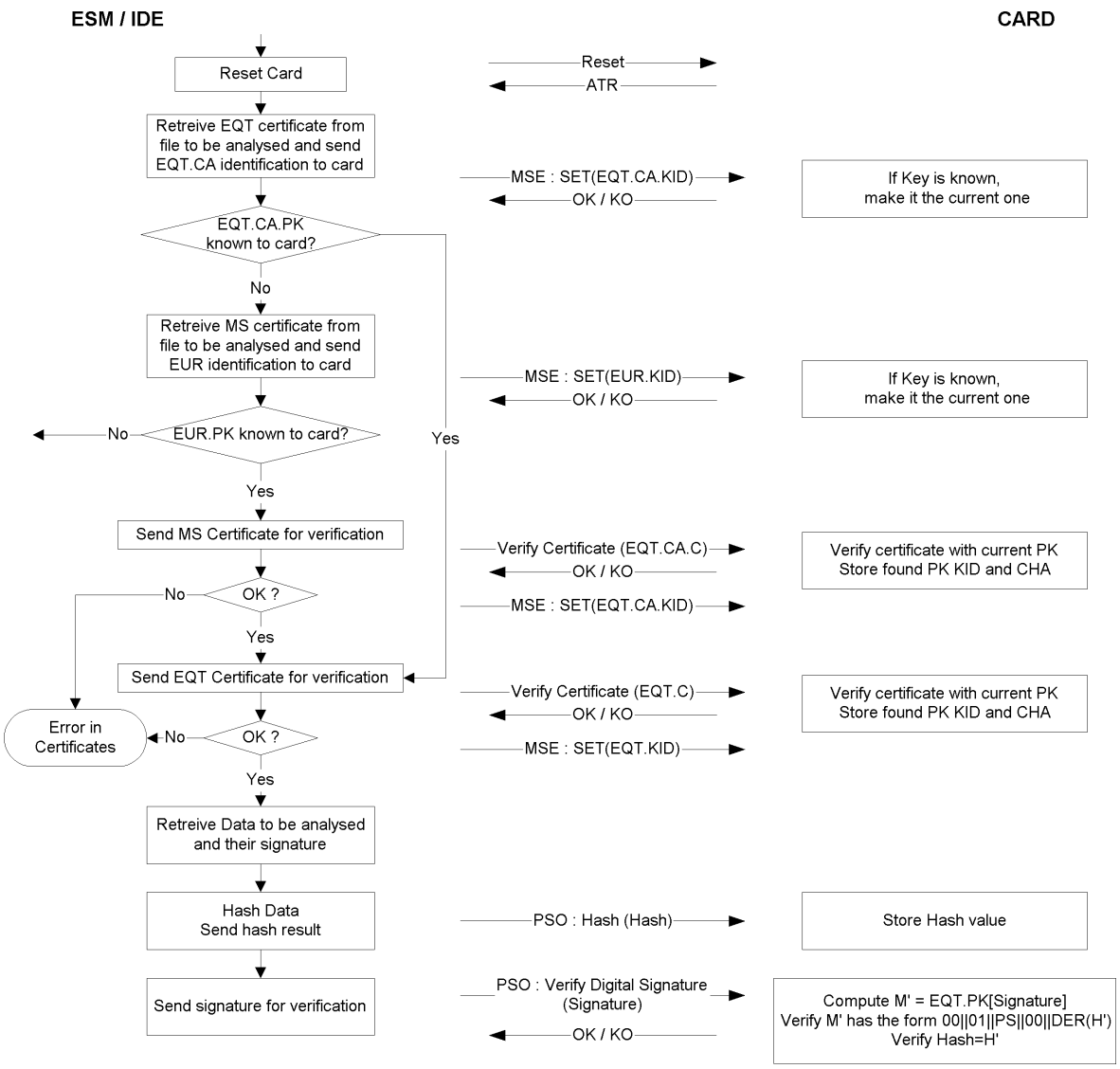
6.2. **Weryfikacja podpisu**

CSM_035 Weryfikacja podpisu danych dla pobranych danych odbywa się zgodnie ze schematem podpisu z dodatkiem zdefiniowanym w odniesieniu (PKCS1) z funkcją skrótu SHA-1.

Europejski klucz publiczny EUR.PK musi być niezależnie znany (i zaufany) przez weryfikatora.

Na schemacie poniżej zilustrowano protokół przenoszenia IDE, z którego może korzystać karta kontrolna przy sprawdzaniu integralności danych pobranych i zapisanych na zewnętrznym nośniku danych (ESM). Karta kontrolna służy do deszyfrowania podpisów cyfrowych. W tym przypadku ta funkcja nie musi być zaimplementowana w IDE.

Urządzenie, które pobiera i podpisuje dane przeznaczone do analizowania, oznaczono EQT.



CZĘŚĆ B

SYSTEM TACHOGRAFU DRUGIEJ GENERACJI

7. WPROWADZENIE

7.1. **Odniesienia**

W tej części dodatku używa się następujących odniesień:

AES	Narodowy Instytut Standaryzacji i Technologii (NIST), FIPS Publikacja 197: Symetryczny szyfr blokowy (AES), 26 listopada 2001 r.
DSS	Narodowy Instytut Standaryzacji i Technologii (NIST), FIPS Publikacja 186-4: Standard podpisu cyfrowego (DSS), lipiec 2013 r.
ISO 7816-4	ISO/IEC 7816-4, Karty identyfikacyjne – Karty elektroniczne – Część 4: Organizacja, zabezpieczenia i polecenia wymiany. Wydanie trzecie 2013-04-15
ISO 7816-8	ISO/IEC 7816-8, Karty identyfikacyjne – Karty elektroniczne – Część 8: Polecenia operacji zabezpieczających. Wydanie drugie, 2004-06-01
ISO 8825-1	ISO/IEC 8825-1 Technologia informacyjna – Reguły kodowania ASN.1: Specyfikacja podstawowych reguł kodowania (BER), kanonicznych reguł kodowania (CER) i wyróżnionych reguł kodowania (DER). Wydanie czwarte, 2008-12-15.
ISO 9797-1	ISO/IEC 9797-1, Technologia informacyjna – Techniki zabezpieczeń – Kody uwierzytelniania komunikatów (MAC) – Część 1: Mechanizmy stosujące szyfr blokowy. Wydanie drugie, 2011-03-01
ISO 10116	ISO/IEC 10116, Technologia informacyjna – Techniki zabezpieczeń – Tryby pracy algorytmu szyfrowania bloków n-bitowych. Wydanie trzecie, 2006-02-01
ISO 16844-3	ISO 16844-3, Pojazdy drogowe – Systemy tachograficzne – Część 3: Interfejs czujnika ruchu. Wydanie pierwsze z 2004 r., w tym sprostowanie techniczne 1 z 2006 r.
RFC 5480	Kryptografia oparta na krzywej eliptycznej – Informacje na temat klucza publicznego podmiotu, marzec 2009 r.
RFC 5639	Kryptografia oparta na krzywej eliptycznej (ECC) – Standardowe krzywe Brainpool i generowanie krzywych, 2010 r.
RFC 5869	Funkcja wyprowadzania klucza przez wyodrębnianie i rozwijanie oparta na algorytmie HMAC (HKDF), maj 2010 r.
SHS	Narodowy Instytut Standaryzacji i Technologii (NIST), FIPS Publikacja 180-4: Bezpieczny standard skrótu, marzec 2012 r.
SP 800-38B	Narodowy Instytut Standaryzacji i Technologii (NIST), Specjalna publikacja 800-38B: Zalecenie dotyczące trybów pracy szyfru blokowego: tryb uwierzytelniania CMAC, 2005 r.
TR-03111	Wytyczne techniczne BSI TR-03111, Kryptografia oparta na krzywej eliptycznej, wersja 2.00, 2012-06-28

7.2. **Oznaczenia i skróty**

W niniejszym dodatku używa się następujących oznaczeń i skrótów:

AES	symetryczny szyfr blokowy
CA	organ certyfikacji
CAR	odniesienie do organu certyfikacji
CBC	tryb wiązania bloków zaszyfrowanych (tryb pracy)

CH	nagłówek polecenia
CHA	upoważnienie posiadacza certyfikatu
CHR	odniesienie do posiadacza certyfikatu
CV	wektor stały
DER	wyróżnione reguły kodowania
DO	obiekt danych
DSRC	dedykowana łączność krótkiego zasięgu
ECC	kryptografia oparta na krzywej eliptycznej
ECDSA	algorytm podpisu cyfrowego krzywej eliptycznej
ECDH	krzywa eliptyczna Diffiego-Hellmana (algorytm uzgadniania klucza)
EGF	urządzenie zewnętrzne GNSS
EQT	urządzenia
IDE	inteligentne urządzenie dedykowane
K_M	klucz główny czujnika ruchu umożliwiający sparowanie przyrządu rejestrującego z czujnikiem ruchu
K_{M-VU}	klucz umieszczony w przyrządach rejestrujących, umożliwiający VU wyprowadzenie klucza głównego czujnika ruchu, jeżeli karta warsztatowa została włożona do VU
K_{M-WC}	klucz umieszczony w kartach warsztatowych, umożliwiający VU wyprowadzenie klucza głównego czujnika ruchu, jeżeli karta warsztatowa została włożona do VU
MAC	kod uwierzytelniania komunikatów
MoS	czujnik ruchu
MSB	najbardziej znaczący bit
PKI	infrastruktura klucza publicznego
RCF	urządzenie do łączności na odległość
SSC	licznik sekwencji wysyłania
SM	bezpieczna wymiana komunikatów
TDES	potrójny algorytm DES
TLV	obiekt TLV (Tag-Length-Value)
VU	przyrząd rejestrujący
X.C	certyfikat klucza publicznego użytkownika X
X.CA	organ certyfikacji, który wydał certyfikat użytkownika X
X.CAR	odniesienie do organu certyfikacji, o którym mowa w certyfikacie użytkownika X
X.CHR	odniesienie do posiadacza certyfikatu, o którym mowa w certyfikacie użytkownika X
X.PK	klucz publiczny użytkownika X
X.SK	klucz prywatny użytkownika X
$X.PK_{eph}$	efemeryczny klucz publiczny użytkownika X
$X.SK_{eph}$	efemeryczny klucz prywatny użytkownika X
‘xx’	wartość heksadecymalna
||	operator konkatenacji

7.3. **Definicje**

Definicje terminów stosowanych w niniejszym dodatku włączono do sekcji I załącznika 1C.

8. SYSTEMY I ALGORYTMY KRYPTOGRAFICZNE

8.1. **Systemy kryptograficzne**

CSM_38 Przyrządy rejestrujące i karty do tachografu używają systemu kryptograficznego opartego na krzywej eliptycznej z kluczem publicznym do zapewniania następujących usług zabezpieczających:

— wzajemne uwierzytelnienie między przyrządem rejestrującym a kartą,

— zgodność kluczy sesji AES między przyrządem rejestrującym a kartą,

— zapewnienie autentyczności, integralności i niezaprzeczalności danych pobranych z przyrządów rejestrujących lub kart do tachografu do zewnętrznych nośników.

CSM_39 Przyrządy rejestrujące i zewnętrzne urządzenia GNSS używają systemu kryptograficznego opartego na krzywej eliptycznej z kluczem publicznym do zapewniania następujących usług zabezpieczających:

— powiązanie między przyrządem rejestrującym a urządzeniem zewnętrznym GNSS,

— wzajemne uwierzytelnienie między przyrządem rejestrującym a urządzeniem zewnętrznym GNSS,

— zgodność klucza sesji AES między przyrządem rejestrującym a urządzeniem zewnętrznym GNSS.

CSM_40 Przyrządy rejestrujące i karty do tachografu używają symetrycznego systemu kryptograficznego opartego na AES do zapewniania następujących usług zabezpieczających:

— zapewnienie autentyczności i integralności danych wymienianych między przyrządem rejestrującym a kartą do tachografu,

— w stosownych przypadkach zapewnienie poufności danych wymienianych między przyrządem rejestrującym a kartą do tachografu.

CSM_41 Przyrządy rejestrujące i urządzenia zewnętrzne GNSS używają symetrycznego systemu kryptograficznego opartego na AES do zapewniania następujących usług zabezpieczających:

— zapewnienie autentyczności i integralności danych wymienianych między przyrządem rejestrującym a urządzeniem zewnętrznym GNSS.

CSM_42 Przyrządy rejestrujące i czujniki ruchu używają symetrycznego systemu kryptograficznego opartego na AES do zapewniania następujących usług zabezpieczających:

— sparowanie przyrządu rejestrującego z czujnikiem ruchu,

— wzajemne uwierzytelnienie między przyrządem rejestrującym a czujnikiem ruchu,

— zapewnienie poufności danych wymienianych między przyrządem rejestrującym a czujnikiem ruchu.

CSM_43 Przyrządy rejestrujące i karty kontrolne używają symetrycznego systemu kryptograficznego opartego na AES do zapewniania następujących usług zabezpieczających na interfejsie łączności na odległość:

— zapewnienie poufności, autentyczności i integralności danych przekazywanych z przyrządu rejestrującego do karty kontrolnej.

Uwagi

— Ściśle rzecz ujmując, dane przekazywane z przyrządu rejestrującego do zdalnego interrogatora pod nadzorem funkcjonariusza służb kontrolnych, za pomocą urządzenia do łączności na odległość, które może znajdować się wewnątrz lub na zewnątrz VU, zob. dodatek 14. Zdalny interrogator wysyła jednak otrzymane dane do karty kontrolnej w celu deszyfrowania i potwierdzenia autentyczności. Z punktu widzenia bezpieczeństwa urządzenie do łączności na odległość i zdalny interrogator cechują się pełną przejrzystością.

— Karta warsztatowa zapewnia interfejsowi DSRC takie same usługi zabezpieczające jak karta kontrolna. Dzięki temu warsztat może zatwierdzać prawidłowe funkcjonowanie interfejsu łączności na odległość VU, z uwzględnieniem bezpieczeństwa. Więcej informacji można znaleźć w sekcji 9.2.2.

8.2. Algorytmy kryptograficzne

8.2.1 *Algorytmy symetryczne*

CSM_44 Przyrządy rejestrujące, karty do tachografu, czujniki ruchu i urządzenia zewnętrzne GNSS obsługują algorytm AES, jak określono w [AES], o długościach klucza wynoszących 128, 192 i 256 bitów.

8.2.2 *Algorytmy asymetryczne i standardowe parametry domeny*

CSM_45 Przyrządy rejestrujące, karty do tachografu i urządzenia zewnętrzne GNSS obsługują kryptografię opartą na krzywej eliptycznej z kluczami o wielkości 256, 384 i 512/521 bitów.

CSM_46 Przyrządy rejestrujące, karty do tachografu i urządzenia zewnętrzne GNSS obsługują algorytm podpisywania ECDSA, jak określono w [DSS].

CSM_47 Przyrządy rejestrujące, karty do tachografu i urządzenia zewnętrzne GNSS obsługują algorytm uzgadniania klucza ECKA-EG, jak określono w [TR 03111].

CSM_48 Przyrządy rejestrujące, karty do tachografu i urządzenia zewnętrzne GNSS obsługują wszystkie standardowe parametry domeny określone w tabeli 1 poniżej w odniesieniu do kryptografii opartej na krzywej eliptycznej.

Tabela 1

Standardowe parametry domeny

Nazwa	Wielkość (bity)	Odniesienie	Identyfikator obiektu
NIST P-256	256	[DSS], [RFC 5480]	`secp256r1`
BrainpoolP256r1	256	[RFC 5639]	`brainpoolP256r1`
NIST P-384	384	[DSS], [RFC 5480]	`secp384r1`
BrainpoolP384r1	384	[RFC 5639]	`brainpoolP384r1`
BrainpoolP512r1	512	[RFC 5639]	`brainpoolP512r1`
NIST P-521	521	[DSS], [RFC 5480]	`secp521r1`

Uwaga: identyfikatory obiektu wspomniane w ostatniej kolumnie tabeli 1 są określone w [RFC 5639] w odniesieniu do krzywych Brainpool oraz w [RFC 5480] w odniesieniu do krzywych NIST.

Przykład 1: identyfikator obiektu krzywej BrainpoolP256r1 to

```
{iso(1)
        identified-organization(3) teletrust(36) algorithm(3)
 signaturealgorithm(3) ecSign(2) ecStdCurvesAndGeneration (8)
                            ellipticCurve(1) versionOne(1) 7}.
```

Lub w zapisie kropkowym: `1.3.36.3.3.2.8.1.1.7.`

Przykład 2: identyfikator obiektu krzywej NIST P-384 to

```
{iso(1) identified-organization(3) certicom(132) curve(0) 34}.
```

Lub w zapisie kropkowym: `1.3.132.0.34.`

8.2.3 *Algorytmy skrótu*

CSM_49 Przyrządy rejestrujące i karty do tachografu obsługują algorytmy SHA-256, SHA-384 i SHA-512 określone w [SHS].

8.2.4 *Mechanizm szyfrowania*

CSM_50 W przypadku algorytmu symetrycznego stosuje się łącznie algorytm asymetryczny lub algorytm skrótu w celu utworzenia protokołu zabezpieczeń, zaś długości kluczy i wielkości skrótów obu algorytmów są (w przybliżeniu) tak samo silne. W tabeli 2 przedstawiono dozwolone mechanizmy szyfrowania:

Tabela 2

Dozwolone mechanizmy szyfrowania

Nr identyfikacyjny mechanizmu szyfrowania	Wielkość klucza ECC (bity)	Długość klucza AES (bity)	Algorytm skrótu	Długość MAC (bajty)
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Uwaga: klucze ECC o wielkości 512 i 521 bitów uznaje się za równe pod względem siły do wszystkich celów określonych w niniejszym dodatku.

9. KLUCZE I CERTYFIKATY

9.1. **Pary kluczy asymetrycznych i certyfikaty kluczy publicznych**

9.1.1 *Uwagi ogólne*

Uwaga: klucze opisane w tej sekcji wykorzystuje się do wzajemnego uwierzytelniania i bezpiecznej wymiany komunikatów między przyrządami rejestrującymi a kartami do tachografu oraz między przyrządami rejestrującymi a urządzenia zewnętrznymi GNSS. Procesy te opisano szczegółowo w rozdziałach 10 i 11 niniejszego dodatku.

CSM_51 W ramach europejskiego systemu tachografów inteligentnych pary kluczy ECC i odpowiadające im certyfikaty są generowane i zarządzane na trzech funkcjonalnych poziomach hierarchicznych:

— poziomie europejskim,

— poziomie państwa członkowskiego,

— poziomie urządzenia.

CSM_52 W ramach całego europejskiego systemu tachografów inteligentnych klucze publiczne i prywatne oraz certyfikaty są generowane, zarządzane i przekazywane za pomocą standardowych i bezpiecznych metod.

9.1.2 *Poziom europejski*

CSM_53 Na poziomie europejskim generuje się jedną unikatową parę kluczy ECC oznaczoną jako EUR. Składa się ona z klucza prywatnego (EUR.SK) i klucza publicznego (EUR.PK). Ta para kluczy tworzy parę kluczy głównych całego europejskiego systemu tachografów inteligentnych PKI. Organem realizującym to zadanie jest Główny Europejski Organ Certyfikacji (ERCA), działający z upoważnienia i na odpowiedzialność Komisji Europejskiej.

CSM_54 ERCA używa europejskiego klucza prywatnego do podpisania głównego certyfikatu (z podpisem własnym) europejskiego klucza publicznego i przekazuje ten europejski certyfikat główny wszystkim państwom członkowskim.

CSM_55 ERCA używa europejskiego klucza prywatnego do podpisywania na żądanie certyfikatów kluczy publicznych państw członkowskich. ERCA prowadzi rejestry wszystkich podpisanych certyfikatów kluczy publicznych państw członkowskich.

CSM_56 Jak przedstawiono na rys. 1 w sekcji 9.1.7, ERCA generuje nową parę europejskich kluczy głównych co 17 lat. Ilekroć ERCA generuje nową parę europejskich kluczy głównych, tworzy nowy certyfikat główny z podpisem własnym dla nowego europejskiego klucza publicznego. Okres ważności europejskiego certyfikatu głównego wynosi 34 lata i 3 miesiące.

Uwaga: wprowadzenie nowej pary kluczy głównych oznacza również, że ERCA wygeneruje nowy klucz główny czujnika ruchu i nowy klucz główny DSRC, zob. sekcje 9.2.1.2 i 9.2.2.2.

CSM_57 Przed wygenerowaniem nowej pary europejskich kluczy głównych ERCA przeprowadza analizę siły kryptograficznej, jaka jest potrzebna w odniesieniu do nowej pary kluczy, biorąc po uwagę fakt, że powinna pozostać bezpieczna przez kolejne 34 lata. W razie konieczności ERCA przechodzi na mechanizm szyfrowania, który jest mocniejszy niż obecny, jak określono wCSM_50.

CSM_58 Ilekroć ERCA generuje nową parę europejskich kluczy głównych, tworzy certyfikat łączący dla nowego europejskiego klucza publicznego i podpisuje go za pomocą poprzedniego europejskiego klucza prywatnego. Okres ważności certyfikatu łączącego wynosi 17 lat. Przedstawiono to również na rys. 1 w sekcji 9.1.7.

Uwaga: ze względu na fakt, że certyfikat łączący zawiera klucz publiczny ERCA generacji *X* i jest podpisany za pomocą klucza prywatnego ERCA generacji $X - 1$, certyfikat łączący oferuje urządzenie wydane w generacji $X - 1$, metodę potwierdzenia niezawodności urządzenia wydanego w generacji *X*.

CSM_59 ERCA nie może używać klucza prywatnego z pary kluczy głównych do jakiegokolwiek celu, po tym jak nowy certyfikat kluczy głównych stanie się ważny.

CSM_60 W każdym momencie ERCA dysponuje następującymi kluczami i certyfikatami kryptograficznymi:

— bieżąca para kluczy europejskich i powiązany certyfikat;

— wszystkie wcześniejsze certyfikaty EUR wykorzystywane do weryfikacji certyfikatów MSCA, które nadal są ważne;

— certyfikaty łączące dla wszystkich generacji certyfikatów EUR, z wyjątkiem pierwszej.

9.1.3 *Poziom państwa członkowskiego*

CSM_61 Na poziomie państwa członkowskiego wszystkie państwa członkowskie zobowiązane do podpisania certyfikatów kart do tachografu generują co najmniej jedną unikatową parę kluczy ECC oznaczoną jako MSCA_Card. Wszystkie państwa członkowskie zobowiązane do podpisania certyfikatów dla przyrządów rejestrujących lub urządzeń zewnętrznych GNSS dodatkowo generują co najmniej jedną unikatową parę kluczy ECC oznaczoną jako MSCA_VU-EGF.

CSM_62 Organem odpowiedzialnym za generowanie par kluczy państwa członkowskiego jest organ certyfikacji państwa członkowskiego (MSCA). Ilekroć MSCA generuje parę kluczy państwa członkowskiego, przesyła ERCA klucz publiczny, aby uzyskać powiązany z nim certyfikat państwa członkowskiego podpisany przez ERCA.

CSM_63 MSCA dobiera siłę pary kluczy państwa członkowskiego w taki sposób, by odpowiadała ona sile pary europejskich kluczy głównych użytej do podpisania powiązanego certyfikatu państwa członkowskiego.

CSM_64 Para kluczy MSCA_VU-EGF, jeżeli występuje, składa się z klucza prywatnego MSCA_VU-EGF.SK i klucza publicznego MSCA_VU-EGF.PK. MSCA używa klucza prywatnego MSCA_VU-EGF.SK wyłącznie do podpisywania certyfikatów klucza publicznego przyrządów rejestrujących oraz urządzeń zewnętrznych GNSS.

CSM_65 Para kluczy MSCA_Card składa się z klucza prywatnego MSCA_Card.SK i klucza publicznego MSCA_Card.PK. MSCA używa klucza prywatnego MSCA_Card.SK wyłącznie do podpisywania certyfikatów klucza publicznego kart do tachografu.

CSM_66 MSCA prowadzi rejestry wszystkich podpisanych certyfikatów VU, certyfikatów urządzeń zewnętrznych GNSS oraz certyfikatów karty i zamieszcza w nim również informacje pozwalające zidentyfikować urządzenie, dla którego wydano dany certyfikat.

CSM_67 Okres ważności certyfikatu MSCA_VU-EGF wynosi 17 lat i 3 miesiące. Okres ważności certyfikatu MSCA_Card wynosi 7 lat i 1 miesiąc.

CSM_68 Jak przedstawiono na rys. 1 w sekcji 9.1.7, okres użytkowania klucza prywatnego pary kluczy MSCA_VU-EGF i klucza prywatnego pary kluczy MSCA_Card wynosi dwa lata.

CSM_69 MSCA nie może używać klucza prywatnego wchodzącego w skład pary kluczy MSCA_VU-EGF do żadnych celów po zakończeniu okresu jego użytkowania. Podobnie MSCA nie może używać klucza prywatnego wchodzącego w skład pary kluczy MSCA_Card do żadnych celów, po zakończeniu okresu jego użytkowania.

CSM_70 W każdym momencie MSCA dysponuje następującymi kluczami i certyfikatami kryptograficznymi:

— bieżącą parą kluczy MSCA_Card i powiązanym certyfikatem;

— wszystkimi poprzednimi certyfikatami MSCA_Card, które mają służyć do weryfikacji certyfikatów kart do tachografu, które są nadal ważne;

— bieżącym certyfikatem EUR koniecznym do przeprowadzenia weryfikacji bieżącego certyfikatu MSCA;

— wszystkimi poprzednimi certyfikatami EUR koniecznymi do zweryfikowania wszystkich certyfikatów MSCA, które są nadal ważne.

CSM_71 Jeżeli MSCA jest również zobowiązana do podpisywania certyfikatów dla przyrządów rejestrujących lub urządzeń zewnętrznych GNSS, musi dodatkowo dysponować następującymi kluczami i certyfikatami:

— bieżącą parą kluczy MSCA_VU-EGF i powiązanym certyfikatem;

— wszystkimi poprzednimi kluczami publicznymi MSCA_VU-EGF, które mają służyć do weryfikacji certyfikatów VU lub urządzeń zewnętrznych GNSS, które są nadal ważne.

9.1.4 *Poziom urządzenia: przyrządy rejestrujące*

CSM_72 Dla każdego przyrządu rejestrującego generuje się dwie unikatowe pary kluczy ECC oznaczone jako VU_MA i VU_Sign. Zadanie to realizują producenci VU. Ilekroć generowana jest para kluczy VU, organ generujący klucz przekazuje klucz publiczny MSCA państwa, w którym organ ten ma swoją siedzibę, aby uzyskać powiązany certyfikat VU podpisany przez MSCA. Klucz prywatny może być używany wyłącznie przez przyrząd rejestrujący.

CSM_73 Data wejścia w życie certyfikatów VU_MA i VU_Sign danego przyrządu rejestrującego musi być taka sama.

CSM_74 Producent VU dobiera siłę pary kluczy VU w taki sposób, by odpowiadała ona sile pary kluczy MSCA użytej do podpisania powiązanego certyfikatu VU.

CSM_75 Przyrząd rejestrujący używa swojej pary kluczy VU_MA, w której skład wchodzi klucz prywatny VU_MA.SK i klucz publiczny VU_MA.PK, wyłącznie do uwierzytelnienia VU w stosunku do kart do tachografu i urządzeń zewnętrznych GNSS, jak określono w sekcjach 10.3 i 11.4 niniejszego dodatku.

CSM_76 Przyrząd rejestrujący musi mieć możliwość generowania par efemerycznych kluczy ECC i musi używać pary kluczy efemerycznych wyłącznie do przeprowadzenia operacji uzgadniania klucza sesji z kartą do tachografu lub urządzeniem zewnętrznym GNSS, jak określono w sekcjach 10.4 i 11.4 niniejszego dodatku.

CSM_77 Przyrząd rejestrujący używa klucza prywatnego VU_Sign.SK wchodzącego w skład pary kluczy VU_Sign wyłącznie do podpisywania pobranych plików danych, jak określono w rozdziale 14 niniejszego dodatku. Powiązanego klucza publicznego VU_Sign.PK używa się wyłącznie do weryfikacji podpisów wygenerowanych przez przyrząd rejestrujący.

CSM_78 Zgodnie z informacjami przedstawionymi na rys. 1 w sekcji 9.1.7 okres ważności certyfikatu VU_MA wynosi 15 lat i 3 miesiące. Okres ważności certyfikatu VU_Sign również wynosi 15 lat i 3 miesiące.

Uwagi

— Wydłużony okres ważności certyfikatu VU_Sign umożliwia przyrządowi rejestrującemu generowanie ważnych podpisów w odniesieniu do pobieranych danych przez pierwsze trzy miesiące po wygaśnięciu certyfikatu zgodnie z przepisami rozporządzenia (UE) nr 581/2010.

— Wydłużony okres ważności certyfikatu VU_MA jest potrzebny, aby umożliwić VU uwierzytelnianie karty kontrolnej lub karty firmowej w ciągu pierwszych trzech miesięcy po wygaśnięciu certyfikatu, dzięki czemu istnieje możliwość pobrania danych.

CSM_79 Przyrząd rejestrujący nie może używać klucza prywatnego wchodzącego w skład pary kluczy VU do żadnych celów po wygaśnięciu powiązanego z nim certyfikatu.

CSM_80 Par kluczy VU (z wyjątkiem par kluczy efemerycznych) i powiązanych z nimi certyfikatów danego przyrządu rejestrującego nie można zastępować ani odnawiać w warunkach polowych po rozpoczęciu eksploatacji przyrządu rejestrującego.

Uwagi

— Wymóg ten nie ma zastosowania do par kluczy efemerycznych, ponieważ VU generuje nową parę kluczy efemerycznych w ramach każdego procesu uwierzytelniania mikroprocesora i uzgadniania klucza sesji – zob. sekcja 10.4. Należy zwrócić uwagę na fakt, że pary kluczy efemerycznych nie są powiązane z żadnymi certyfikatami.

— Wymóg ten nie uniemożliwia zastąpienia statycznych par kluczy VU w trakcie modernizacji lub naprawy przeprowadzanej w bezpiecznym środowisku kontrolowanym przez producenta VU.

CSM_81 W chwili ich oddawania do eksploatacji przyrządy rejestrujące muszą zawierać następujące klucze i certyfikaty kryptograficzne:

— klucz prywatny VU_MA i powiązany certyfikat;

— klucz prywatny VU_Sign i powiązany certyfikat;

— certyfikat MSCA_VU-EGF zawierający klucz publiczny MSCA_VU-EGF.PK służący do weryfikacji certyfikatu VU_MA oraz certyfikatu VU_Sign;

— certyfikat EUR zawierający klucz publiczny EUR.PK służący do weryfikacji certyfikatu MSCA_VU-EGF;

— certyfikat EUR, którego okres ważności wygasa bezpośrednio przed okresem ważności certyfikatu EUR służącego do weryfikacji certyfikatu MSCA_VU-EGF, o ile istnieje;

— certyfikat łączący wspomniane dwa certyfikaty EUR, o ile istnieje.

CSM_82 Poza kluczami i certyfikatami kryptograficznymi wymienionymi w CSM_81 przyrządy rejestrujące muszą również zawierać klucze i certyfikaty wskazane w części A niniejszego dodatku, dzięki czemu przyrząd rejestrujący może komunikować się z kartami do tachografu pierwszej generacji.

9.1.5 *Poziom urządzenia: karty do tachografu*

CSM_83 Dla każdej karty do tachografu generuje się jedną unikatową parę kluczy ECC oznaczoną jako Card_MA. Dla każdej karty kierowcy i karty warsztatowej generuje się dodatkowo drugą unikatową parę kluczy ECC oznaczoną jako Card_Sign. Zadanie to mogą realizować producenci kart lub instytucje dokonujące personalizacji kart. Ilekroć generowana jest para kluczy karty, organ generujący klucz przekazuje klucz publiczny MSCA państwa, w którym organ ten ma swoją siedzibę, aby uzyskać powiązany certyfikat karty podpisany przez MSCA. Klucz prywatny może być używany wyłącznie przez kartę do tachografu.

CSM_84 Data wejścia w życie certyfikatów Card_MA i Card_Sign danej karty kierowcy i karty warsztatowej musi być taka sama.

CSM_85 Producent kart lub instytucja dokonująca personalizacji kart dobiera siłę par kluczy karty w taki sposób, by odpowiadała ona sile pary kluczy MSCA użytej do podpisania powiązanego certyfikatu karty.

CSM_86 Karta do tachografu używa swojej pary kluczy Card_MA, w której skład wchodzi klucz prywatny Card_MA.SK i klucz publiczny Card_MA.PK, wyłącznie do wzajemnego uwierzytelniania i uzgadniania klucza sesji w stosunku do przyrządów rejestrujących, jak określono w sekcjach 10.3 i 10.4 niniejszego dodatku.

CSM_87 Karta kierowcy lub karta warsztatowa używa klucza prywatnego Card_Sign.SK wchodzącego w skład pary kluczy Card_Sign wyłącznie do podpisywania pobranych plików danych, jak określono w rozdziale 14 niniejszego dodatku. Powiązanego klucza publicznego Card_Sign.PK używa się wyłącznie do weryfikacji podpisów wygenerowanych przez kartę.

CSM_88 Okres ważności certyfikatu Card_MA wynosi:

— w przypadku kart kierowcy: 5 lat;

— w przypadku kart firmowych: 2 lata;

— w przypadku kart kontrolnych: 2 lata;

— w przypadku kart warsztatowych: 1 rok.

CSM_89 Okres ważności certyfikatu Card_Sign wynosi:

— w przypadku kart kierowcy: 5 lat i 1 miesiąc;

— w przypadku kart warsztatowych: 1 rok i 1 miesiąc.

Uwaga: wydłużony okres ważności certyfikatu Card_Sign umożliwia karta kierowcy generowanie ważnych podpisów w odniesieniu do pobieranych danych przez pierwszy miesiąc po wygaśnięciu certyfikatu. Jest to konieczne w świetle wymogu ustanowionego w rozporządzeniu (UE) nr 581/2010, zgodnie z którym pobranie danych z karty kierowcy musi być możliwe przez okres do 28 dni od daty dokonania ostatniego zapisu danych na tej karcie.

CSM_90 Par kluczy i powiązanych certyfikatów danej karty do tachografu nie można zastępować ani odnawiać po wydaniu karty.

CSM_91 W chwili ich wydawania karty do tachografu muszą zawierać następujące klucze i certyfikaty kryptograficzne:

— klucz prywatny Card_MA i powiązany certyfikat;

— w przypadku kart kierowcy i kart warsztatowych dodatkowo: klucz prywatny Card_Sign i powiązany certyfikat;

— certyfikat MSCA_Card zawierający klucz publiczny MSCA_Card.PK służący do weryfikacji certyfikatu Card_MA oraz certyfikatu Card_Sign;

— certyfikat EUR zawierający klucz publiczny EUR.PK służący do weryfikacji certyfikatu MSCA_Card;

— certyfikat EUR, którego okres ważności wygasa bezpośrednio przed okresem ważności certyfikatu EUR służącego do weryfikacji certyfikatu MSCA_Card, o ile istnieje;

— certyfikat łączący wspomniane dwa certyfikaty EUR, o ile istnieje.

CSM_92 Poza kluczami i certyfikatami kryptograficznymi wymienionymi w CSM_91 karty do tachografu muszą również zawierać klucze i certyfikaty wskazane w części A niniejszego dodatku, dzięki czemu mogą komunikować się z VU pierwszej generacji.

9.1.6 *Poziom urządzenia: urządzenia zewnętrzne GNSS*

CSM_93 Dla każdego urządzenia zewnętrznego GNSS generuje się jedną unikatową parę kluczy ECC oznaczoną jako EGF_MA. Zadanie to realizują producenci urządzeń zewnętrznych GNSS. Ilekroć generowana jest para kluczy EGF_MA, organ generujący klucze przekazuje klucz publiczny MSCA państwa, w którym organ ten ma swoją siedzibę, aby uzyskać powiązany certyfikat EGF_MA podpisany przez MSCA. Klucz prywatny może być używany wyłącznie przez urządzenie zewnętrzne GNSS.

CSM_94 Producent EGF dobiera siłę pary kluczy EGF_MA w taki sposób, by odpowiadała ona sile pary kluczy MSCA użytej do podpisania powiązanego certyfikatu EGF_MA.

CSM_95 Urządzenie zewnętrzne GNSS używa swojej pary kluczy EGF_MA, w której skład wchodzi klucz prywatny EGF_MA.SK i klucz publiczny EGF_MA.PK, wyłącznie do wzajemnego uwierzytelniania i uzgadniania klucza sesji w stosunku do przyrządów rejestrujących, jak określono w sekcjach 11.4 i 11.4 niniejszego dodatku.

CSM_96 Okres ważności certyfikatu EGF_MA wynosi 15 lat.

CSM_97 Urządzenie zewnętrzne GNSS nie może używać klucza prywatnego wchodzącego w skład pary kluczy EGF_MA do wiązania się z przyrządem rejestrującym po wygaśnięciu powiązanego z nim certyfikatu.

Uwaga: jak wyjaśniono w sekcji 11.3.3, EGF może potencjalnie używać swojego klucza prywatnego na potrzeby wzajemnego uwierzytelniania w stosunku do VU, jeżeli został już z nim powiązany, nawet po upływie okresu ważności powiązanego certyfikatu.

CSM_98 Pary kluczy EGF_MA i powiązanych certyfikatów danego urządzenia zewnętrznego GNSS nie można zastępować ani odnawiać w warunkach polowych po rozpoczęciu eksploatacji EGF.

Uwaga: wymóg ten nie uniemożliwia zastąpienia par kluczy EGF w trakcie modernizacji lub naprawy przeprowadzanej w bezpiecznym środowisku kontrolowanym przez producenta EGF.

CSM_99 W chwili ich oddawania do eksploatacji urządzenia zewnętrzne GNSS muszą zawierać następujące klucze i certyfikaty kryptograficzne:

— klucz prywatny EGF_MA i powiązany certyfikat;

— certyfikat MSCA_VU-EGF zawierający klucz publiczny MSCA_VU-EGF.PK służący do weryfikacji certyfikatu EGF_MA;

— certyfikat EUR zawierający klucz publiczny EUR.PK służący do weryfikacji certyfikatu MSCA_VU-EGF;

— certyfikat EUR, którego okres ważności wygasa bezpośrednio przed okresem ważności certyfikatu EUR służącego do weryfikacji certyfikatu MSCA_VU-EGF, o ile istnieje;

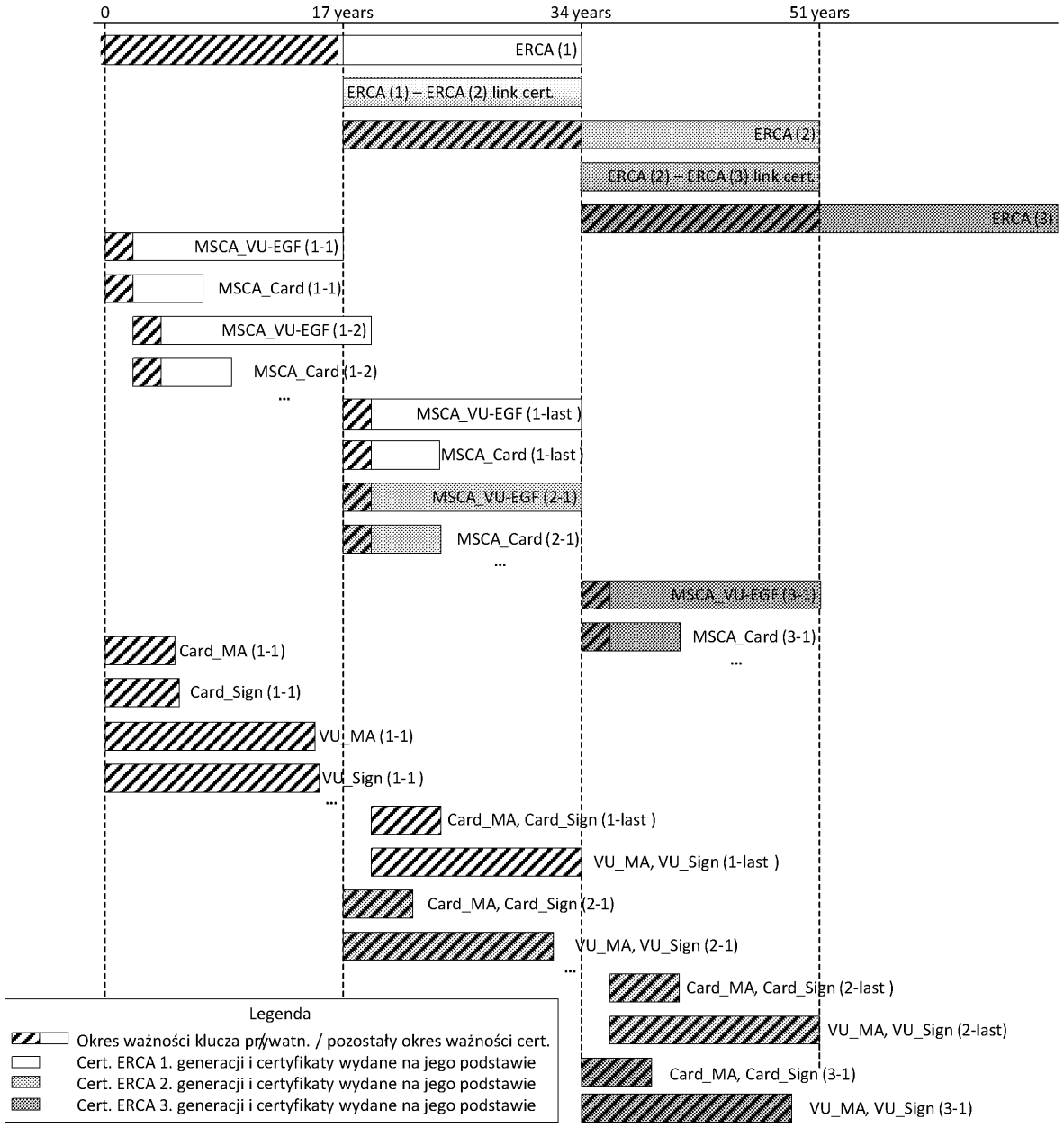
— certyfikat łączący wspomniane dwa certyfikaty EUR, o ile istnieje.

9.1.7 *Przegląd: zastąpienie certyfikatu*

Na rys. 1 poniżej przedstawiono, w jaki sposób różne generacje certyfikatów głównych ERCA, certyfikatów łączących ERCA, certyfikatów MSCA oraz certyfikatów urządzeń (VU i kart) są wydawane i wykorzystywane na przestrzeni czasu:

Rysunek 1

Wydawanie i używanie różnych generacji certyfikatów głównych ERCA, certyfikatów łączących ERCA, certyfikatów MSCA i certyfikatów urządzeń



Uwagi do rys. 1

1. poszczególne generacje certyfikatów głównych oznaczono cyfrą w nawiasie. Na przykład ERCA (1) oznacza pierwszą generację certyfikatu głównego ERCA, ERCA (2) – drugą generację itd.;

2. pozostałe certyfikaty są oznaczone dwiema cyframi w nawiasach: pierwsza z nich wskazuje generację certyfikatu głównego, w której wydano dany certyfikat, natomiast druga określa generację samego certyfikatu. Na przykład MSCA_Card (1-1) oznacza pierwszy certyfikat MSCA_Card wydany na podstawie ERCA (1); MSCA_Card (2-1) oznacza pierwszy certyfikat MSCA_Card wydany na podstawie ERCA (2); MSCA_Card (2-ostatni) oznacza ostatni certyfikat MSCA_Card wydany na podstawie ERCA (2); Card_MA (2-1) oznacza pierwszy certyfikat karty na potrzeby wzajemnego uwierzytelnienia wydany na podstawie ERCA (2) itp.;

3. certyfikaty MSCA_Card (2-1) i MSCA_Card (1-ostatni) wydaje się z bardzo zbliżoną datą. MSCA_Card (2-1) oznacza pierwszy certyfikat MSCA_Card wydany na podstawie ERCA (2), który wydaje się nieco później niż MSCA_Card (1-ostatni), czyli ostatni certyfikat MSCA_Card wydany na podstawie ERCA (1);

4. zgodnie z informacjami przedstawionymi na rysunku pierwsze certyfikaty VU i certyfikaty karty wydane na podstawie ERCA (2) pojawią się niemal dwa lata przed ostatnimi certyfikatami VU i certyfikatami karty wydanymi na podstawie ERCA (1). Wynika to z faktu, że certyfikaty VU i certyfikaty karty wydaje się na podstawie certyfikatu MSCA, nie zaś bezpośrednio na podstawie certyfikatu ERCA. Certyfikat MSCA (2-1) zostanie wydany bezpośrednio po uzyskaniu ważności przez ERCA (2), ale certyfikat MSCA (1-ostatni) zostanie wydany tylko nieznacznie później, tj. w ostatnim dniu, w którym certyfikat ERCA (1) jest nadal ważny. Z tego względu obydwa certyfikaty MSCA będą miały niemal taki sam okres ważności, mimo że należą do różnych generacji;

5. podany okres ważności kart odpowiada okresowi ważności kart kierowcy (5 lat);

6. aby zaoszczędzić miejsce, różnica w okresie ważności certyfikatów Card_MA i Card_Sign oraz w okresie ważności certyfikatów VU_MA i VU_Sign została podana wyłącznie dla certyfikatów pierwszej generacji.

9.2. **Klucze symetryczne**

9.2.1 *Klucze do zabezpieczania łączności między VU a czujnikiem ruchu*

9.2.1.1 *Uwagi ogólne*

Uwaga: zakłada się, że czytelnicy tego rozdziału są zaznajomieni z treścią normy [ISO 16844-3], w której opisano interfejs pomiędzy przyrządem rejestrującym a czujnikiem ruchu. Proces parowania VU i czujnika ruchu opisano szczegółowo w rozdziale 12 niniejszego dodatku.

CSM_100 Potrzeba wielu kluczy symetrycznych do sparowania przyrządów rejestrujących i czujników ruchu, wzajemnego uwierzytelnienia między przyrządami rejestrującymi a czujnikami ruchu oraz zaszyfrowania łączności między przyrządami rejestrującymi a czujnikami ruchu, jak pokazano w tabeli 3. Wszystkie te klucze muszą być kluczami AES o długości klucza równej długości klucza głównego czujnika ruchu, która z kolei musi być powiązana z (przewidywaną) długością pary europejskich kluczy głównych, jak opisano w CSM_50.

Tabela 3

Klucze do zabezpieczania łączności między przyrządem rejestrującym a czujnikiem ruchu

Klucz	Symbol	Generowany przez	Metoda generowania	Przechowywany przez
Klucz główny czujnika ruchu – część dotycząca VU	$K_{M\text{-}VU}$	ERCA	Losowo	ERCA, MSCA zaangażowane w wydawanie certyfikatów VU, producenci VU, przyrządy rejestrujące

Klucz	Symbol	Generowany przez	Metoda generowania	Przechowywany przez
Klucz główny czujnika ruchu – część dotycząca warsztatu	K_{M-WC}	ERCA	Losowo	ERCA, MSCA, producenci kart, karty warsztatowe
Klucz główny czujnika ruchu	K_M	Nie jest generowany oddzielnie	Obliczany jako $K_M = K_{M-VU}$ XOR K_{M-WC}	ERCA, MSCA zaangażowane w wydawanie kluczy czujników ruchu (opcjonalnie) (*)
Klucz identyfikacyjny	K_{ID}	Nie jest generowany oddzielnie	Obliczany jako $K_{ID} = K_M$ XOR CV, gdzie CV jest określony w CSM_106	ERCA, MSCA zaangażowane w wydawanie kluczy czujników ruchu (opcjonalnie) (*)
Klucz parowania	K_P	Producent czujnika ruchu	Losowo	Jeden czujnik ruchu
Klucz sesji	K_S	VU (w trakcie parowania VU z czujnikiem ruchu)	Losowo	Jeden VU i jeden czujnik ruchu

(*) Przechowywanie K_M i K_{ID} jest opcjonalne, ponieważ klucze te można wyprowadzić z K_{M-VU}, K_{M-WC} i CV.

CSM_101 Główny Europejski Organ Certyfikacji generuje K_{M-WU} i K_{M-WC}, dwa losowe, unikatowe klucze AES, na podstawie których można obliczyć klucz główny czujnika ruchu K_M jako K_{M-VU} XOR K_{M-WC}. Na wniosek organów certyfikacji państw członkowskich ERCA przekazuje im K_M, K_{M-VU} i K_{M-WC}.

CSM_102 ERCA przypisuje każdemu kluczowi głównemu czujnika ruchu K_M unikatowy numer wersji mający zastosowanie również do kluczy ustanawiających K_{M-VU} i K_{M-WC} oraz do powiązanego klucza identyfikacyjnego K_{ID}. ERCA powiadamia MSCA o numerze wersji, gdy przekazuje im K_{M-VU} i K_{M-WC}.

Uwaga: numer wersji wykorzystuje się do rozróżnienia poszczególnych generacji wspomnianych kluczy, jak wyjaśniono szczegółowo w sekcji 9.2.1.2.

CSM_103 Organ certyfikacji państwa członkowskiego przekazuje K_{M-VU} wraz z jego numerem wersji producentom przyrządów rejestrujących na ich wniosek. Producenci VU umieszczają K_{M-VU} wraz z jego numerem wersji we wszystkich wytwarzanych VU.

CSM_104 Organ certyfikacji państwa członkowskiego zapewnia umieszczenie K_{M-WC} wraz z jego numerem wersji w każdej karcie warsztatowej wydanej pod nadzorem MSCA.

Uwagi

— Zobacz opis typu danych `SensorInstallationSecData` w dodatku 2.

— Jak wyjaśniono w sekcji 9.2.1.2, w praktyce w niektórych przypadkach może zachodzić konieczność umieszczenia wielu generacji K_{M-WC} w pojedynczej karcie warsztatowej.

CSM_105 Poza kluczem AES, o którym mowa w CSM_104, MSCA zapewnia również umieszczenie klucza TDES Km_{WC}, o którym mowa w wymogu CSM_037 w części A niniejszego dodatku, w każdej karcie warsztatowej wydanej pod nadzorem MSCA.

Uwagi

— Zapewnia to możliwość użycia karty warsztatowej drugiej generacji do powiązania z VU pierwszej generacji.

— Karta warsztatowa drugiej generacji będzie posiadała dwie różne aplikacje, z których jedna będzie zgodna z częścią B niniejszego dodatku, a druga – z częścią A niniejszego dodatku. Ta druga aplikacja będzie zawierała klucz TDES Km_{WC}.

CSM_106 MSCA zaangażowany w wydawanie certyfikatów czujników ruchu wyprowadza klucz identyfikacyjny z klucza głównego czujnika ruchu, za pomocą funkcji XOR z wykorzystaniem wektora stałego CV. Przyjmuje się, że CV ma następującą wartość:

— w odniesieniu do 128-bitowych kluczy głównych czujnika ruchu: CV = 'B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5E 83'

— w odniesieniu do 192-bitowych kluczy głównych czujnika ruchu: CV = '72 AD EA FA 00 BB F4 EE F4 99 15 70 5B 7E EE BB 1C 54 ED 46 8B 0E F8 25'

— w odniesieniu do 256-bitowych kluczy głównych czujnika ruchu: CV = '1D 74 DB F0 34 C7 37 2F 65 55 DE D5 DC D1 9A C3 23 D6 A6 25 64 CD BE 2D 42 0D 85 D2 32 63 AD 60'

Uwaga: wektory stałe generuje się w następujący sposób:

Pi_10 = pierwsze 10 bajtów dziesiętnej części stałej matematycznej π = '24 3F 6A 88 85 A3 08 D3 13 19'

CV_128-bits = pierwszych 16 bajtów SHA-256(Pi_10)

CV_192-bits = pierwsze 24 bajty SHA-384(Pi_10)

CV_256-bits = pierwsze 32 bajty SHA-512(Pi_10)

CSM_107 Producenci czujników ruchu generują losowy i unikatowy klucz parowania K_P dla każdego czujnika ruchu i przesyłają każdy klucz parowania organowi certyfikacji państwa członkowskiego (MSCA). MSCA szyfruje każdy klucz parowania oddzielnie za pomocą klucza głównego czujnika ruchu K_M i zwraca zaszyfrowany klucz producentowi czujników ruchu. W przypadku każdego zaszyfrowanego klucza MSCA powiadamia producenta czujników ruchu o numerze wersji powiązanego K_M.

Uwaga: jak wyjaśniono w sekcji 9.2.1.2, w praktyce może zachodzić konieczność wygenerowania przez producenta czujników ruchu wielu unikatowych kluczy parowania dla pojedynczego czujnika ruchu.

CSM_108 Producenci czujników ruchu generują unikatowy numer seryjny dla każdego czujnika ruchu i przesyłają wszystkie numery seryjne organowi certyfikacji państwa członkowskiego. MSCA szyfruje każdy numer seryjny oddzielnie za pomocą klucza identyfikacyjnego K_{ID} i zwraca zaszyfrowany numer seryjny producentowi czujników ruchu. W przypadku każdego zaszyfrowanego numeru seryjnego MSCA powiadamia producenta czujników ruchu o numerze wersji powiązanego K_{ID}.

CSM_109 W odniesieniu do wymogów CSM_107 i CSM_108 MSCA korzysta z algorytmu AES w trybie wiązania bloków zaszyfrowanych, jak określono w normie [ISO 10116], z naprzemiennym parametrem *m* = 1 oraz wektorem inicjującym SV = '00' {16}, tj. szesnaście bajtów o wartości binarnej 0. W razie potrzeby MSCA korzysta z metody wypełniania 2 określonej w normie [ISO 9797-1].

CSM_110 Producent czujników ruchu przechowuje zaszyfrowany klucz parowania i zaszyfrowany numer seryjny w przewidzianym czujniku ruchu wraz z odpowiadającymi wartościami zwykłego tekstu i numerem wersji K_M i K_{ID} użytymi do szyfrowania.

Uwaga: jak wyjaśniono w sekcji 9.2.1.2, w praktyce może zachodzić konieczność umieszczenia przez producenta czujników ruchu wielu zaszyfrowanych kluczy parowania i wielu zaszyfrowanych numerów seryjnych w pojedynczym czujniku ruchu.

CSM_111 Oprócz materiału kryptograficznego opartego na AES określonego w CSM_110, producent czujników ruchu może również przechowywać w każdym czujniku ruchu materiał kryptograficzny oparty na TDES, jak określono w niniejszym dodatku część A wymóg CSM_037.

Uwaga: dzięki temu możliwe będzie powiązanie czujnika ruchu drugiej generacji z VU pierwszej generacji.

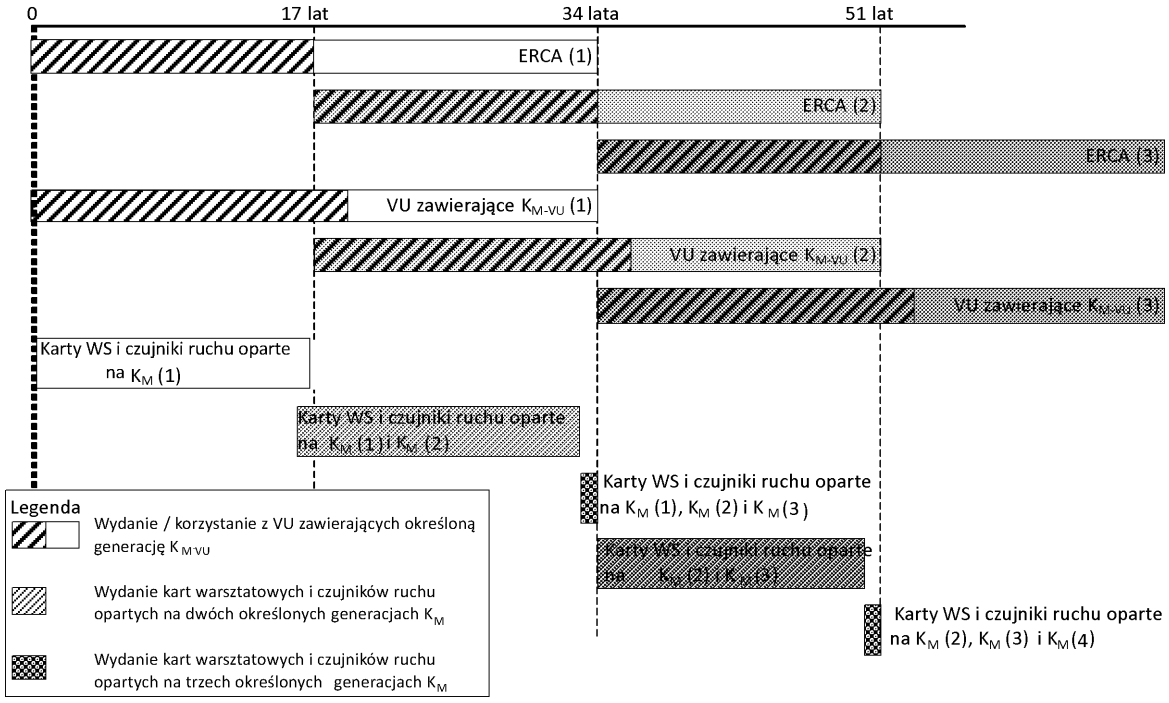
CSM_112 Długość klucza sesji K_S wygenerowanego przez VU w trakcie parowania z czujnikiem ruchu jest powiązana z długością jego K_{M-VU}, jak opisano w CSM_50.

9.2.1.2 *Zastąpienie klucza głównego czujnika ruchu w urządzeniu drugiej generacji*

CSM_113 Każdy klucz główny czujnika ruchu i wszystkie powiązane klucze (zob. tabela 3) są powiązane z określoną generacją pary kluczy głównych ERCA. Klucze te wymienia się zatem co 17 lat. Okres ważności każdej generacji klucza głównego czujnika ruchu rozpoczyna się rok wcześniej, zanim powiązana para kluczy głównych ERCA stanie się ważna, i kończy się po upływie ważności powiązanej pary kluczy głównych ERCA. Przedstawiono to na rys. 2.

Rys. 2

Wydawanie różnych generacji klucza głównego czujnika ruchu i ich używanie w przyrządach rejestrujących, czujnikach ruchu i kartach warsztatowych



CSM_114 Co najmniej rok przed wygenerowaniem nowej pary europejskich kluczy głównych, jak opisano w CSM_56, ERCA generuje nowy klucz główny czujnika ruchu K_M poprzez wygenerowanie nowych K_{M-VU} i K_{M-WC}. Długość klucza głównego czujnika ruchu jest powiązana z przewidywaną siłą nowej pary europejskich kluczy głównych zgodnie z CSM_50. Na wniosek MSCA ERCA przekazuje im nowe K_M, K_{M-VU} i K_{M-WC} wraz z ich numerem wersji.

CSM_115 MSCA zapewnia, aby wszystkie ważne generacje K_{M-WC} były przechowywane na karcie warsztatowej wydanej z jego upoważnienia wraz z numerami wersji, jak przedstawiono na rys. 2.

Uwaga: oznacza to, że w ostatnim roku okresu ważności certyfikatu ERCA karty warsztatowe będą wydawane z trzema różnymi generacjami K_{M-WC}, jak przedstawiono na rys. 2.

CSM_116 W odniesieniu do procesu opisanego w CSM_107 i CSM_108 powyżej: MSCA szyfruje każdy klucz parowania K_P, który otrzymuje od producenta czujników ruchu, oddzielnie za pomocą każdej ważnej generacji klucza głównego czujnika ruchu K_M. MSCA szyfruje również każdy numer seryjny, który otrzymuje od producenta czujników ruchu, oddzielnie za pomocą każdej ważnej generacji klucza identyfikacyjnego K_{ID}. Producent czujników ruchu przechowuje wszystkie zaszyfrowane klucze parowania i wszystkie zaszyfrowane numery seryjne w przewidzianym czujniku ruchu wraz z odpowiadającymi wartościami zwykłego tekstu i numerami wersji K_M i K_{ID} użytymi do szyfrowania.

Uwaga: oznacza to, że w ostatnim roku okresu ważności certyfikatu ERCA czujniki ruchu będą wydawane z zaszyfrowanymi danymi opartymi na trzech różnych generacjach $K_{M,}$, jak przedstawiono na rys. 2.

CSM_117 W odniesieniu do procesu opisanego powyżej w CSM_107: ze względu na fakt, że długość klucza parowania K_P jest powiązana z długością K_M (zob. CSM_100), producent czujnika ruchu może być zmuszony do wygenerowania do trzech różnych kluczy parowania (o różnej długości) dla jednego czujnika ruchu, w przypadku gdy kolejne generacje K_M mają różne długości. W takim przypadku producent przesyła MSCA każdy klucz parowania. MSCA zapewnia, aby każdy klucz parowania był zaszyfrowany za pomocą prawidłowej generacji klucza głównego czujnika ruchu tj. klucza mającego taką samą długość.

Uwaga: w przypadku gdy producent czujników ruchu zdecyduje się wygenerować klucz parowania oparty na TDES dla czujnika ruchu drugiej generacji (zob. CSM_111), producent wskazuje MSCA, że klucz główny czujnika ruchu oparty na TDES musi zostać użyty do zaszyfrowania tego klucza parowania. Wynika to z tego, że długość klucza TDES może być równa długości klucza AES, tak więc MSCA nie może dokonać oceny wyłącznie na podstawie długości klucza.

CSM_118 Producenci przyrządów rejestrujących umieszczają tylko jedną generację K_{M-VU} w każdym przyrządzie rejestrującym wraz z jego numerem wersji. Wspomniana generacja K_{M-VU} musi być powiązana z certyfikatem ERCA, na których opierają się certyfikaty VU.

Uwagi

— Przyrząd rejestrujący oparty na certyfikacie ERCA generacji *X* zawiera jedynie K_{M-VU} generacji X, nawet jeżeli został wydany po rozpoczęciu okresu ważności certyfikatu ERCA generacji *X + 1*. Przedstawiono to na rys. 2.

— Przyrządu rejestrującego generacji *X* nie można sparować z czujnikiem ruchu generacji *X − 1*.

— Ze względu na fakt, że okres ważności kart warsztatowych wynosi jeden rok, w wyniku zastosowania CSM_113 – CSM_118 wszystkie karty warsztatowe będą zawierały nowy K_{M-WC} w momencie wydania pierwszego VU zawierającego nowy K_{M-VU}. W związku z tym taki VU zawsze będzie w stanie obliczyć nowy K_M. Ponadto do tego czasu większość nowych czujników ruchu będzie zawierała zaszyfrowane dane również oparte na nowym K_M.

9.2.2 *Klucze do zabezpieczania łączności DSRC*

9.2.2.1 *Uwagi ogólne*

CSM_119 Autentyczność i poufność danych przekazanych organowi kontrolnemu z przyrządu rejestrującego za pośrednictwem kanału DSRC do łączności na odległość zapewnia się za pomocą zestawu kluczy AES specyficznych dla VU, który wyprowadzono z pojedynczego klucza głównego DSRC, KM_{DSRC}.

CSM_120 Klucz główny DSRC KM_{DSRC} stanowi klucz AES, który jest bezpiecznie generowany, przechowywany i rozpowszechniany przez ERCA. Długość klucza może wynosić 128, 192 lub 256 bitów i jest powiązana z długością pary europejskich kluczy głównych, jak opisano w CSM_50.

CSM_121 Na wniosek organów certyfikacji państw członkowskich ERCA przekazuje im klucz główny DSRC w sposób bezpieczny w celu umożliwienia im wyprowadzenia kluczy DSRC specyficznych dla VU i zapewnienia umieszczenia klucza głównego DSRC we wszystkich kartach kontrolnych i kartach warsztatowych wydanych na ich odpowiedzialność.

CSM_122 ERCA przypisuje każdemu kluczowi głównemu DSRC unikatowy numer wersji. ERCA powiadamia MSCA o numerze wersji, gdy przesyła im klucz główny DSRC.

Uwaga: numer wersji wykorzystuje się do rozróżnienia poszczególnych generacji klucza głównego DSRC, jak wyjaśniono szczegółowo w sekcji 9.2.2.2.

CSM_123 W odniesieniu do każdego przyrządu rejestrującego producent takiego przyrządu tworzy unikatowy numer seryjny VU i przesyła taki numer swojemu organowi certyfikacji państwa członkowskiego we wniosku w celu uzyskania zestawu dwóch kluczy DSRC specyficznych dla VU. Numer seryjny VU posiada typ danych `VuSerialNumber`i do kodowania wykorzystuje się wyróżnione reguły kodowania (DER) zgodnie z normą [ISO 8825-1].

CSM_124 Po otrzymaniu wniosku o klucze DSRC specyficzne dla VU MSCA wyprowadza dwa klucze AES dla przyrządu rejestrującego, zwane K_VU_{DSRC}_ENC i K_VU_{DSRC}_MAC. Wspomniane klucze specyficzne dla VU mają taką samą długość jak klucz główny DSRC. MSCA korzysta z funkcji wyprowadzania klucza zdefiniowanej w [RFC 5869]. Funkcja skrótu, która jest niezbędna do utworzenia wystąpienia funkcji HMAC-Hash, jest powiązana z długością klucza głównego DSRC, jak opisano w CSM_50. Z funkcji wyprowadzania klucza w [RFC 5869] korzysta się w następujący sposób:

krok 1: (wyodrębnienie):

— *PRK* = HMAC-Hash (*salt, IKM*) gdzie *salt* oznacza pusty ciąg *''*, a *IKM* oznacza KM_{DSRC};

krok 2: (rozszerzenie):

— *OKM* = *T(1)*, gdzie

T(1) = HMAC-Hash (*PRK, T(0)* || *info* || '01')

— *T(0)* = pusty ciąg (*''*)

— *info* = numer seryjny VU, jak określono w CSM_123

— K_VU_{DSRC}_ENC = pierwsze oktety *L OKM* i

K_VU_{DSRC}_MAC = ostatnie oktety *L OKM*

gdzie *L* oznacza wymaganą długość K_VU_{DSRC}_ENC i K_VU_{DSRC}_MAC w oktetach.

CSM_125 MSCA przekazuje K_VU_{DSRC}_ENC i K_VU_{DSRC}_MAC producentowi VU w sposób bezpieczny w celu umieszczenia w przewidzianym przyrządzie rejestrującym.

CSM_126 Po wydaniu przyrząd rejestrujący przechowuje K_VU_{DSRC}_ENC i K_VU_{DSRC}_MAC w swojej bezpiecznej pamięci, aby móc zapewnić integralność, autentyczność i poufność danych wysyłanych za pośrednictwem kanału do łączności na odległość. Przyrząd rejestrujący przechowuje również numer wersji klucza głównego DSRC użyty do wyprowadzenia tych kluczy specyficznych dla VU.

CSM_127 Po wydaniu karty kontrolne i karty warsztatowe przechowują KM_{DSRC} w swojej bezpiecznej pamięci, aby móc zweryfikować integralność i autentyczność danych wysyłanych przez VU za pośrednictwem kanału do łączności na odległość oraz aby deszyfrować te dane. Karty kontrolne i karty warsztatowe przechowują również numer wersji klucza głównego DSRC.

Uwaga: jak wyjaśniono w sekcji 9.2.2.2, w praktyce może zachodzić konieczność umieszczenia wielu generacji KM_{DSRC} w pojedynczej karcie warsztatowej lub pojedynczej karcie kontrolnej.

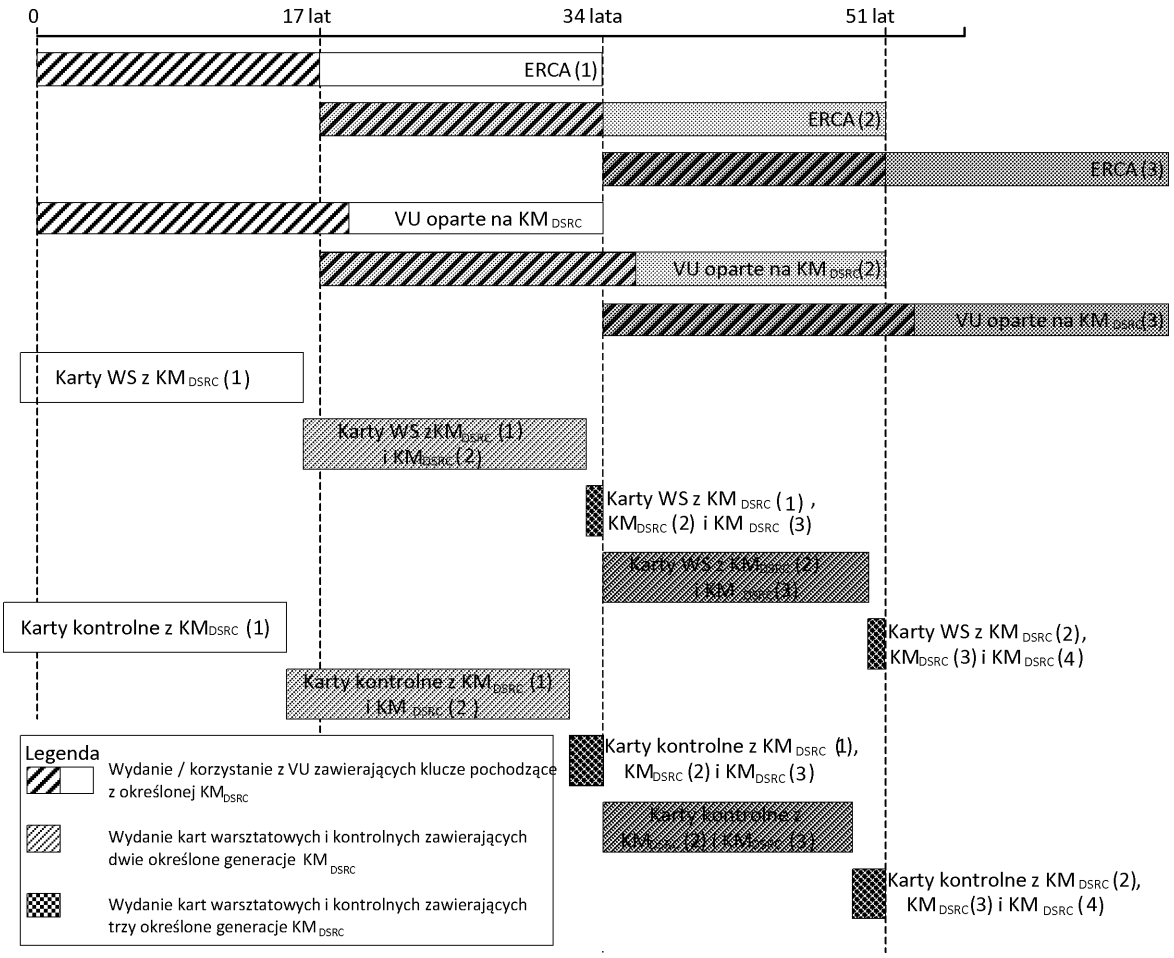
CSM_128 MSCA prowadzi rejestry wszystkich wygenerowanych kluczy DSRC specyficznych dla VU, ich numery wersji i identyfikację VU, dla którego każdy zestaw kluczy jest przeznaczony.

9.2.2.2 *Zastąpienie klucza głównego DSRC*

CSM_129 Każdy klucz główny DSRC jest powiązany z określoną generacją pary kluczy głównych ERCA. ERCA zastępuje zatem klucz główny DSRC co 17 lat. Okres ważności każdej generacji klucza głównego DSRC rozpoczyna się dwa lata wcześniej, zanim powiązana para kluczy głównych ERCA stanie się ważna, i kończy się po upływie ważności powiązanej pary kluczy głównych ERCA. Przedstawiono to na rys. 3.

Rys. 3

Wydawanie różnych generacji klucza głównego DSRC i ich używanie w przyrządach rejestrujących, kartach warsztatowych i kartach kontrolnych



CSM_130 Co najmniej dwa lata przed wygenerowaniem nowej pary europejskich kluczy głównych, jak opisano w CSM_56, ERCA generuje nowy klucz główny DSRC. Długość klucza DSRC jest powiązana z przewidywaną siłą nowej pary europejskich kluczy głównych zgodnie z CSM_50. Na wniosek MSCA ERCA przekazuje im nowy klucz główny DSRC wraz z jego numerem wersji.

CSM_131 MSCA zapewnia, aby wszystkie ważne generacje KM_{DSRC} były przechowywane na karcie kontrolnej wydanej z jego upoważnienia wraz z numerami wersji, jak przedstawiono na rys. 3.

Uwaga: oznacza to, że w ciągu ostatnich dwóch lat okresu ważności certyfikatu ERCA karty kontrolne będą wydawane z trzema różnymi generacjami KM_{DSRC}, jak przedstawiono na rys. 3.

CSM_132 MSCA zapewnia, aby wszystkie generacje KM_{DSRC}, które były ważne przez co najmniej rok i nadal są ważne, były przechowywane na karcie warsztatowej wydanej z jego upoważnienia wraz z numerami wersji, jak przedstawiono na rys. 3.

Uwaga: oznacza to, że w ostatnim roku okresu ważności certyfikatu ERCA karty warsztatowe będą wydawane z trzema różnymi generacjami KM_{DSRC}, jak przedstawiono na rys. 3.

CSM_133 Producenci przyrządów rejestrujących umieszczają tylko jeden zestaw kluczy DSRC specyficznych dla VU w każdym przyrządzie rejestrującym wraz z jego numerem wersji. Wspomniany zestaw kluczy wyprowadza się z generacji KM_{DSRC} powiązanej z certyfikatem ERCA, na którym opierają się certyfikaty VU.

Uwagi

— Oznacza to, że przyrząd rejestrujący oparty na certyfikacie ERCA generacji *X* zawiera jedynie K_VU_{DSRC}_ENC i K_VU_{DSRC}_MAC generacji *X*, nawet jeżeli VU został wydany po rozpoczęciu okresu ważności certyfikatu ERCA generacji *X + 1*. Przedstawiono to na rys. 3.

— Ze względu na fakt, że okres ważności kart warsztatowych wynosi jeden rok, a kart kontrolnych dwa lata, w wyniku zastosowania CSM_131 – CSM_133 wszystkie karty warsztatowe i karty kontrolne będą zawierały nowy klucz główny DSRC w momencie wydania pierwszego VU zawierającego klucze specyficzne dla VU, oparte na przedmiotowym kluczu głównym.

9.3. **Certyfikaty**

9.3.1 *Uwagi ogólne*

CSM_134 Wszystkie certyfikaty w europejskim systemie tachografów inteligentnych są certyfikatami samoopisującymi, weryfikowalnymi przez kartę (CV) zgodnie z normami [ISO 7816-4] i [ISO 7816-8].

CSM_135 Wyróżnione reguły kodowania (DER) zgodnie z normą [ISO 8825-1] wykorzystuje się do kodowania zarówno struktur danych ASN.1 i (specyficznych dla aplikacji) obiektów danych w ramach certyfikatów.

Uwaga: w wyniku takiego kodowania uzyskuje się następującą strukturę TLV:

znacznik: znacznik jest zakodowany w jednym oktecie lub dwóch oktetach i określa treść;

długość: długość jest zakodowana jako liczba całkowita bez znaku w jednym oktecie, dwóch lub trzech oktetach, co skutkuje uzyskaniem maksymalnej długości 65 535 oktetów. Stosuje się minimalną liczbę oktetów;

wartość: wartość nie jest zakodowana w żadnym oktecie lub jest zakodowana w większej liczbie oktetów.

9.3.2 *Treść certyfikatu*

CSM_136 Wszystkie certyfikaty mają strukturę przedstawioną w profilu certyfikatu w tabeli 4.

Tabela 4

Wersja 1 profilu certyfikatu

Pole	Nr ID pola	Znacznik	Długość (bajty)	Typ danych ASN.1 (zob. dodatek 1)
Certyfikat ECC	C	'7F 21'	var	
Treść certyfikatu ECC	B	'7F 4E'	var	

Pole	Nr ID pola	Znacznik	Długość (bajty)	Typ danych ASN.1 (zob. dodatek 1)
Identyfikator profilu certyfikatu	CPI	'5F 29'	'01'	INTEGER(0..255)
odniesienie do organu certyfikacji	CAR	'42'	'08'	KeyIdentifier
upoważnienie posiadacza certyfikatu	CHA	'5F 4C'	'07'	CertificateHolder Authorisation
Klucz publiczny	PK	'7F 49'	var	
Parametry domeny	DP	'06'	var	IDENTYFIKATOR OBIEKTU
Punkt publiczny	PP	'86'	var	OCTET STRING
odniesienie do posiadacza certyfikatu	CHR	'5F 20'	'08'	KeyIdentifier
Data wejścia w życie certyfikatu	CEfD	'5F 25'	'04'	TimeReal
Data wygaśnięcia certyfikatu	CExD	'5F 24'	'04'	TimeReal
Podpis certyfikatu ECC	S	'5F 37'	var	OCTET STRING

Uwaga: identyfikator pola zostanie wykorzystany w dalszych częściach niniejszego dodatku w celu wskazania poszczególnych pól certyfikatu np. X.CAR oznacza odniesienie do organu certyfikacji, o którym mowa w certyfikacie użytkownika X.

9.3.2.1 Identyfikator profilu certyfikatu

CSM_137 Certyfikaty używają identyfikatora profilu certyfikatu do wskazania użytego profilu certyfikatu. Wersję 1, jak wskazano w tabeli 4, określa się za pomocą wartości '00'.

9.3.2.2 Odniesienie do organu certyfikacji

CSM_138 Odniesienie do organu certyfikacji wykorzystuje się do określenia klucza publicznego, który ma zostać użyty do weryfikacji podpisu certyfikatu. Odniesienie do organu certyfikacji pokrywa się zatem z odniesieniem do posiadacza certyfikatu w certyfikacie odpowiedniego organu certyfikacji.

CSM_139 Certyfikat główny ERCA jest certyfikatem z podpisem własnym, tj. odniesienie do organu certyfikacji pokrywa się z odniesieniem do posiadacza certyfikatu w certyfikacie.

CSM_140 W przypadku certyfikatu łączącego ERCA odniesienie do posiadacza certyfikatu pokrywa się z odniesieniem do posiadacza certyfikatu nowego certyfikatu głównego ERCA. W przypadku certyfikatu łączącego odniesienie do organu certyfikacji pokrywa się z odniesieniem do posiadacza certyfikatu poprzedniego certyfikatu głównego ERCA.

9.3.2.3 Upoważnienie posiadacza certyfikatu

CSM_141 Upoważnienie posiadacza certyfikatu służy do identyfikowania rodzaju certyfikatu. Składa się ono z sześciu najbardziej znaczących bajtów identyfikatora aplikacji tachograficznej połączonych z typem urządzenia, dla którego certyfikat jest przeznaczony.

9.3.2.4 Klucz publiczny

Klucz publiczny zawiera dwa elementy danych: standardowe parametry domeny stosowane z kluczem publicznym w certyfikacie i wartość punktu publicznego.

CSM_142 Element danych „parametry domeny" zawiera jeden z identyfikatorów obiektu określony w tabeli 1 w celu odniesienia do zestawu standardowych parametrów domeny.

CSM_143 Element danych „punkt publiczny" zawiera punkt publiczny. Punkty publiczne krzywej eliptycznej przekształca się w ciągi oktetowe, jak określono w [TR-03111]. Stosuje się nieskompresowany format kodowania. Podczas odzyskiwania punktu krzywej eliptycznej z jej zakodowanego formatu zawsze przeprowadza się autoryzacje opisane w [TR-03111].

9.3.2.5 odniesienie do posiadacza certyfikatu

CSM_144 Odniesienie do posiadacza certyfikatu to identyfikator klucza publicznego umieszczony w certyfikacie. Używa się go celem odniesienia do tego klucza publicznego w innych certyfikatach.

CSM_145 W przypadku certyfikatów kart i certyfikatów urządzeń zewnętrznych GNSS odniesienie do posiadacza certyfikatu posiada typ danych `ExtendedSerialNumber`, określony w dodatku 1.

CSM_146 W przypadku przyrządów rejestrujących producent, składając wniosek o certyfikat, może znać specyficzny dla danego producenta numer seryjny VU, dla którego przeznaczony jest dany certyfikat i powiązany klucz prywatny, ale nie musi go znać. W pierwszym przypadku odniesienie do posiadacza certyfikatu posiada typ danych `ExtendedSerialNumber`, określony w dodatku 1. W tym drugim przypadku odniesienie do posiadacza certyfikatu posiada typ danych `CertificateRequestID`, określony w dodatku 1.

CSM_147 W przypadku certyfikatów ERCA i MSCA odniesienie do posiadacza certyfikatu posiada typ danych `CertificationAuthorityKID`, określony w dodatku 1.

9.3.2.6 Data wejścia w życie certyfikatu

CSM_148 Data wejścia w życie certyfikatu określa datę i godzinę rozpoczęcia okresu ważności certyfikatu. Data wejścia w życie certyfikatu oznacza datę wygenerowania certyfikatu.

9.3.2.7 Data wygaśnięcia certyfikatu

CSM_149 Data wygaśnięcia certyfikatu określa datę i godzinę zakończenia okresu ważności certyfikatu.

9.3.2.8 Podpis certyfikatu

CSM_150 Podpis na certyfikacie tworzy się nad zakodowaną treścią certyfikatu, uwzględniając znacznik i długość treści certyfikatu. Algorytmem podpisu jest ECDSA, jak określono w [DSS], używający algorytmu skrótu powiązanego z wielkością klucza jednostki podpisującej, jak określono w CSM_50. Format podpisu jest odkryty, jak określono w [TR-03111].

9.3.3 *Składanie wniosków o certyfikaty*

CSM_151 Składając wniosek o certyfikat, podmiot wnioskujący przesyła swojemu organowi certyfikacji następujące dane:

— identyfikator profilu certyfikatu, którego dotyczy wniosek;

— odniesienie do organu certyfikacji, w przypadku którego oczekuje się, że zostanie użyte do podpisania certyfikatu;

— klucz publiczny, który ma zostać podpisany.

CSM_152 Oprócz danych określonych w CSM_151 MSCA przesyła ERCA następujące dane we wniosku o certyfikat, co umożliwi ERCA utworzenie odniesienia do posiadacza certyfikatu dla nowego certyfikatu MSCA:

— numeryczny kod krajowy organu certyfikacji (typ danych `NationNumeric` , określony w dodatku 1);

— alfanumeryczny kod krajowy organu certyfikacji (typ danych `NationAlpha` , określony w dodatku 1);

— 1-bajtowy numer seryjny umożliwiającym rozróżnienie poszczególnych kluczy organu certyfikacji w przypadku zmiany kluczy;

— 2-bajtowe pole zawierające dodatkowe informacje na temat określonego organu certyfikacji.

CSM_153 Oprócz danych określonych w CSM_151 producent urządzenia przesyła MSCA następujące dane we wniosku o certyfikat, co umożliwi MSCA utworzenie odniesienia do posiadacza certyfikatu dla nowego certyfikatu urządzenia:

— specyficzny dla producenta identyfikator typu urządzenia;

— numer seryjny urządzenia, unikalny dla producenta, typu urządzenia i miesiąc wyprodukowania, jeżeli dane te są znane (zob. CSM_154). W przeciwnym razie – unikatowy identyfikator wniosku o certyfikat;

— miesiąc i rok produkcji urządzenia lub miesiąc i rok sporządzenia wniosku o certyfikat.

Producent zapewnia, aby przedmiotowe dane były prawidłowe, a certyfikat zwrócony przez MSCA został umieszczony w przewidzianym urządzeniu.

CSM_154 W przypadku VU producent, składając wniosek o certyfikat, może znać specyficzny dla danego producenta numer seryjny VU, dla którego przeznaczony jest dany certyfikat i powiązany klucz prywatny, ale nie musi go znać. Producent VU przesyła MSCA numer seryjny, jeżeli jest on znany. Jeżeli nie jest znany, producent jednoznacznie identyfikuje każdy wniosek o certyfikat i przesyła MSCA taki numer seryjny wniosku o certyfikat. Otrzymany certyfikat będzie wówczas zawierał numer seryjny wniosku o certyfikat. Po umieszczeniu certyfikatu w określonym VU producent informuje MSCA o połączeniu między numerem seryjnym wniosku o certyfikat a identyfikacją VU.

10. WZAJEMNE UWIERZYTELNIANIE I BEZPIECZNA WYMIANA KOMUNIKATÓW MIĘDZY VU A KARTĄ

10.1. **Uwagi ogólne**

CSM_155 Na wysokim szczeblu bezpieczna łączność między przyrządem rejestrującym a kartą do tachografu odbywa się w następujących etapach:

— po pierwsze każda strona wykazuje drugiej, że posiada ważny certyfikat klucza publicznego, podpisany przez organ certyfikacji państwa członkowskiego. Z kolei certyfikat klucza publicznego MSCA musi zostać podpisany przez Główny Europejski Organ Certyfikacji. Etap ten nazywany jest weryfikacją łańcucha certyfikatów i został szczegółowo opisany w sekcji 10.2;

— po drugie przyrząd rejestrujący wykazuje karcie, że posiada klucz prywatny odpowiadający kluczowi publicznemu w przedstawionym certyfikacie. Dokonuje tego poprzez podpisanie losowego numeru wysłanego przez kartę. Karta weryfikuje podpis na losowym numerze. Jeżeli weryfikacja zakończy się powodzeniem, VU zostaje uwierzytelniony. Etap ten nazywany jest uwierzytelnieniem VU i został szczegółowo opisany w sekcji 10.3;

— po trzecie obie strony niezależnie obliczają dwa klucze sesji AES, korzystając z asymetrycznego algorytmu uzgadniania klucza. Korzystając z jednego z tych kluczy sesji karta tworzy kod uwierzytelniania komunikatów (MAC) w odniesieniu do niektórych danych wysłanych przez VU. VU weryfikuje MAC. Jeżeli weryfikacja zakończy się powodzeniem, karta zostaje uwierzytelniona. Etap ten nazywany jest uwierzytelnieniem karty i został szczegółowo opisany w sekcji 10.4;

— po czwarte VU i karta używają zatwierdzonych kluczy sesji w celu zapewnienia poufności, integralności i autentyczności wszystkich wymienianych komunikatów. Etap ten nazywany jest bezpieczną wymianą komunikatów i został szczegółowo opisany w sekcji 10.5.

CSM_156 Mechanizm opisany w CSM_155 jest uruchamiany przez przyrząd rejestrujący za każdym razem, gdy w jeden z czytników kart zostaje włożona karta.

10.2. **Wzajemna weryfikacja łańcucha certyfikatów**

10.2.1 *Weryfikacja łańcucha certyfikatów karty przez VU*

CSM_157 Przyrządy rejestrujące używają protokołu przedstawionego na rys. 4 w celu weryfikacji łańcucha certyfikatów karty do tachografu.

Uwagi do rys. 4:

— certyfikaty i klucze publiczne karty wskazane na rysunku są certyfikatami i kluczami, których używa się do wzajemnego uwierzytelnienia. W sekcji 9.1.5 oznaczono je jako Card_MA;

— certyfikaty i klucze publiczne Card.CA wskazane na rysunku są certyfikatami i kluczami używanymi do podpisywania certyfikatów karty i jest to wskazane w CAR certyfikatu Card.CA. W sekcji 9.1.3 oznaczono je jako MSCA_Card;

— certyfikat Card.CA.EUR wspomniany na rysunku jest europejskim certyfikatem głównym wskazanym w CAR certyfikatu Card.CA;

— certyfikat Card.Link wskazany na rysunku jest certyfikatem łączącym karty, o ile istnieje. Jak określono w sekcji 9.1.2, jest to certyfikat łączący dla nowej pary europejskich kluczy głównych wygenerowanej przez ERCA i podpisanej za pomocą poprzedniego europejskiego klucza prywatnego;

— certyfikat Card.Link.EUR jest europejskim certyfikatem głównym wskazanym w CAR certyfikatu Card.Link.

CSM_158 Jak wskazano na rys. 4, weryfikacja łańcucha certyfikatów karty rozpoczyna się po włożeniu karty. Przyrząd rejestrujący odczytuje odniesienie do posiadacza karty (`cardExtendedSerialNumber`) z pliku elementarnego ICC. VU sprawdza, czy zna kartę tj. czy pomyślnie zweryfikował łańcuch certyfikatów karty w przeszłości i zapisało go na potrzeby przyszłych odniesień. Jeżeli VU zna kartę, certyfikat karty nadal jest ważny, a proces jest kontynuowany i następuje weryfikacja łańcucha certyfikatów VU. W przeciwnym razie VU kolejno odczytuje z karty certyfikat MSCA_Card, który ma służyć do weryfikacji certyfikatu karty Card.CA, certyfikat EUR, który ma służyć do weryfikacji certyfikatu MSCA_Card, oraz ewentualnie certyfikat łączący, do momentu aż znajdzie certyfikat, który rozpozna lub może zweryfikować. Jeżeli znajdzie taki certyfikat, VU używa tego certyfikatu w celu zweryfikowania podstawowych certyfikatów karty, które odczytał z karty. Jeżeli proces przebiegnie pomyślnie, nastąpi weryfikacja łańcucha certyfikatów VU. Jeżeli nie, VU zignoruje kartę.

Uwaga: istnieją trzy sposoby na rozpoznanie certyfikatu Card.CA.EUR przez VU:

— certyfikat Card.CA.EUR jest taki sam jak certyfikat EUR VU;

— certyfikat Card.CA.EUR poprzedza certyfikat EUR VU i VU zawierał już ten certyfikat w chwili wydania (zob. CSM_81);

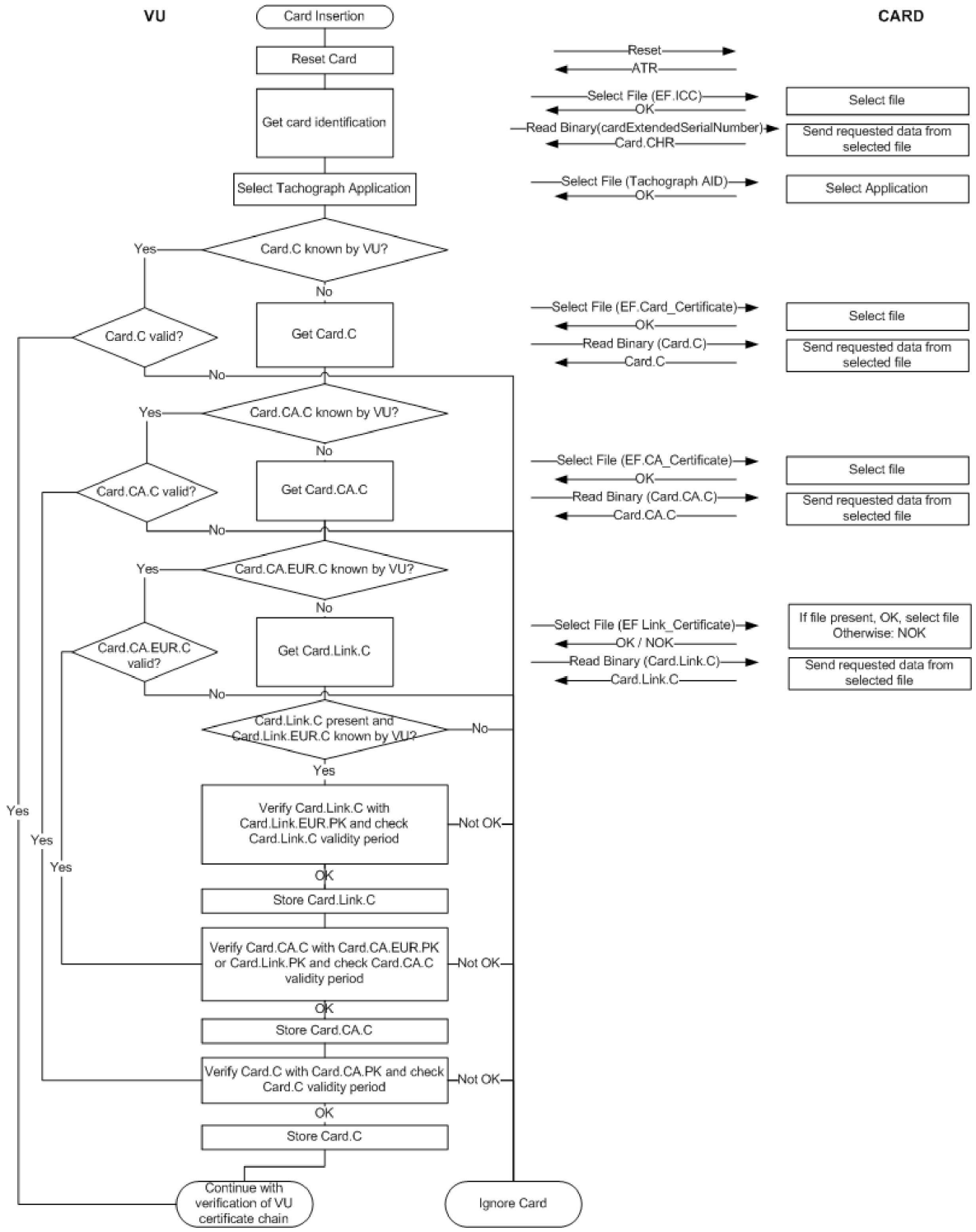
— certyfikat Card.CA.EUR zastępuje certyfikat EUR VU i VU otrzymał w przeszłości certyfikat łączący z innej karty do tachografu, zweryfikował go i zapisał na potrzeby przyszłych odniesień.

CSM_159 Jak wskazano na rys. 4, po zweryfikowaniu przez VU autentyczności i ważności uprzednio nieznanego certyfikatu VU może zapisać ten certyfikat na potrzeby przyszłych odniesień, tak aby nie musiał po raz kolejny weryfikować autentyczności tego certyfikatu, gdy zostanie mu ponownie przedstawiony. Zamiast zapisywać cały certyfikat, VU może zdecydować się na zapisanie jedynie treści certyfikatu, jak określono w sekcji 9.3.2.

CSM_160 VU weryfikuje czasową ważność każdego certyfikatu odczytanego z karty lub przechowywanego w jej pamięci i odrzuca certyfikaty, które wygasły. W celu zweryfikowania czasowej ważności certyfikatu przedstawionego przez kartę VU używa swojego wewnętrznego zegara.

Rys. 4

Protokół weryfikacji łańcucha certyfikatów karty przez VU

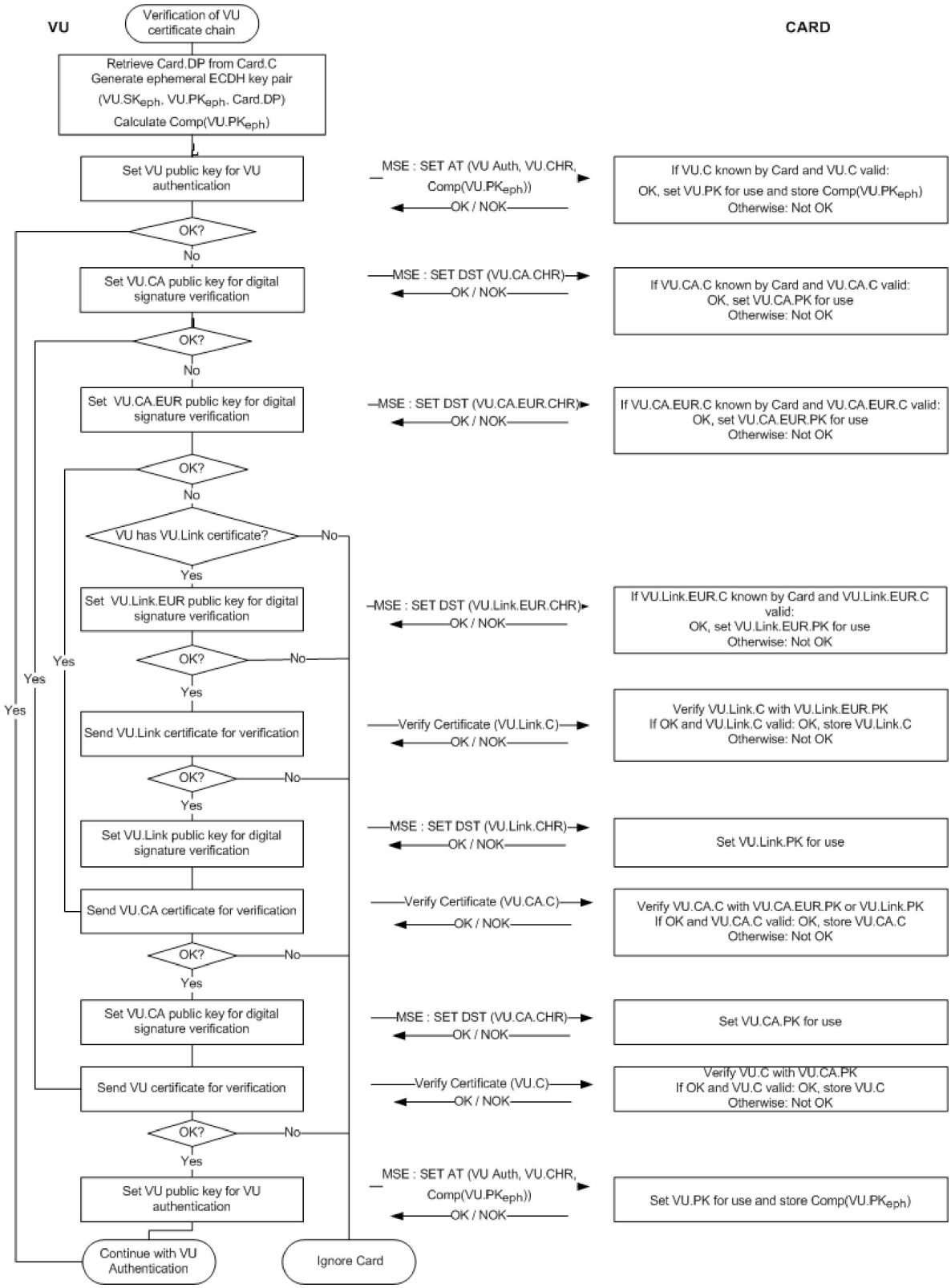


10.2.2 *Weryfikacja łańcucha certyfikatów VU przez kartę*

CSM_161 Karty do tachografu używają protokołu przedstawionego na rys. 5 w celu weryfikacji łańcucha certyfikatów VU.

Rys. 5

Protokół weryfikacji łańcucha certyfikatów VU przez kartę



Uwagi do rys. 5:

— certyfikaty i klucze publiczne VU wskazane na rysunku są certyfikatami i kluczami, których używa się do wzajemnego uwierzytelnienia. W sekcji 9.1.4 oznaczono je jako VU_MA;

— certyfikaty i klucze publiczne VU.CA wskazane na rysunku są certyfikatami i kluczami używanymi do podpisywania certyfikatów VU i urządzenia zewnętrznego GNSS. W sekcji 9.1.3 oznaczono je jako MSCA_VU-EGF;

— certyfikat VU.CA.EUR przedstawiony na rysunku jest europejskim certyfikatem głównym wskazanym w CAR certyfikatu VU.CA;

— certyfikat VU.Link wskazany na rysunku jest certyfikatem łączącym VU, o ile istnieje. Jak określono w sekcji 9.1.2, jest to certyfikat łączący dla nowej pary europejskich kluczy głównych wygenerowanej przez ERCA i podpisanej za pomocą poprzedniego europejskiego klucza prywatnego;

— certyfikat VU.Link.EUR jest europejskim certyfikatem głównym wskazanym w CAR certyfikatu VU.Link.

CSM_162 Jak wskazano na rys. 5, weryfikacja łańcucha certyfikatów przyrządu rejestrującego rozpoczyna się, gdy przyrząd rejestrujący podejmuje próbę ustawienia swojego własnego klucza publicznego w celu użycia go w karcie do tachografu. Jeżeli proces ten powiedzie się, oznacza to, że karta pomyślnie zweryfikowała łańcuch certyfikatów VU w przeszłości i zapisała certyfikat VU na potrzeby przyszłych odniesień. W tym przypadku certyfikat VU ustawia się jako używany, a proces jest kontynuowany i następuje uwierzytelnienie VU. Jeżeli karta nie zna certyfikatu VU, VU kolejno przedstawia certyfikat VU.CA, który ma służyć do weryfikacji certyfikatu VU, certyfikat VU.CA. EUR, który ma służyć do weryfikacji certyfikatu VU.CA, oraz ewentualnie certyfikat łączący, w celu znalezienia certyfikatu rozpoznanego lub weryfikowalnego przez kartę. W przypadku znalezienia takiego certyfikatu karta używa tego certyfikatu do zweryfikowania podstawowych certyfikatów VU przedstawionych jej przez VU. Jeżeli proces przebiegnie pomyślnie, VU ostatecznie ustawi swój klucz publiczny do używania w karcie do tachografu. Jeżeli nie, VU zignoruje kartę.

Uwaga: istnieją dwa sposoby na rozpoznanie certyfikatu VU.CA.EUR:

— certyfikat VU.CA.EUR jest taki sam jak certyfikat EUR karty;

— certyfikat VU.CA.EUR poprzedza certyfikat EUR karty i karta zawierała już ten certyfikat w chwili wydania (zob. CSM_91);

— certyfikat VU.CA.EUR zastępuje certyfikat EUR karty i karta otrzymała w przeszłości certyfikat łączący z innego przyrządu rejestrującego, zweryfikowała go i zapisała na potrzeby przyszłych odniesień.

CSM_163 VU używa polecenia MSE:Set AT, aby ustawić swój klucz publiczny do używania w karcie do tachografu. Jak określono w dodatku 2, polecenie to zawiera opis mechanizmu kryptograficznego, który będzie używany wraz z ustawionym kluczem. Mechanizm ten określa się mianem uwierzytelnienia VU za pomocą algorytmu ECDSA w połączeniu z algorytmem skrótu powiązanym z wielkością pary kluczy VU VU_MA, jak określono w CSM_50.

CSM_164 Polecenie MSE: Set AT zawiera również opis pary kluczy efemerycznych, których VU będzie używał podczas uzgadniania klucza sesji (zob. sekcja 10.4). W związku z tym przed wysłaniem polecenia MSE: Set AT VU generuje parę kluczy efemerycznych ECC. W celu wygenerowania pary kluczy efemerycznych VU używa standardowych parametrów domeny wskazanych w certyfikacie karty. Parę kluczy efemerycznych oznacza się jako ($VU.SK_{eph}$, $VU.PK_{eph}$, Card.DP). VU uznaje współrzędną x efemerycznego punktu publicznego ECDH za identyfikację klucza; określa się to mianem skompresowanej reprezentacji klucza publicznego i oznacza jako $Comp(VU.PK_{eph})$.

CSM_165 Jeżeli polecenie MSE: Set AT jest skuteczne, karta ustawia wskazany VU.PK w celu późniejszego użycia podczas uwierzytelnienia przyrządu rejestrującego i tymczasowo zapisuje $Comp(VU.PK_{eph})$. W przypadku wysłania co najmniej dwóch skutecznych poleceń MSE: Set AT przed uzgodnieniem klucza sesji karta zapisuje tylko ostatni otrzymany $Comp(VU.PK_{eph})$.

CSM_166 Karta weryfikuje czasową ważność każdego certyfikatu przedstawionego przez VU lub wskazanego przez VU przez odniesienie i zapisanego w pamięci karty i odrzuca certyfikaty, które wygasły.

CSM_167 W celu zweryfikowania czasowej ważności certyfikatu przedstawionego przez VU każda karta do tachografu zapisuje wewnętrznie niektóre dane pokazujące czas bieżący. Dane te nie mogą podlegać bezpośredniej aktualizacji przez VU. W momencie wydania czas bieżący karty ustawia się tak, aby odpowiadał dacie wejścia w życie certyfikatu karty Card_MA. Karta aktualizuje swój czas bieżący, jeżeli data wejścia w życie autentycznego certyfikatu będącego „wiarygodnym źródłem czasu" i przedstawionego przez VU jest późniejsza niż czas bieżący określony na karcie. W takim przypadku karta ustawia swój czas bieżący zgodnie z datą wejścia w życie takiego certyfikatu. Za wiarygodne źródło czasu karta uznaje wyłącznie następujące certyfikaty:

— certyfikaty łączące ERCA drugiej generacji

— certyfikaty MSCA drugiej generacji

— certyfikaty VU drugiej generacji wydane przez to samo państwo, które wydało certyfikaty własne karty.

Uwaga: ostatni wymóg oznacza, że karta jest w stanie rozpoznać CAR certyfikatu VU, tj. certyfikatu MSCA_VU-EGF. Nie będzie się on pokrywał z CAR certyfikatu własnego karty, którym jest certyfikat MSCA_Card.

CSM_168 Jak wskazano na rys. 5, po zweryfikowaniu przez kartę autentyczności i ważności uprzednio nieznanego certyfikatu, karta może zapisać ten certyfikat na potrzeby przyszłych odniesień, tak aby nie musiała po raz kolejny weryfikować autentyczności tego certyfikatu, gdy zostanie jej ponownie przedstawiony. Zamiast zapisywać cały certyfikat, karta może zdecydować się na zapisanie jedynie treści certyfikatu, jak określono w sekcji 9.3.2.

10.3. **Uwierzytelnienie VU**

CSM_169 Przyrządy rejestrujące i karty używają protokołu uwierzytelniania Vu wskazanego na rys. 6 w celu uwierzytelnienia VU w stosunku do karty. Uwierzytelnienie VU umożliwia karcie do tachografu wyraźne zweryfikowanie, że VU jest autentyczny. W tym celu VU używa swojego klucza prywatnego do podpisania żądania wygenerowanego przez kartę.

CSM_170 Oprócz żądania karty VU umieszcza w podpisie odniesienie do posiadacza karty uzyskane z certyfikatu karty.

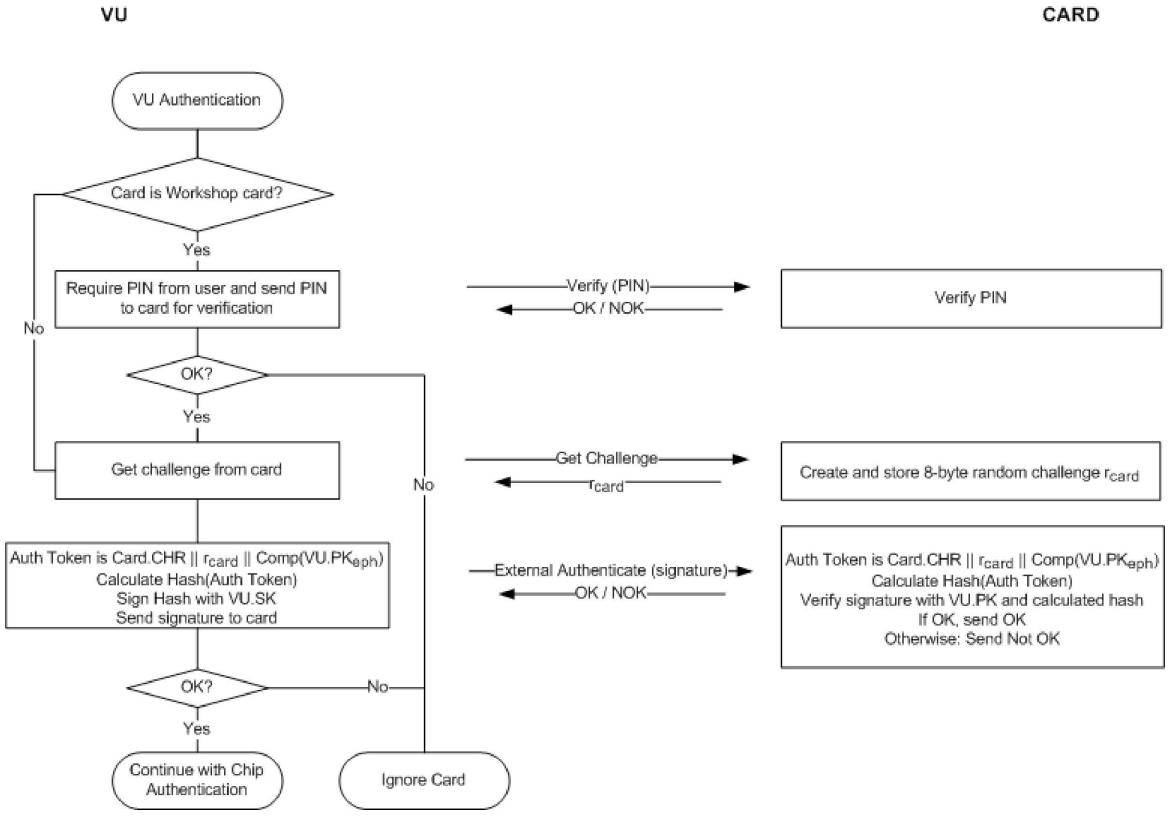
Uwaga: gwarantuje to, że karta, w odniesieniu do której VU się uwierzytelnia, jest tą samą kartą, której łańcuch certyfikatów został wcześniej zweryfikowany przez VU.

CSM_171 VU umieszcza również w podpisie identyfikator efemerycznego klucza publicznego Comp(VU. PK_{eph}), z którego będzie korzystał w celu ustanowienia bezpiecznej wymiany komunikatów podczas procesu uwierzytelniania chipu określonego w sekcji 10.4.

Uwaga: gwarantuje to, że VU, z którym karta komunikuje się podczas sesji bezpiecznej wymiany komunikatów, jest tym samym VU, który został uwierzytelniony przez kartę.

Rys. 6

Protokół uwierzytelniania VU



CSM_172 Jeżeli VU wysyła wielokrotnie polecenie GET CHALLENGE podczas uwierzytelniania VU, karta zwraca za każdym razem nowe 8-bajtowe losowe żądanie, ale zapisuje tylko ostatnie żądanie.

CSM_173 Algorytmem podpisywania używanym przez VU w celu uwierzytelnienia VU jest ECDSA, jak określono w [DSS], używający algorytmu skrótu powiązanego z wielkością klucza pary kluczy VU VU_MA, jak określono w CSM_50. Format podpisu jest odkryty, jak określono w [TR-03111]. VU przesyła uzyskany podpis karcie.

CSM_174 Po otrzymaniu podpisu VU w poleceniu EXTERNAL AUTHENTICATE karta:

— oblicza token uwierzytelniania poprzez połączenie Card.CHR, żądania karty r_{card} i identyfikatora efemerycznego klucza publicznego VU Comp($VU.PK_{eph}$);

— oblicza skrót tokena uwierzytelniania, używając algorytmu skrótu powiązanego z wielkością pary kluczy VU VU_MA, jak określono w CSM_50;

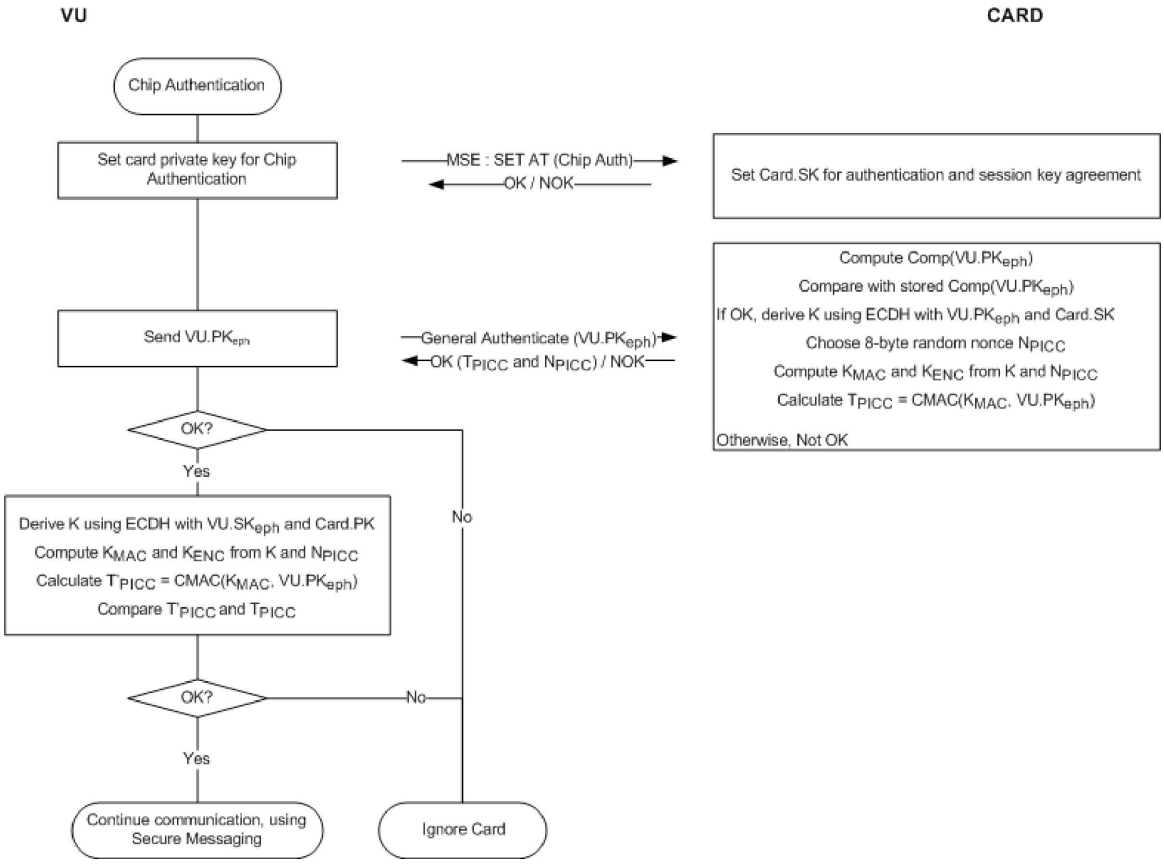
— weryfikuje podpis VU za pomocą algorytmu ECDSA w połączeniu z VU.PK i obliczonym skrótem.

10.4. Uwierzytelnianie chipu i uzgadnianie klucza sesji

CSM_175 Przyrządy rejestrujące i karty korzystają z protokołu uwierzytelniania chipu wskazanego na **rys. 7** w celu uwierzytelnienia karty w stosunku do VU. Uwierzytelnienie chipu umożliwia przyrządowi rejestrującemu wyraźne zweryfikowanie, że karta jest autentyczna.

Rys. 7

Uwierzytelnianie chipu i uzgadnianie klucza sesji



CSM_176 VU i karta podejmują następujące kroki:

1. przyrząd rejestrujący inicjuje proces uwierzytelniania chipu poprzez wysłanie polecenia MSE: Set AT określającego uwierzytelnianie chipu za pomocą algorytmu ECDH, w wyniku którego długość klucza sesji AES jest powiązana z wielkością klucza w parze kluczy karty Card_MA, jak określono w CSM_50. VU określa wielkość klucza w parze kluczy karty na podstawie certyfikatu karty;

2. VU przesyła karcie punkt publiczny $VU.PK_{eph}$ swojej pary kluczy efemerycznych. Jak wyjaśniono w CSM_164, VU wygenerował tę parę kluczy efemerycznych przed zweryfikowaniem łańcucha certyfikatów VU. VU przesłał karcie identyfikator efemerycznego klucza publicznego Comp(VU. PK_{eph}) i karta zapisuje ten identyfikator;

3. karta oblicza Comp($VU.PK_{eph}$) na podstawie $VU.PK_{eph}$ i porównuje go z zapisaną wartością Comp($VU.PK_{eph}$);

4. używając algorytmu ECDH w połączeniu ze statycznym kluczem prywatnym karty i efemerycznym kluczem publicznym VU, karta oblicza tajny K;

5. karta wybiera losowy 8-bajtowy identyfikator jednorazowy N_{PICC} i używa go do wyprowadzenia dwóch kluczy sesji AES K_{MAC} i K_{ENC} z K. Zob. CSM_179;

6. za pomocą K_{MAC}, karta oblicza token uwierzytelniania w odniesieniu do identyfikatora efemerycznego klucza publicznego VU: T_{PICC} = CMAC(K_{MAC}, $VU.PK_{eph}$). Karta wysyła N_{PICC} i T_{PICC} do przyrządu rejestrującego;

7. używając algorytmu ECDH w połączeniu ze statycznym kluczem publicznym karty i efemerycznym kluczem prywatnym VU, przyrząd rejestrujący oblicza ten sam tajny K co karta w ramach kroku 4;

8. VU wyprowadza klucze sesji K_{MAC} i K_{ENC} z K i N_{PICC}; zob. CSM_179;

9. VU weryfikuje token uwierzytelniania T_{PICC}.

CSM_177 W ramach powyższego kroku 3 karta oblicza Comp(VU.PKeph) jako współrzędną x punktu publicznego w VU.PKeph.

CSM_178 W ramach powyższych kroków 4 i 7 karta i przyrząd rejestrujący używają algorytmu ECKA-EG, jak określono w [TR-03111].

CSM_179 W ramach powyższych kroków 5 i 8 karta i przyrząd rejestrujący używają funkcji wyprowadzania klucza w odniesieniu do kluczy sesji AES zdefiniowanych w [TR-03111] z następującą dokładnością i następującymi zmianami:

— wartość licznika wynosi '00 00 00 01' w odniesieniu do K_{ENC} i '00 00 00 02' w odniesieniu do K_{MAC};

— używa się opcjonalnego identyfikatora jednorazowego *r*, który jest równy N_{PICC};

— w celu wyprowadzenia 128-bitowych kluczy AES używa się algorytmu skrótu SHA-256;

— w celu wyprowadzenia 192-bitowych kluczy AES używa się algorytmu skrótu SHA-384;

— w celu wyprowadzenia 256-bitowych kluczy AES używa się algorytmu skrótu SHA-512.

Długość kluczy sesji (tj. długość, do której skrócono skrót) jest powiązana z wielkością pary kluczy Card_MA, jak określono w CSM_50.

CSM_180 W powyższych krokach 6 i 9 karta i przyrząd rejestrujący używają algorytmu AES w trybie CMAC, jak określono w [SP 800-38B]. Długość T_{PICC} jest powiązana z długością kluczy sesji AES, jak określono w CSM_50.

10.5. **Bezpieczna wymiana komunikatów**

10.5.1 *Uwagi ogólne*

CSM_181 Wszystkie polecenia i odpowiedzi wymieniane między przyrządem rejestrującym a kartą do tachografu po pomyślnym uwierzytelnieniu chipu oraz do zakończenia sesji są chronione za pomocą bezpiecznej wymiany komunikatów.

CSM_182 Z wyjątkiem sytuacji, w której ma miejsce odczyt z pliku z warunkiem dostępu SM-R-ENC-MAC-G2 (zob. dodatek 2 sekcja 4), bezpieczną wymianę komunikatów stosuje się w trybie tylko uwierzytelniania. W tym trybie kryptograficzną sumę kontrolną (zwaną również MAC) dodaje się do wszystkich poleceń i odpowiedzi w celu zapewnienia autentyczności i integralności komunikatów.

CSM_183 Przy odczycie danych z pliku z warunkiem dostępu SM-R-ENC-MAC-G2 bezpieczną wymianę komunikatów stosuje się w trybie uwierzytelniania po wcześniejszym zaszyfrowaniu, co oznacza, że dane odpowiedzi najpierw są szyfrowane w celu zapewnienia poufności komunikatu, a następnie obliczany jest MAC w stosunku do sformatowanych zaszyfrowanych danych w celu zapewnienia autentyczności i integralności.

CSM_184 W ramach bezpiecznej wymiany komunikatów stosuje się AES określony w [AES] z kluczami sesji K_{MAC} i K_{ENC} uzgodnionymi w procesie uwierzytelniania chipu.

CSM_185 Jako licznik sekwencji wysyłania (SSC) stosuje się liczbę całkowitą bez znaku w celu zapobieżenia atakom przez powtórzenie. Rozmiar SSC jest równy rozmiarowi bloku AES, tj. wynosi 128 bitów. SSC ma format, w którym najbardziej znaczący bit znajduje się na początku. Licznik sekwencji wysyłania jest zerowany (tj. ma wartość '00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00') w momencie rozpoczęcia bezpiecznej wymiany komunikatów. Wartość SSC jest zwiększana przed każdym wygenerowaniem polecenia lub odpowiedzi APDU, czyli ponieważ wartością początkową SSC w sesji bezpiecznej wymiany komunikatów jest 0, wartość SSC w pierwszym poleceniu będzie wynosiła 1. Wartość SSC dla pierwszej odpowiedzi będzie wynosiła 2.

CSM_186 W przypadku szyfrowania komunikatów stosuje się klucz K_{ENC} z AES w trybie wiązania bloków zaszyfrowanych, jak określono w normie [ISO 10116], z naprzemiennym parametrem m = 1 oraz wektorem inicjującym SV = E(K_{ENC}, SSC), tj. bieżącą wartością licznika sekwencji wysyłania zaszyfrowanego kluczem K_{ENC}.

CSM_187 Do uwierzytelniania komunikatów stosuje się klucz K_{MAC} z AES w trybie CMAC, jak określono w [SP 800-38B]. Długość MAC jest powiązana z długością kluczy sesji AES, jak określono w CSM_50. Licznik sekwencji wysyłania uwzględnia się w MAC poprzez dodanie go przed datagramem, który ma zostać uwierzytelniony.

10.5.2 *Struktura bezpiecznego komunikatu*

CSM_188 W bezpiecznej wymianie komunikatów używa się wyłącznie obiektów danych bezpiecznej wymiany komunikatów (zob. [ISO 7816-4]) wymienionych w tabeli 5. W każdym komunikacie wspomniane obiekty danych stosuje się w kolejności określonej w poniższej tabeli.

Tabela 5

Obiekty danych bezpiecznej wymiany komunikatów

Nazwa obiektu danych	Znacznik	Obecność: obowiązkowa (M), warunkowa (C) lub zabroniona (F) w	
		poleceniach	odpowiedziach
Odkryta wartość niekodowana w BER-TLV	'81'	C	C
Odkryta wartość kodowana w BER-TLV, lecz nie zawiera obiektów danych bezpiecznej wymiany komunikatów	'B3'	C	C
Po wskaźniku treści wypełnienia następuje kryptogram, wartość odkryta nie jest kodowana w BER-TLV	'87'	C	C
Chroniona długość	'97'	C	F
Status przetwarzania	'99'	F	M
Kryptograficzna suma kontrolna	'8E'	M	M

Uwaga: jak określono w dodatku 2, karty do tachografu mogą obsługiwać polecenia READ BINARY i UPDATE BINARY z nieparzystym bajtem INS ('B1' odp. 'D7'). Wymaga się, aby przedstawione warianty poleceń umożliwiały odczyt i aktualizację plików o rozmiarze 32 768 bajtów lub więcej. W przypadku zastosowania takiego wariantu używa się obiektu danych ze znacznikiem 'B3' zamiast obiektu ze znacznikiem '81'. Aby uzyskać więcej informacji, zob. dodatek 2.

CSM_189 Wszystkie obiekty danych bezpiecznej wymiany komunikatów koduje się w DER TLV, jak określono w [ISO 8825-1]. W wyniku takiego kodowania uzyskuje się następującą strukturę TLV:

znacznik: znacznik jest zakodowany w jednym oktecie lub dwóch oktetach i określa treść;

długość: długość jest zakodowana jako liczba całkowita bez znaku w jednym oktecie, dwóch lub trzech oktetach, co skutkuje uzyskaniem maksymalnej długości 65 535 oktetów. Stosuje się minimalną liczbę oktetów;

wartość: wartość nie jest zakodowana w żadnym oktecie lub jest zakodowana w większej liczbie oktetów.

CSM_190 Polecenia APDU chronione bezpieczną wymianą komunikatów generuje się w następujący sposób:

— nagłówek polecenia uwzględnia się w obliczeniach MAC, w związku z czym wartość '0C' stosuje się w przypadku klasy bajtów CLA;

— jak określono w dodatku 2, wszystkie bajty INS są parzyste, ewentualnie z wyjątkiem nieparzystych bajtów INS w przypadku poleceń READ BINARY i UPDATE BINARY;

— wartość rzeczywista Lc zostanie zmieniona na Lc' po zastosowaniu bezpiecznej wymiany komunikatów;

— pole danych składa się z obiektów danych bezpiecznej wymiany komunikatów;

— w chronionym poleceniu APDU nowy bajt Le otrzymuje wartość '00'. W razie konieczności obiekt danych '97' umieszcza się w polu danych w celu przekazania wartości oryginalnej bajtu Le.

CSM_191 Każdy obiekt danych wymagający zaszyfrowania wypełnia się zgodnie z [ISO 7816-4] przy użyciu wskaźnika treści wypełnienia '01'. Na potrzeby obliczenia MAC każdy obiekt danych w APDU wypełnia się również oddzielnie zgodnie z [ISO 7816-4].

Uwaga: wypełnianie na potrzeby bezpiecznej wymiany komunikatów zawsze przeprowadza się za pomocą warstwy bezpiecznej wymiany komunikatów, a nie algorytmów CMAC czy CBC.

Podsumowanie i przykłady

Polecenie APDU z zastosowaniem bezpiecznej wymiany komunikatów będzie miało następującą strukturę w zależności od przypadku odpowiadającego mu niezabezpieczonego polecenia („DO" oznacza obiekt danych):

Przypadek 1:	CLA INS P1 P2 || Lc' || DO '8E' || Le
Przypadek 2:	CLA INS P1 P2 || Lc' || DO '97' || DO'8E' || Le
Przypadek 3 (parzysty bajt INS):	CLA INS P1 P2 || Lc' || DO '81' || DO'8E' || Le
Przypadek 3 (nieparzysty bajt INS):	CLA INS P1 P2 || Lc' || DO 'B3' || DO'8E' || Le
Przypadek 4 (parzysty bajt INS):	CLA INS P1 P2 || Lc' || DO '81' || DO'97' || DO'8E' || Le
Przypadek 4 (nieparzysty bajt INS):	CLA INS P1 P2 || Lc' || DO 'B3' || DO'97' || DO'8E' || Le

gdzie Le = '00' albo '00 00' w zależności od tego, czy stosuje się krótkie długości pól czy rozszerzone długości pól; zob. [ISO 7816-4].

Odpowiedź APDU z zastosowaniem bezpiecznej wymiany komunikatów będzie miała następującą strukturę w zależności od przypadku odpowiadającej mu niezabezpieczonej odpowiedzi:

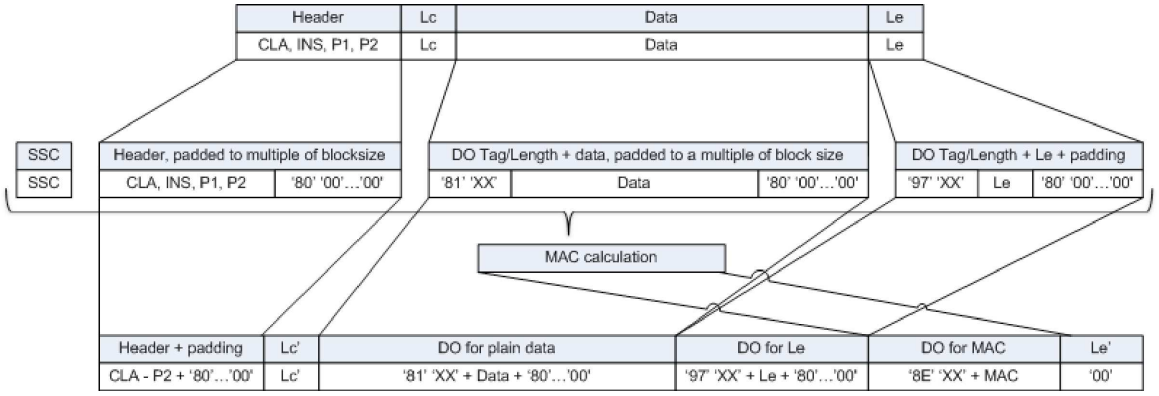
Przypadek 1 lub 3:	DO '99' || DO '8E' || SW1SW2
Przypadek 2 lub 4 (parzysty bajt INS) z szyfrowaniem:	DO '81' || DO '99' || DO '8E' || SW1SW2
Przypadek 2 lub 4 (parzysty bajt INS) bez szyfrowania:	DO '87' || DO '99' || DO '8E' || SW1SW2
Przypadek 2 lub 4 (nieparzysty bajt INS) bez szyfrowania:	DO 'B3' || DO '99' || DO '8E' || SW1SW2

Uwaga: przypadków 2 lub 4 (nieparzysty bajt INS) z szyfrowaniem nigdy nie stosuje się w łączności między VU a kartą.

Poniżej przedstawiono trzy przykłady przekształceń APDU w odniesieniu do poleceń z parzystym kodem INS. Rys. 8 przedstawia uwierzytelnione polecenie APDU określone w przypadku 4, rys. 9 przedstawia uwierzytelnioną odpowiedź APDU określoną w przypadku 2/4, a rys. 10 przedstawia zaszyfrowaną i uwierzytelnioną odpowiedź APDU określoną w przypadku 2/4.

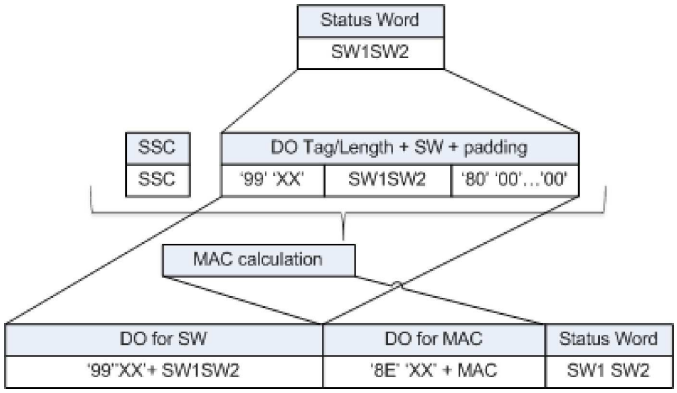
Rys. 8

Przekształcenie uwierzytelnionego polecenia APDU określonego w przypadku 4



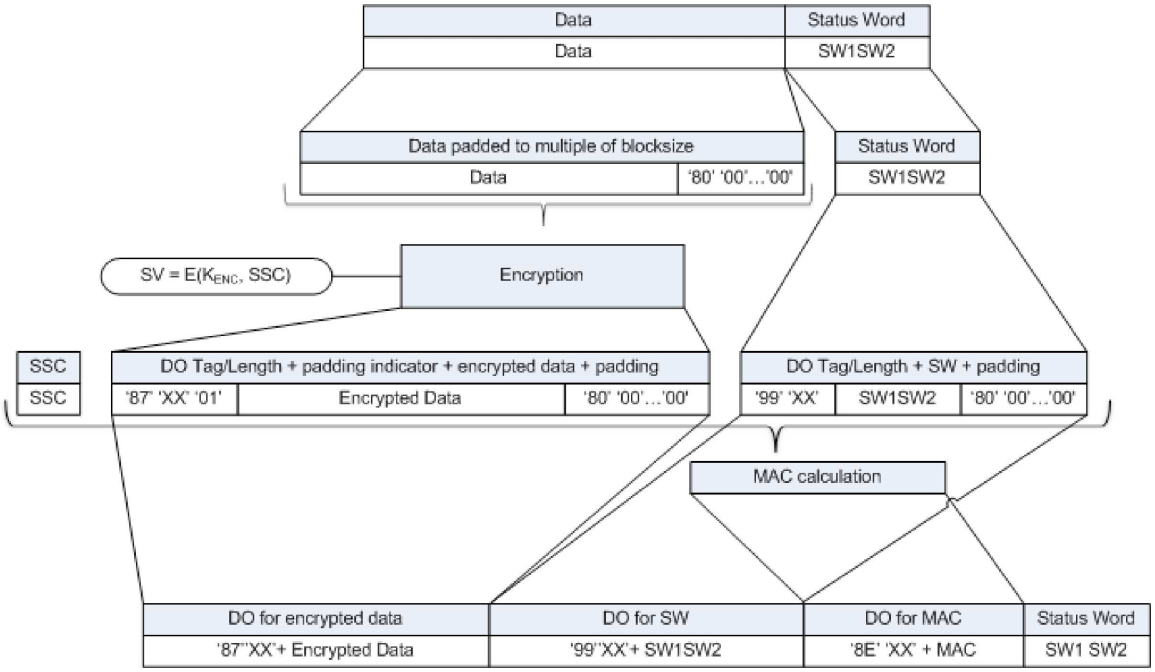
Rys. 9

Przekształcenie uwierzytelnionej odpowiedzi APDU określonej w przypadku 1/3



Rys. 10

Przekształcenie zaszyfrowanej i uwierzytelnionej odpowiedzi APDU określonej w przypadku 2/4



10.5.3 *Przerwanie sesji bezpiecznej wymiany komunikatów*

CSM_192 Przyrząd rejestrujący przerywa trwającą sesję bezpiecznej wymiany komunikatów tylko i wyłącznie wówczas, gdy zaistnieje jeden z poniższych warunków:

— przyrząd otrzyma odkrytą odpowiedź APDU;

— przyrząd wykryje błąd bezpiecznej wymiany komunikatów w odpowiedzi APDU:

— brak oczekiwanego obiektu danych bezpiecznej wymiany komunikatów, nieprawidłową kolejność obiektów danych lub uwzględnienie nieznanego obiektu danych,

— nieprawidłowy obiekt danych bezpiecznej wymiany komunikatów, np. nieprawidłowa wartość MAC, nieprawidłową strukturę TLV lub wskaźnik wypełnienia w znaczniku '87' nie jest równy '01',

— karta wyśle bajt stanu wskazujący na wykrycie błędu bezpiecznej wymiany komunikatów (zob. CSM_194);

— osiągnięty zostanie limit dotyczący liczby poleceń i powiązanych odpowiedzi w ramach bieżącej sesji. Dla danego VU limit ten określa producent, uwzględniając wymogi bezpieczeństwa dotyczące używanego sprzętu, przy czym maksymalna liczba poleceń i powiązanych odpowiedzi w ramach bezpiecznej wymiany komunikatów wynosi 240 w każdej sesji.

CSM_193 Karta do tachografu przerywa trwającą sesję bezpiecznej wymiany komunikatów tylko i wyłącznie wówczas, gdy zaistnieje jeden z poniższych warunków:

— karta otrzyma odkryte polecenie APDU;

— karta wykryje błąd bezpiecznej wymiany komunikatów w poleceniu APDU:

— brak oczekiwanego obiektu danych bezpiecznej wymiany komunikatów, nieprawidłową kolejność obiektów danych lub uwzględnienie nieznanego obiektu danych,

— NIEPRAWIDŁOWY obiekt danych bezpiecznej wymiany komunikatów, np. nieprawidłowa wartość MAC lub nieprawidłowa struktura TLV;

— karta straci zasilanie lub zostanie zresetowana;

— VU wybierze aplikację na karcie;

— VU rozpocznie proces uwierzytelniania VU;

— osiągnięty zostanie limit dotyczący liczby poleceń i powiązanych odpowiedzi w ramach bieżącej sesji. W odniesieniu do danej karty limit ten określa producent, uwzględniając wymogi bezpieczeństwa dotyczące używanego sprzętu, przy czym maksymalna liczba poleceń i powiązanych odpowiedzi w ramach bezpiecznej wymiany komunikatów wynosi 240 w każdej sesji.

CSM_194 W odniesieniu do obsługi błędów w ramach bezpiecznej wymiany komunikatów przez kartę do tachografu:

— jeżeli w poleceniu APDU wystąpi brak niektórych oczekiwanych obiektów danych bezpiecznej wymiany komunikatów, kolejność obiektów danych jest nieprawidłowa lub zawarto nieznane obiekty danych, karta do tachografu wysyła odpowiedź zawierającą bajty stanu '69 87';

— jeżeli w poleceniu APDU obiekt danych bezpiecznej wymiany komunikatów jest nieprawidłowy, karta do tachografu wysyła odpowiedź zawierającą bajty stanu '69 88'.

W takim przypadku bajty stanu są odsyłane bez zastosowania bezpiecznej wymiany komunikatów.

CSM_195 Jeżeli sesja bezpiecznej wymiany komunikatów między VU a kartą do tachografu zostanie przerwana, VU i karta do tachografu:

— w bezpieczny sposób niszczą przechowywane klucze sesji;

— natychmiast ustanawiają nową sesję bezpiecznej wymiany komunikatów, jak opisano w sekcjach 10.2 – 10.5.

CSM_196 Jeżeli z jakiejkolwiek przyczyny VU zdecyduje się ponownie uruchomić proces wzajemnego uwierzytelniania w stosunku do włożonej karty, proces ten ponownie rozpoczyna się od weryfikacji łańcucha certyfikatów karty, jak opisano w sekcji 10.2, i jest kontynuowany, jak opisano w sekcjach 10.2–10.5.

11. POWIĄZANIE, WZAJEMNE UWIERZYTELNIANIE I BEZPIECZNA WYMIANA KOMUNIKATÓW MIĘDZY VU A URZĄDZENIEM ZEWNĘTRZNYM GNSS

11.1. **Uwagi ogólne**

CSM_197 Urządzenie GNSS wykorzystywane przez VU do ustalania jego położenia może być wewnętrzne (tj. wbudowane w obudowę VU i nieodłączalne) bądź też może stanowić moduł zewnętrzny. W pierwszym przypadku standaryzacja łączności wewnętrznej między urządzeniem GNSS a VU nie jest potrzebna, a wymogi określone w tym rozdziale nie mają zastosowania. W drugim przypadku łączność między VU a urządzeniem zewnętrznym GNSS wymaga standaryzacji i ochrony, jak opisano w tym rozdziale.

CSM_198 Bezpieczna łączność między przyrządem rejestrującym a urządzeniem zewnętrznym GNSS odbywa się na takiej samej zasadzie jak bezpieczna łączność między przyrządem rejestrującym a kartą do tachografu, przy czym urządzenie zewnętrzne GNSS przyjmuje rolę karty. Urządzenie zewnętrzne GNSS musi spełniać wszystkie wymogi, o których mowa w rozdziale 10 w odniesieniu do kart do tachografu, z uwzględnieniem odstępstw, wyjaśnień i uzupełnień przedstawionych w tym rozdziale. W szczególności procesy wzajemnej weryfikacji łańcucha certyfikatów, uwierzytelniania VU i uwierzytelniania chipu przeprowadza się w sposób opisany w sekcjach 11.3 i 11.4.

CSM_199 Łączność między przyrządem rejestrującym a EGF różni się od łączności między przyrządem rejestrującym a kartą pod takim względem, że przyrząd rejestrujący i EGF muszą zostać powiązane w warsztacie, zanim będą mogły dokonywać wymiany danych opartych na GNSS w trakcie normalnej pracy. Proces ustanawiania powiązania opisano w sekcji 11.2.

CSM_200 W przypadku łączności między przyrządem rejestrującym a EGF stosuje się polecenia i odpowiedzi APDU na podstawie [ISO 7816-4] i [ISO 7816-8]. Dokładną składnię tych poleceń i odpowiedzi APDU określono w dodatku 2 do niniejszego załącznika.

11.2. **Ustanowienie powiązania między VU a urządzeniem zewnętrznym GNSS**

CSM_201 Powiązanie między przyrządem rejestrującym a EGF w pojeździe ustanawia warsztat. W trakcie normalnej pracy tylko powiązany przyrząd rejestrujący i EGF mogą nawiązywać łączność.

CSM_202 Ustanowienie powiązania między przyrządem rejestrującym a EGF jest możliwe, wyłącznie gdy przyrząd rejestrujący znajduje się w trybie kalibracyjnym. Proces ustanawiania powiązania inicjuje przyrząd rejestrujący.

CSM_203 Warsztat może w dowolnym momencie ponownie połączyć przyrząd rejestrujący z innym lub z tym samym EGF. W trakcie ustanawiania ponownego połączenia VU w sposób bezpieczny niszczy istniejący certyfikat EGF_MA w jego pamięci i przechowuje certyfikat EGF_MA EGF, z którym jest powiązany.

CSM_204 Warsztat może w dowolnym momencie ponownie powiązać urządzenie zewnętrzne GNSS z innym lub tym samym VU. W trakcie ustanawiania ponownego powiązania EGF w sposób bezpieczny niszczy istniejący certyfikat VU_MA w jego pamięci i przechowuje certyfikat VU_MA VU, z którym jest wiązany.

11.3. **Wzajemna weryfikacja łańcucha certyfikatów**

11.3.1 *Uwagi ogólne*

CSM_205 Wzajemna weryfikacja łańcucha certyfikatów między VU a EGF odbywa się wyłącznie w trakcie procesu ustanawiania przez warsztat powiązania między VU a EGF. W czasie normalnej pracy powiązanego VU i EGF nie przeprowadza się weryfikacji certyfikatów. Zamiast tego VU i EGF ufają certyfikatom, które zapisały podczas ustanawiania powiązania, po sprawdzeniu czasowej ważności tych certyfikatów. VU i EGF nie mogą ufać żadnym innym certyfikatom dotyczącym ochrony łączności między VU a EGF w czasie normalnej pracy.

11.3.2 *Podczas ustanawiania powiązania między VU a EGF*

CSM_206 Podczas ustanawiania powiązania z EGF przyrząd rejestrujący używa protokołu przedstawionego na rys. 4 (sekcja 10.2.1) w celu weryfikacji łańcucha certyfikatów urządzenia zewnętrznego GNSS.

Uwagi do rys. 4 w tym kontekście:

— kontrola łączności nie jest objęta zakresem niniejszego dodatku. EGF nie jest jednak inteligentną kartą, a zatem VU prawdopodobnie nie wyśle komunikatu „Reset" w celu nawiązania łączności i nie otrzyma odpowiedzi na ponowne inicjowanie (ATR);

— certyfikaty i klucze publiczne karty wskazane na rysunku interpretuje się jako certyfikaty i klucze publiczne EGF na potrzeby wzajemnego uwierzytelniania. W sekcji 9.1.6 oznaczono je jako EGF_MA;

— certyfikaty i klucze publiczne Card.CA wskazane na rysunku interpretuje się jako certyfikaty i klucze publiczne MSCA na potrzeby podpisywania certyfikatów EGF. W sekcji 9.1.3 oznaczono je jako MSCA_VU-EGF;

— certyfikat Card.CA.EUR przedstawiony na rysunku interpretuje się jako europejski certyfikat główny wskazany w CAR certyfikatu MSCA_VU-EGF;

— certyfikat Card.Link wskazany na rysunku interpretuje się jako certyfikat łączący EGF, o ile istnieje. Jak określono w sekcji 9.1.2, jest to certyfikat łączący dla nowej pary europejskich kluczy głównych wygenerowanej przez ERCA i podpisanej za pomocą poprzedniego europejskiego klucza prywatnego;

— certyfikat Card.Link.EUR jest europejskim certyfikatem głównym wskazanym w CAR certyfikatu Card.Link.

— zamiast `cardExtendedSerialNumber` VU odczyta `sensorGNSSserialNumber` z pliku elementarnego ICC;

— zamiast AID tachografu VU wybiera AID EGF;

— komunikat „Ignore Card" interpretuje się jako komunikat „Ignore EGF".

CSM_207 Po zweryfikowaniu certyfikatu EGF_MA przyrząd rejestrujący zapisuje ten certyfikat do wykorzystania w czasie normalnej pracy; zob. sekcja 11.3.3.

CSM_208 Podczas ustanawiania powiązania z VU zewnętrzna jednostka GNSS używa protokołu przedstawionego na rys. 5 (sekcja 10.2.2) w celu weryfikacji łańcucha certyfikatów VU.

Uwagi do rys. 5 w tym kontekście:

— VU generuje nową parę kluczy efemerycznych przy użyciu parametrów domeny określonych w certyfikacie EGF;

— certyfikaty i klucze publiczne VU wskazane na rysunku są certyfikatami i kluczami, których używa się do wzajemnego uwierzytelnienia. W sekcji 9.1.4 oznaczono je jako VU_MA;

— certyfikaty i klucze publiczne VU.CA wskazane na rysunku są certyfikatami i kluczami używanymi do podpisywania certyfikatów VU i urządzenia zewnętrznego GNSS. W sekcji 9.1.3 oznaczono je jako MSCA_VU-EGF;

— certyfikat VU.CA.EUR przedstawiony na rysunku jest europejskim certyfikatem głównym wskazanym w CAR certyfikatu VU.CA;

— certyfikat VU.Link wskazany na rysunku jest certyfikatem łączącym VU, o ile istnieje. Jak określono w sekcji 9.1.2, jest to certyfikat łączący dla nowej pary europejskich kluczy głównych wygenerowanej przez ERCA i podpisanej za pomocą poprzedniego europejskiego klucza prywatnego;

— certyfikat VU.Link.EUR jest europejskim certyfikatem głównym wskazanym w CAR certyfikatu VU.Link.

CSM_209 W odróżnieniu od wymogu CSM_167 EGF wykorzystuje czas GNSS do celów weryfikacji czasowej ważności każdego przedstawionego certyfikatu.

CSM_210 Po zweryfikowaniu certyfikatu VU_MA zewnętrzna jednostka GNSS przechowuje ten certyfikat do wykorzystania w czasie normalnej pracy; zob. sekcja 11.3.3.

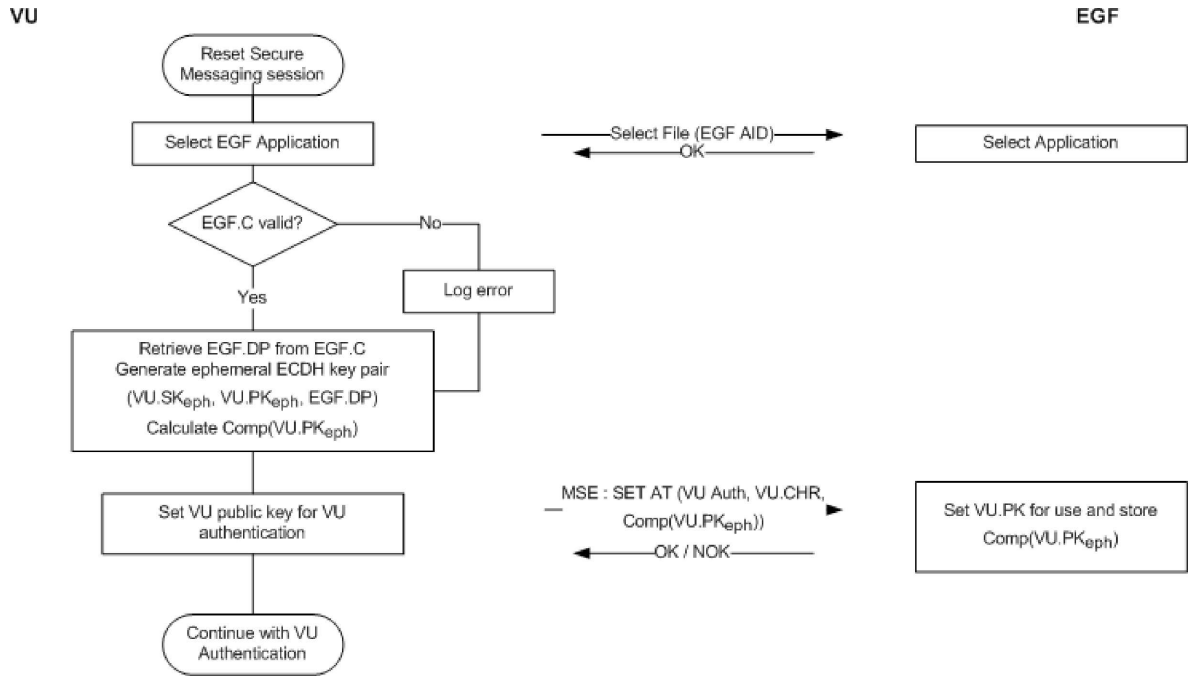
11.3.3 *W czasie normalnej pracy*

CSM_211 W czasie normalnej pracy przyrząd rejestrujący i EGF używają protokołu wskazanego na rys. 11 w celu weryfikacji czasowej ważności przechowywanych certyfikatów EGF_MA i VU_MA oraz do celów ustalenia klucza publicznego VU_MA na potrzeby późniejszego uwierzytelnienia VU. W czasie normalnej pracy nie odbywa się dalsza wzajemna weryfikacja łańcuchów certyfikatów.

Należy zauważyć, że rys. 11 zasadniczo zawiera pierwsze kroki przedstawione na rys. 4 i rys. 5. Ponownie należy zauważyć, że ponieważ EGF nie jest inteligentną kartą, VU prawdopodobnie nie wyśle komunikatu „Reset" w celu nawiązania łączności i nie otrzyma ATR. W żadnym przypadku kwestia ta nie jest objęta zakresem niniejszego dodatku.

Rys. 11

Wzajemna weryfikacja czasowej ważności certyfikatu w czasie normalnej pracy VU–EGF



CSM_212 Jak przedstawiono na rys. 11, przyrząd rejestrujący rejestruje błąd, jeżeli certyfikat EGF_MA nie jest już aktualny. Wzajemne uwierzytelnienie, uzgodnienie klucza i późniejsza łączność za pośrednictwem bezpiecznej wymiany komunikatów odbywa się jednak normalnie.

11.4. Uwierzytelnienie VU, uwierzytelnienie chipu i uzgodnienie klucza sesji

CSM_213 Uwierzytelnienie VU, uwierzytelnienie chipu i uzgodnienie klucza sesji między VU a EGF odbywa się podczas ustanawiania powiązania oraz za każdym razem, gdy sesja bezpiecznej wymiany komunikatów jest ponownie ustanawiana w czasie normalnej pracy. VU i EGF przeprowadzają procesy opisane w sekcjach 10.3 i 10.4. Zastosowanie mają wszystkie wymogi określone w tych sekcjach.

11.5. Bezpieczna wymiana komunikatów

CSM_214 Wszystkie polecenia i odpowiedzi wymieniane między przyrządem rejestrującym a urządzeniem zewnętrznym GNSS po pomyślnym uwierzytelnieniu chipu i do zakończenia sesji są chronione za pomocą bezpiecznej wymiany komunikatów odbywającej się w trybie tylko uwierzytelniania. Zastosowanie mają wszystkie wymogi określone w sekcji 10.5.

CSM_215 W przypadku przerwania sesji bezpiecznej wymiany komunikatów między VU a EGF przyrząd rejestrujący natychmiast ustanawia nową sesję bezpiecznej wymiany komunikatów, jak opisano w sekcjach 11.3.3 i 11.4.

12. PAROWANIE VU Z CZUJNIKIEM RUCHU I ŁĄCZNOŚĆ MIĘDZY TYMI URZĄDZENIAMI

12.1. **Uwagi ogólne**

CSM_216 Łączność pomiędzy przyrządem rejestrującym a czujnikiem ruchu odbywa się za pomocą protokołu interfejsu określonego w [ISO 16844-3] w czasie parowania i normalnej pracy, z uwzględnieniem zmian opisanych w tym rozdziale oraz w sekcji 9.2.1.

Uwaga: zakłada się, że czytelnicy tego rozdziału są zaznajomieni z treścią normy [ISO 16844-3].

12.2. **Parowanie VU z czujnikiem ruchu przy użyciu różnych generacji kluczy**

Jak wyjaśniono w sekcji 9.2.1, klucz główny czujnika ruchu i wszystkie powiązane klucze są regularnie zastępowane. Skutkuje to obecnością do trzech kluczy AES K_{M-WC} związanych z czujnikiem ruchu (kolejnych generacji kluczy) w kartach warsztatowych. Podobnie w czujnikach ruchu może występować do trzech różnych rodzajów szyfrowania danych opartych na AES (na podstawie kolejnych generacji klucza głównego czujnika ruchu K_M). Przyrząd rejestrujący zawiera tylko jeden klucz K_{M-VU} związany z czujnikiem ruchu.

CSM_217 Parowanie VU drugiej generacji i czujnika ruchu drugiej generacji odbywa się w sposób przedstawiony poniżej (por. tabela 6 w [ISO 16844-3]).

1. Kartę warsztatową drugiej generacji wkłada się do VU, który jest połączony z czujnikiem ruchu.

2. VU odczytuje wszystkie dostępne klucze K_{M-WC} z karty warsztatowej, sprawdza ich numery wersji kluczy i wybiera klucz pasujący do numeru wersji klucza K_{M-VU} VU. Jeżeli w karcie warsztatowej nie ma pasującego klucza K_{M-WC}, VU przerywa proces parowania i wyświetla posiadaczowi karty warsztatowej odpowiedni komunikat o błędzie.

3. VU oblicza klucz główny czujnika ruchu K_M na podstawie K_{M-VU} i K_{M-WC} oraz klucz identyfikacyjny K_{ID} na podstawie K_M, jak określono w sekcji 9.2.1.

4. VU wysyła instrukcję rozpoczęcia procesu pasowania w stosunku do czujnika ruchu, jak opisano w normie [ISO 16844-3], i szyfruje numer seryjny otrzymany od czujnika ruchu za pomocą klucza identyfikacyjnego K_{ID}. VU wysyła zaszyfrowany numer seryjny z powrotem do czujnika ruchu.

5. Czujnik ruchu dopasowuje zaszyfrowany numer seryjny kolejno do każdego przechowywanego wewnętrznie zaszyfrowanego numeru seryjnego. Jeżeli znajdzie odpowiedni numer, VU zostaje uwierzytelniony. Czujnik ruchu rejestruje generację klucza K_{ID} użytego przez VU i przekazuje z powrotem pasującą zaszyfrowaną wersję klucza parowania; tj. zaszyfrowany numer stworzony przy zastosowaniu klucza K_M tej samej generacji.

6. VU odszyfrowuje klucz parowania za pomocą klucza K_M, generuje klucz sesji $K_{S,}$ szyfruje go za pomocą klucza parowania i wysyła uzyskany rezultat do czujnika ruchu. Czujnik ruchu odszyfrowuje klucz K_S.

7. VU gromadzi informacje o parowaniu, jak określono w [ISO 16844-3], szyfruje te informacje za pomocą klucza parowania i wysyła uzyskany rezultat do czujnika ruchu. Czujnik ruchu odszyfrowuje informacje o parowaniu.

8. Czujnik ruchu szyfruje otrzymane informacje o parowaniu za pomocą otrzymanego klucza K_S i przesyła te informacje z powrotem do VU. VU sprawdza, czy informacje o parowaniu są tymi samymi informacjami, które VU wysłał do czujnika ruchu w poprzednim kroku. Jeżeli tak, oznacza to, że czujnik ruchu użył tego samego klucza K_S co VU i zgodnie z krokiem 5 wysłał swój klucz parowania zaszyfrowany za pomocą klucza K_M prawidłowej generacji. Czujnik ruchu jest zatem uwierzytelniony.

Należy zauważyć, że kroki 2 i 5 różnią się od standardowego procesu określonego w [ISO 16844-3]; pozostałe kroki są krokami standardowymi.

Przykład: załóżmy, że proces parowania odbywa się w pierwszym roku ważności certyfikatu ERCA (3); zob. rys. 2 w sekcji 9.2.1.2. Ponadto

— załóżmy, że czujnik ruchu wydano w ostatnim roku ważności certyfikatu ERCA (1). Będzie zatem zawierał następujące klucze i dane:

  — N_s[1]: swój numer seryjny zaszyfrowany kluczem K_{ID} 1. generacji;

  — N_s[2]: swój numer seryjny zaszyfrowany kluczem K_{ID} 2. generacji;

  — N_s[3]: swój numer seryjny zaszyfrowany kluczem K_{ID} 3. generacji;

  — K_P[1]: swój klucz parowania 1. generacji ([1]), zaszyfrowany kluczem K_M 1. generacji;

  — K_P[2]: swój klucz parowania 2. generacji, zaszyfrowany kluczem K_M 2. generacji;

  — K_P[3]: swój klucz parowania 3. generacji, zaszyfrowany kluczem K_M 3. generacji;

— załóżmy, że kartę warsztatową wydano w pierwszym roku ważności certyfikatu ERCA (3). Będzie zatem zawierała klucz $K_{M\text{-}WC}$ 2. i 3. generacji;

— załóżmy, że VU jest VU 2. generacji zawierającym klucz $K_{M\text{-}VU}$ 2. generacji.

W takim przypadku w krokach 2–5 zajdą następujące procesy:

— krok 2: VU odczytuje klucze $K_{M\text{-}WC}$ 2. i 3. generacji z karty warsztatowej i sprawdza ich numery wersji;

— krok 3: VU łączy klucz $K_{M\text{-}WC}$ 2. generacji ze swoim kluczem $K_{M\text{-}VU}$ w celu obliczenia kluczy K_M i K_{ID};

— krok 4: VU szyfruje numer seryjny otrzymany od czujnika ruchu za pomocą klucza K_{ID};

— krok 5: czujnik ruchu porównuje otrzymane dane z numerem N_s[1] i nie znajduje odpowiedniego numeru. Następnie porównuje dane z numerem N_s[2] i znajduje odpowiedni numer. Ustala, że VU jest VU 2. generacji, w związku z czym odsyła klucz K_P[2].

12.3. **Parowanie VU z czujnikiem ruchu i łączność między tymi urządzeniami z wykorzystaniem AES**

CSM_218 Zgodnie z tabelą 3 w sekcji 9.2.1 wszystkie klucze uczestniczące w parowaniu przyrządu rejestrującego i czujnika ruchu (drugiej generacji) oraz w późniejszej łączności są kluczami AES, a nie kluczami TDES podwójnej długości, jak określono w [ISO 16844-3]. Takie klucze AES mogą mieć długość 128, 192 lub 256 bitów. Ponieważ rozmiar bloku AES wynosi 16 bajtów, długość zaszyfrowanego komunikatu musi stanowić wielokrotność 16 bajtów, w porównaniu z 8 bajtami w przypadku TDES. Ponadto niektóre takie komunikaty będą wykorzystywane do transportu kluczy AES, których długość może wynosić 128, 192 lub 256 bitów. W związku z tym liczbę bajtów danych zgodnie z instrukcją w tabeli 5 normy [ISO 16844-3] należy zmienić w sposób określony w tabeli 6:

Tabela 6

Liczba bajtów danych zwykłego tekstu i danych zaszyfrowanych zgodnie z instrukcją określoną w [ISO 16844-3]

Instrukcja	Żądanie / odpowiedź	Opis danych	Liczba bajtów danych zwykłego tekstu zgodnie z [ISO 16844-3]	Liczba bajtów danych zwykłego tekstu przy użyciu kluczy AES	Liczba bajtów zaszyfrowanych danych przy użyciu kluczy AES o długości w bitach		
					128	192	256
10	żądanie	Dane uwierzytelniania + numer pliku	8	8	16	16	16

([1]) Należy zauważyć, że klucze parowania 1., 2. i 3. generacji mogą w rzeczywistości być tym samym kluczem lub mogą być trzema różnymi kluczami różnej długości, jak wyjaśniono w CSM_117.

Instrukcja	Żądanie / odpowiedź	Opis danych	Liczba bajtów danych zwykłego tekstu zgodnie z [ISO 16844-3]	Liczba bajtów danych zwykłego tekstu przy użyciu kluczy AES	Liczba bajtów zaszyfrowanych danych przy użyciu kluczy AES o długości w bitach		
					128	192	256
11	odpowiedź	Dane uwierzytelniania + zawartość pliku	16 lub 32 w zależności od pliku	16 lub 32 w zależności od pliku	16 / 32	16 / 32	16 / 32
41	żądanie	Numer seryjny czujnika ruchu	8	8	16	16	16
41	odpowiedź	Klucz parowania	16	16 / 24 / 32	16	32	32
42	żądanie	Klucz sesji	16	16 / 24 / 32	16	32	32
43	żądanie	Informacje o parowaniu	24	24	32	32	32
50	odpowiedź	Informacje o parowaniu	24	24	32	32	32
70	żądanie	Dane uwierzytelniania	8	8	16	16	16
80	odpowiedź	Wartość licznika czujnika ruchu + dane uwierzytelniania	8	8	16	16	16

CSM_219 Informacje o parowaniu wysyłane w instrukcjach 43 (żądanie VU) i 50 (odpowiedź czujnika ruchu) są gromadzone zgodnie z wymogami określonymi w sekcji 7.6.10 normy [ISO 16844-3], z tym że zamiast algorytmu TDES należy stosować algorytm AES w systemie szyfrowania danych dotyczących parowania, co skutkuje uzyskaniem dwóch szyfrów AES i przyjęciem wypełnienia zgodnie z CSM_220 w celu dopasowania do rozmiaru bloku AES. Klucz K'_p, używany do takiego szyfrowania, generuje się w następujący sposób:

— jeżeli długość klucza parowania K_p wynosi 16 bajtów: $K'_p = K_p \text{ XOR } (N_s||N_s)$,

— jeżeli długość klucza parowania K_p wynosi 24 bajty: $K'_p = K_p \text{ XOR } (N_s||N_s||N_s)$,

— jeżeli długość klucza parowania K_p wynosi 32 bajty: $K'_p = K_p \text{ XOR } (N_s||N_s||N_s||N_s)$,

gdzie N_s jest 8-bajtowym numerem seryjnym czujnika ruchu.

CSM_220 Jeżeli długość danych zwykłego tekstu (przy użyciu kluczy AES) nie jest wielokrotnością 16 bajtów, należy stosować metodę wypełniania 2 określoną w normie [ISO 9797-1].

Uwaga: w normie [ISO 16844-3] liczba bajtów danych zwykłego tekstu jest zawsze wielokrotnością 8, tak aby wypełnienie nie było konieczne przy użyciu TDES. Definicja danych i komunikatów w normie [ISO 16844-3] nie jest zmieniona w tej części niniejszego dodatku, co pociąga za sobą konieczność stosowania wypełnienia.

CSM_221 W odniesieniu do instrukcji 11 i w przypadku konieczności zaszyfrowania więcej niż jednego bloku danych stosuje się tryb wiązania bloków zaszyfrowanych zgodnie z wymogami normy [ISO 10116], z naprzemiennym parametrem $m = 1$. Wektorem inicjującym, jaki należy zastosować, jest:

— w przypadku instrukcji 11: 8-bajtowy blok uwierzytelniania zdefiniowany w sekcji 7.6.3.3 normy [ISO 16844-3], wypełniony za pomocą metody wypełniania 2 określonej w normie [ISO 9797-1]; zob. również sekcja 7.6.5 i 7.6.6 normy [ISO 16844-3];

— w przypadku wszystkich pozostałych instrukcji, w których przekazuje się więcej niż 16 bajtów, zgodnie z tabelą 6: '00' {16}, tj. szesnaście bajtów o wartości binarnej 0.

Uwaga: jak przedstawiono w sekcjach 7.6.5 i 7.6.6 normy [ISO 16844-3], w momencie gdy czujnik ruchu szyfruje pliki danych do celów włączenia ich do instrukcji 11, blok uwierzytelniania jest zarówno:

— używany jako wektor inicjujący do celów szyfrowania plików danych w trybie CBC; jak i

— szyfrowany i włączany jako pierwszy blok w danych, które są wysyłane do VU.

12.4. **Parowanie VU z czujnikiem ruchu w przypadku różnych generacji urządzeń**

CSM_222 Jak wyjaśniono w sekcji 9.2.1, czujnik ruchu drugiej generacji może zawierać zaszyfrowane w oparciu o TDES dane dotyczące parowania (zgodnie z częścią A niniejszego dodatku), co umożliwia parowanie tego czujnika ruchu z VU pierwszej generacji. W takim przypadku proces parowania VU pierwszej generacji z czujnikiem ruchu drugiej generacji odbywa się zgodnie z opisem przedstawionym w części A niniejszego dodatku oraz w normie [ISO 16844-3]. Na potrzeby procesu parowania można użyć karty warsztatowej pierwszej lub drugiej generacji.

Uwagi

— Nie jest możliwe sparowanie VU drugiej generacji z czujnikiem ruchu pierwszej generacji.

— Nie jest możliwe użycie karty warsztatowej pierwszej generacji do celów powiązania VU drugiej generacji z czujnikiem ruchu.

13. BEZPIECZEŃSTWO ŁĄCZNOŚCI NA ODLEGŁOŚĆ W RAMACH DSRC

13.1. **Uwagi ogólne**

Jak określono w dodatku 14, VU regularnie generuje dane dotyczące zdalnego monitorowania tachografu (RTM) i wysyła te dane do (wewnętrznego lub zewnętrznego) urządzenia do łączności na odległość (RCF). Urządzenie do łączności na odległość odpowiada za wysłanie tych danych za pośrednictwem interfejsu DSRC opisanego w dodatku 14 do zdalnego interrogatora. W dodatku 1 określono, że dane dotyczące zdalnego monitorowania tachografu stanowią połączenie:

zaszyfrowanego ładunku tachografu zaszyfrowanego zwykłego tekstu ładunku tachografu;

danych zabezpieczające DSRC opisanych poniżej.

Format danych ładunku tachografu zawierających zwykły tekst określono w dodatku 1 i szczegółowo opisano w dodatku 14. W tej sekcji opisano strukturę danych zabezpieczających DSRC; formalne specyfikacje przedstawiono w dodatku 1.

CSM_223 Dane zawierające zwykły tekst `tachographPayload` przekazywane przez VU do urządzenia do łączności na odległość (jeżeli RCF znajduje się na zewnątrz VU) lub przez przyrząd rejestrujący do zdalnego interrogatora za pośrednictwem interfejsu DSRC (jeżeli RCF znajduje się wewnątrz VU) są chronione w trybie uwierzytelnienia po wcześniejszym zaszyfrowaniu, co oznacza, że dane dotyczące ładunku tachografu są najpierw szyfrowane w celu zapewnienia poufności komunikatu, a następnie obliczany jest MAC w celu zapewnienia autentyczności i integralności.

CSM_224 Dane zabezpieczające DSRC składają się z połączenia poniższych elementów danych w następującej kolejności; zob. również rys. 12:

aktualnej daty i godziny	tj. aktualnej data i godziny VU (typ danych `TimeReal`)
licznika	tj. 3-bajtowego licznika, zob. CSM_225

numeru seryjnego VU	tj. numeru seryjnego VU (typ danych `VuSerialNumber`)
numeru wersji klucza głównego DSRC	tj. 1-bajtowego numeru wersji klucza głównego DSRC, z którego wyprowadzono klucze DSRC specyficzne dla VU; zob. sekcja 9.2.2.
MAC	tj. MAC obliczanego na podstawie wszystkich wcześniejszych bajtów w danych dotyczących zdalnego monitorowania tachografu.

CSM_225 3-bajtowy licznik w danych zabezpieczających DSRC ma format, w którym najbardziej znaczący bit znajduje się na początku. Za pierwszym razem, gdy VU oblicza zbiór danych dotyczących zdalnego monitorowania tachografu po rozpoczęciu jego produkcji, ustawia wartość licznika na 0. VU zwiększa wartość licznika o 1 za każdym razem, zanim obliczy kolejny zbiór danych dotyczących zdalnego monitorowania tachografu.

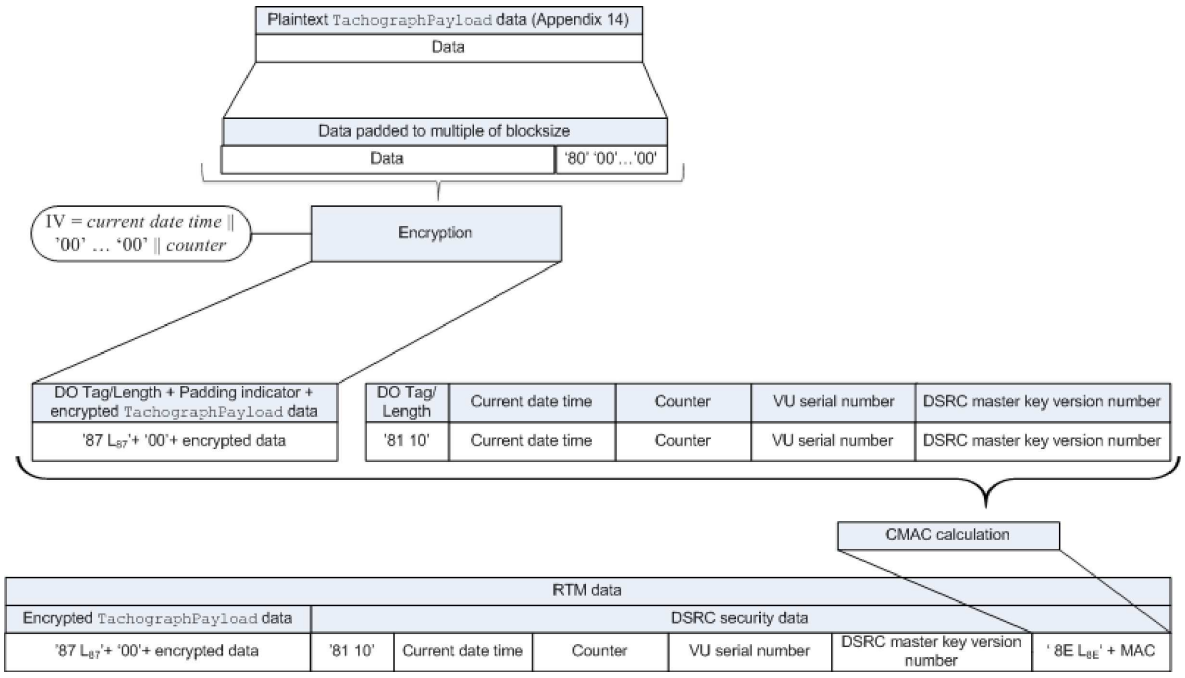
13.2. Szyfrowanie ładunku tachografu i generowanie MAC

CSM_226 Po otrzymaniu elementu danych w formie zwykłego tekstu zawierającego typ danych `TachographPayload` , jak opisano w dodatku 14, VU szyfruje te dane zgodnie z rys. 12: służącego do szyfrowania klucza DSRC przyrządu rejestrującego $K\_VU_{DSRC}\_ENC$ (zob. sekcja9.2.2) używa się wraz z AES w trybie wiązania bloków zaszyfrowanych (CBC), jak określono w [ISO 10116], z naprzemiennym parametrem $m = 1$. Wektor inicjujący ma wartość *IV = aktualna data i godzina || '00 00 00 00 00 00 00 00' || licznik*, przy czym wartości *aktualnej daty i godzina* oraz *licznika* określono w CSM_224. Dane, które mają zostać zaszyfrowane, wypełnia się za pomocą metody 2 określonej w [ISO 9797-1].

CSM_227 VU oblicza MAC w danych zabezpieczających DSRC zgodnie z rys. 12: MAC oblicza się na podstawie wszystkich wcześniejszych bajtów zawartych w danych dotyczących zdalnego monitorowania tachografu, do wartości numeru wersji klucza głównego DSRC włącznie oraz z uwzględnieniem znaczników i długości obiektów danych. VU używa swojego klucza DSRC do zapewnienia autentyczności $K\_VU_{DSRC}\_MAC$ (zob. sekcja 9.2.2) z algorytmem AES w trybie CMAC, jak określono w [SP 800-38B]. Długość MAC jest powiązana z długością kluczy DSRC specyficznych dla VU, jak określono w CSM_50.

Rys. 12

Szyfrowanie ładunku tachografu i generowanie MAC



13.3. **Weryfikacja i odszyfrowywanie ładunku tachografu**

CSM_228 Gdy zdalny interrogator otrzymuje od VU dane dotyczące zdalnego monitorowania tachografu, wysyła wszystkie dane dotyczące zdalnego monitorowania tachografu do karty kontrolnej w polu danych polecenia PROCESS DSRC MESSAGE, jak opisano w dodatku 2. Następnie:

1. karta kontrolna sprawdza numer wersji klucza głównego DSRC w danych zabezpieczających DSRC. Jeżeli karta kontrolna nie rozpozna wskazanego klucza głównego DSRC, zwraca komunikat o błędzie określony w dodatku 2 i przerywa proces;

2. karta kontrolna stosuje wskazany klucz główny DSRC w połączeniu z numerem seryjnym VU zawartym w danych zabezpieczających DSRC w celu wyprowadzenia kluczy DSRC K_VU_{DSRC}_ENC i K_VU_{DSRC}_MAC specyficznych dla VU, jak określono w CSM_124;

3. karta kontrolna używa klucza K_VU_{DSRC}_MAC do weryfikacji MAC zawartego w danych zabezpieczających DSRC, jak określono w CSM_227. Jeżeli MAC jest nieprawidłowy, karta kontrolna zwraca komunikat o błędzie określony w dodatku 2 i przerywa proces;

4. karta kontrolna wykorzystuje klucz K_VU_{DSRC}_ENC do celów odszyfrowania zaszyfrowanego ładunku tachografu, jak określono w CSM_226. Karta kontrolna usuwa wypełnienie i odsyła odszyfrowane dane ładunku tachografu do zdalnego interrogatora.

CSM_229 W celu zapobieżenia atakom przez powtórzenie zdalny interrogator weryfikuje aktualność danych dotyczących zdalnego monitorowania tachografu poprzez sprawdzenie, czy *aktualna data i godzina* zawarta w danych zabezpieczających DSRC nie odbiega zbytnio od czasu bieżącego zdalnego interrogatora.

Uwagi

— W tym celu konieczne jest, aby zdalny interrogator posiadał dokładne i wiarygodne źródło czasu.

— Ponieważ dodatek 14 zawiera wymóg, aby VU obliczał nowy zbiór danych dotyczących zdalnego monitorowania tachografu co 60 sekund, a zegar VU może odbiegać od czasu rzeczywistego o 1 minutę, dolna granica w odniesieniu do aktualności danych dotyczących zdalnego monitorowania tachografu wynosi 2 minuty. Faktyczna aktualność, jaka jest wymagana, zależy również od dokładności zegara zdalnego interrogatora.

CSM_230 Gdy warsztat weryfikuje prawidłowość działania funkcji DSRC VU, wysyła wszystkie otrzymane od VU dane dotyczące zdalnego monitorowania tachografu do karty warsztatowej w polu danych polecenia PROCESS DSRC MESSAGE, jak opisano w dodatku 2. Karta warsztatowa przeprowadza wszystkie kontrole i działania określone w wymogu CSM_228.

14. PODPISYWANIE POBIERANYCH DANYCH I SPRAWDZANIE PODPISÓW

14.1. **Uwagi ogólne**

CSM_231 Inteligentne urządzenie dedykowane (IDE) przechowuje dane otrzymane z VU lub karty podczas jednej sesji pobierania w jednym fizycznym pliku danych. Dane mogą być przechowywane na zewnętrznym nośniku danych. Plik zawiera podpisy cyfrowe bloków danych zgodnie z opisem znajdującym się w dodatku 7. Plik ten zawiera również następujące certyfikaty (zob. sekcja 9.1):

— w przypadku pobierania przez VU:

— certyfikat VU_Sign;

— certyfikat MSCA_VU-EGF zawierający klucz publiczny służący do weryfikacji certyfikatu VU_Sign;

— w przypadku pobierania przez kartę:

— certyfikat Card_Sign;

— certyfikat MSCA_Card zawierający klucz publiczny służący do weryfikacji certyfikatu Card_Sign.

CSM_232 IDE posiada również:

— w przypadku gdy używa karty kontrolnej do weryfikacji podpisu, jak wskazano na rys. 13: certyfikat łączący najnowszy certyfikat EUR z certyfikatem EUR, którego okres ważności wygasa bezpośrednio przed okresem ważności tego najnowszego certyfikatu EUR, o ile istnieje;

— w przypadku gdy samodzielnie weryfikuje podpis: wszystkie ważne europejskie certyfikaty główne.

Uwaga: metody stosowanej przez IDE do pobierania tych certyfikatów nie określono w niniejszym dodatku.

14.2. **Generowanie podpisu**

CSM_233 Algorytmem podpisywania służącym do tworzenia podpisów cyfrowych w odniesieniu do pobieranych danych jest ECDSA, jak określono w [DSS], używający algorytmu skrótu powiązanego z wielkością klucza VU lub karty, jak określono w CSM_50. Format podpisu jest odkryty, jak określono w [TR-03111].

14.3. **Weryfikacja podpisu**

CSM_234 IDE może samodzielnie przeprowadzać weryfikację podpisu złożonego w odniesieniu do pobranych danych lub może do tego celu używać karty kontrolnej. W przypadku używania karty kontrolnej weryfikacja podpisów odbywa się zgodnie ze schematem przedstawionym na rys. 13. W przypadku gdy urządzenie samodzielnie przeprowadza weryfikację podpisy, IDE weryfikuje autentyczność i ważność wszystkich certyfikatów w łańcuchu certyfikatów w pliku danych oraz weryfikuje podpis złożony w stosunku do danych według schematu podpisu określonego w [DSS].

Uwagi do rys. 13:

— urządzenie, które podpisuje dane przeznaczone do analizowania, oznaczono EQT.

— certyfikaty i klucze publiczne ETQ wskazane na rysunku są certyfikatami i kluczami używanymi do podpisywania, tj. VU_Sign lub Card_Sign;

— certyfikaty EQT.CA i klucze publiczne wskazane na rysunku są certyfikatami i kluczami używanymi do podpisywania w stosownych przypadkach certyfikatów VU lub kart;

— certyfikat EQT.CA.EUR wskazany na rysunku jest europejskim certyfikatem głównym wskazanym w CAR certyfikatu EQT.CA;

— certyfikat EQT.Link wskazany na rysunku jest certyfikatem łączącym EQT, o ile istnieje. Jak określono w sekcji 9.1.2, jest to certyfikat łączący dla nowej pary europejskich kluczy głównych wygenerowanej przez ERCA i podpisanej za pomocą poprzedniego europejskiego klucza prywatnego;

— certyfikat EQT.Link.EUR jest europejskim certyfikatem głównym wskazanym w CAR certyfikatu EQT.Link.

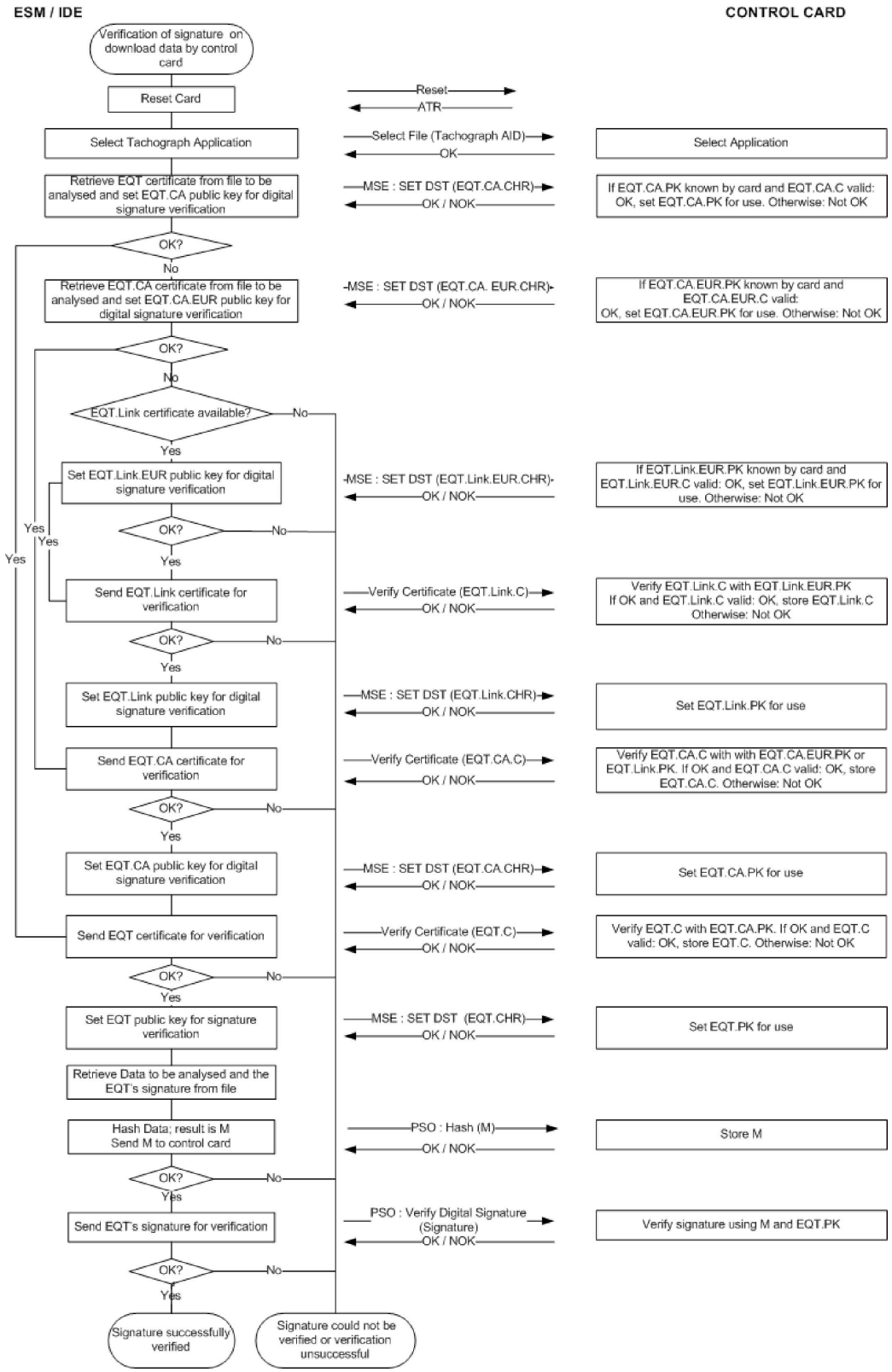
CSM_235 Do celów obliczania skrótu M wysyłanego do karty kontrolnej w poleceniu PSO:Hash IDE stosuje algorytm skrótu powiązany z wielkością klucza VU lub karty, z których dane są pobierane, jak określono w CSM_50.

CSM_236 Do celów zweryfikowania podpisu EQT karta kontrolna wykonuje czynności według schematu podpisu określonego w [DSS].

Uwaga: w niniejszym dokumencie nie określono żadnego działania, jakie należy podjąć, jeżeli podpisu złożonego w odniesieniu do pobranego pliku danych nie można zweryfikować lub jeżeli weryfikacja się nie powiedzie.

Rys. 13

Protokół weryfikacji podpisu złożonego w odniesieniu do pobranego pliku danych



Dodatek 12

OKREŚLANIE POŁOŻENIA Z WYKORZYSTANIEM GLOBALNEGO SYSTEMU NAWIGACJI SATELITARNEJ (GNSS)

SPIS TREŚCI

1. WPROWADZENIE

Niniejszy dodatek zawiera wymogi techniczne dotyczące danych GNSS wykorzystywanych przez przyrząd rejestrujący, z uwzględnieniem protokołów, które należy wdrożyć w celu zapewnienia bezpiecznego i prawidłowego przesyłania danych z informacjami o położeniu.

Głównymi artykułami w niniejszym rozporządzeniu (UE) nr 165/2014, na których opierają się te wymogi, są: „Artykuł 8 Zapisywanie położenia pojazdu w pewnych punktach podczas dziennego okresu pracy", „Artykuł 10 Interfejs do inteligentnych systemów transportowych" oraz „Artykuł 11 Szczegółowe przepisy dotyczące inteligentnych tachografów".

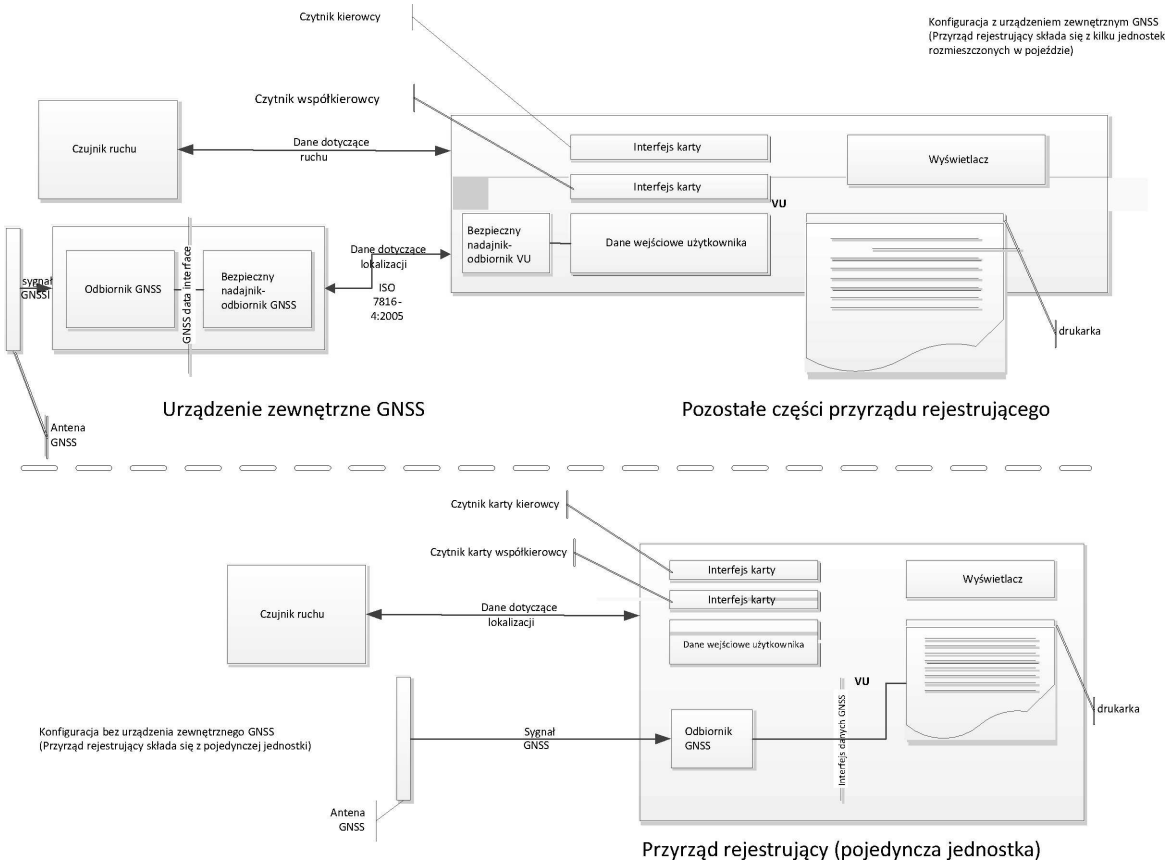
1.1. **Zakres stosowania**

GNS_1 Przyrząd rejestrujący musi gromadzić dane dotyczące lokalizacji z co najmniej jednego GNSS w celu wsparcia wdrożenia przepisów art. 8.

Przyrząd rejestrujący może posiadać urządzenie zewnętrzne GNSS lub nie, jak przedstawiono na rys. 1:

Rys. 1

Różne konfiguracje odbiornika GNSS.



1.2. **Akronimy i skróty**

W niniejszym dodatku używa się następujących skrótów:

DOP Rozmycie dokładności

EGF Plik elementarny urządzenia GNSS

GNSS Globalny system nawigacji satelitarnej

EGNOS Europejski system wspomagania satelitarnego

GSA Rozmycie dokładności GPS i aktywne satelity

HDOP Poziome rozmycie dokładności

ICD Dokument kontroli interfejsu

NMEA National Marine Electronics Association

PDOP Trójwymiarowe rozmycie dokładności

RMC Zalecane minimalne dane GNSS

SIS Sygnał w przestrzeni

VDOP Pionowe rozmycie dokładności

VU Przyrząd rejestrujący

2. SPECYFIKACJA ODBIORNIKA GNSS

Niezależnie od konfiguracji tachografu inteligentnego z urządzeniem zewnętrznym GNSS lub bez niego, dostarczanie dokładnych i wiarygodnych informacji o położeniu jest niezbędne do zapewnienia skutecznego funkcjonowania tachografów inteligentnych. W związku z tym należy wprowadzić wymóg zapewnienia kompatybilności tego systemu z usługami świadczonymi przez programy Galileo i European Geostationary Navigation Overlay Service (EGNOS), które zostały określone w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 1285/2013 ([1]). System ustanowiony w ramach programu Galileo jest niezależnym światowym systemem nawigacji satelitarnej, zaś system ustanowiony w ramach programu EGNOS jest regionalnym systemem nawigacji satelitarnej poprawiającym jakość sygnału globalnego systemu pozycjonowania.

GNS_2 Producenci zapewniają, aby odbiorniki GNSS instalowane w tachografach inteligentnych były kompatybilne z usługami w zakresie lokalizacji zapewnianymi przez systemy Galileo i EGNOS. Ponadto producenci mogą również wybrać kompatybilność z innymi systemami nawigacji satelitarnej.

GNS_3 Odbiornik GNSS musi być zdolny do obsługi uwierzytelniania sygnałów usługi otwartej systemu Galileo, kiedy usługę taką będzie oferował system Galileo i gdy będzie ona wspierana przez producentów odbiorników GNSS. Jednak w przypadku tachografów inteligentnych wprowadzonych do obrotu przed spełnieniem powyższych warunków i niezdolnych do wspierania uwierzytelnienia usługi otwartej Galileo, modernizacja nie będzie wymagana.

3. KOMUNIKATY NMEA

Niniejsza sekcja zawiera opis komunikatów NMEA wykorzystywanych w funkcjonowaniu tachografu inteligentnego. Sekcja ta ma zastosowanie w odniesieniu do konfiguracji tachografu inteligentnego z urządzeniem zewnętrznym GNSS lub bez niego.

GNS_4 Dane dotyczące lokalizacji opierają się na zalecanych minimalnych danych GNSS (RMC) w komunikacie NMEA, który zawiera informacje o położeniu (długość i szerokość geograficzną), czas w formacie UTC (ggmmss,ss), prędkość nad dnem wyrażoną w węzłach oraz dodatkowe wartości.

Format komunikatu RMC jest następujący (według standardu NMEA V4.1):

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1285/2013 z dnia 11 grudnia 2013 r. w sprawie realizacji i eksploatacji europejskich systemów nawigacji satelitarnej oraz uchylające rozporządzenie Rady (WE) nr 876/2002 i rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 683/2008 (Dz.U. L 347 z 20.12.2013, s. 1).

Rys. 2

Struktura komunikatu RMC

1) Czas (UTC)
2) Status, A = prawidłowe położenie, V = ostrzeżenie
3) Szerokość geograficzna
4) N lub S
5) Długość geograficzna
6) E lub W
7) Prędkość nad dnem w węzłach
8) Tor prawidłowy, stopnie prawidłowe
9) Data, ddmmrr
10) Deklinacja magnetyczna w stopniach
11) E lub W
12) Suma kontrolna

Parametr „Status" informuje o tym, czy sygnał GNSS jest dostępny. Dopóki wartość „Statusu" nie zostanie ustawiona na „A", otrzymywanych danych (np. dotyczących czasu lub długości/szerokości geograficznej) nie można wykorzystywać do rejestrowania położenia pojazdu w VU.

Dokładność położenia opiera się na formacie komunikatu RMC opisanym powyżej. Pierwszą część pól 3) i 5) (dwie pierwsze wartości) wykorzystuje się do określenia stopni. Pozostałe określają minuty kątowe z dokładnością do trzech miejsc po przecinku. Zatem dokładność wynosi 1/1 000 minuty kątowej lub 1/60 000 stopnia (ponieważ jedna minuta to 1/60 stopnia).

GNS_5 Przyrząd rejestrujący przechowuje w bazie danych VU informacje o położeniu dotyczące szerokości i długości geograficznej z dokładnością 1/10 minuty kątowej lub 1/600 stopnia, jak określono w dodatku 1 w odniesieniu do współrzędnych geograficznych „GeoCoordinates".

VU może wykorzystać polecenie GSA (dotyczące rozmycia dokładności GPS i aktywnych satelitów) w celu ustalenia i zarejestrowania gotowości i dokładności sygnału. W szczególności HDOP stosuje się w celu wskazania poziomu dokładności zarejestrowanych danych dotyczących lokalizacji (zob. pkt 4.2.2). VU będzie przechowywał wartość poziomego rozmycia dokładności (HDOP) obliczaną jako minimum wartości HDOP zgromadzonych w dostępnych systemach GNSS.

Identyfikator GNSS wskazuje system GPS, Glonass, Galileo, Beidou lub system wspomagający oparty na wyposażeniu satelitarnym SBAS.

Rys. 3

Struktura komunikatu GSA

1) Tryb wyboru
2) Tryb
3) ID pierwszego satelity użytego do ustalenia położenia
4) ID drugiego satelity użytego do ustalenia położenia
...
14) ID dwunastego satelity użytego do ustalenia położenia
15) PDOP w metrach
16) HDOP w metrach
17) VDOP w metrach
18) Identyfikator GNSS
19) Suma kontrolna

gdzie „Tryb" (2) wskazuje, czy ustalenie położenia jest niemożliwe (Tryb = 1) lub czy ustalenie położenia możliwe dla pozycji 2D (Tryb = 2) lub 3D (Tryb = 3).

GNS_6 Komunikat *GSA* przechowuje się z numerem rekordu „06".

GNS_7 Maksymalny rozmiar komunikatów NMEA (np. RMC, GSA lub innych), jaki można zastosować w celu ustalenia rozmiaru polecenia Read Record, wynosi 85 bajtów (zob. tabela 1).

4. PRZYRZĄD REJESTRUJĄCY Z URZĄDZENIEM ZEWNĘTRZNYM GNSS

4.1. **Konfiguracja**

4.1.1 *Główne elementy składowe i interfejsy*

W tej konfiguracji odbiornik GNSS stanowi część urządzenia zewnętrznego GNSS.

GNS_8 Urządzenie zewnętrzne GNSS musi być obsługiwane przez specjalny interfejs pojazdu.

GNS_9 Urządzenie zewnętrzne GNSS składa się z następujących elementów składowych (zob. rys. 4):

a) komercyjnego odbiornika GNSS zapewniającego dane o położeniu za pośrednictwem interfejsu danych GNSS. Przykładowo interfejs danych GNSS może być w standardzie NMEA V4.10, gdzie odbiornik GNSS pełni funkcję nadajnika i przesyła komunikaty NMEA do bezpiecznego nadajnika-odbiornika GNSS z częstotliwością 1 Hz dla zdefiniowanego wcześniej zbioru komunikatów NMEA, który musi zawierać co najmniej komunikaty RMC i GSA. Wdrożenie interfejsu danych GNSS zależy od uznania producentów urządzeń zewnętrznych GNSS;

b) zespołu nadajnika-odbiornika (bezpiecznego nadajnika-odbiornika GNSS) zdolnego do zapewnienia zgodności z wymogami normy ISO/IEC 7816-4:2013 (zob. pkt 4.2.1) w celu łączenia się z przyrządem rejestrującym i obsługi interfejsu danych GNSS odbiornika GNSS. Zespół ten jest wyposażony w pamięć do przechowywania danych identyfikacyjnych z odbiornika GNSS i urządzenia zewnętrznego GNSS;

c) systemu obudowy z funkcją wykrywania manipulowania, obejmującego zarówno odbiornik GNSS, jak i bezpieczny nadajnik-odbiornik GNSS. Funkcja wykrywania manipulowania umożliwia wdrażanie środków bezpieczeństwa zgodnie z wymogami określonymi w profilu zabezpieczenia tachografu inteligentnego;

d) anteny GNSS zainstalowanej na pojeździe i połączonej z odbiornikiem GNSS poprzez system obudowy.

GNS_10 Urządzenie zewnętrzne GNSS posiada co najmniej następujące interfejsy zewnętrzne:

a) interfejs anteny GNSS zainstalowanej na pojeździe ciężarowym w przypadku korzystania z anteny zewnętrznej;

b) interfejs przyrządu rejestrującego.

GNS_11 W VU bezpieczny nadajnik-odbiornik VU znajduje się na drugim końcu bezpiecznej łączności z bezpiecznym nadajnikiem-odbiornikiem GNSS i musi zapewniać zgodność z wymogami normy ISO/IEC 7816-4:2013 w zakresie łączności z urządzeniem zewnętrznym GNSS.

GNS_12 W zakresie warstwy fizycznej łączności z urządzeniem zewnętrznym GNSS przyrząd rejestrujący musi zapewniać zgodność z wymogami normy ISO/IEC 7816-12:2005 lub innej normy zgodnej z normą ISO/IEC 7816-4:2013 (zob. pkt 4.2.1).

4.1.2 *Stan urządzenia zewnętrznego GNSS na koniec procesu produkcji*

GNS_13 Urządzenie zewnętrzne GNSS przechowuje następujące wartości w pamięci trwałej bezpiecznego nadajnika-odbiornika GNSS w momencie opuszczenia zakładu produkcyjnego:

— parę kluczy EGF_MA i powiązany certyfikat;

— certyfikat MSCA_VU-EGF zawierający klucz publiczny MSCA_VU-EGF.PK służący do weryfikacji certyfikatu EGF_MA;

— certyfikat EUR zawierający klucz publiczny EUR.PK służący do weryfikacji certyfikatu MSCA_VU-EGF;

— certyfikat EUR, którego okres ważności wygasa bezpośrednio przed okres ważności certyfikatu EUR służącego do celów weryfikacji certyfikatu MSCA_VU-EGF, o ile istnieje;

— certyfikat łączący wspomniane dwa certyfikaty EUR, o ile istnieje;

— rozszerzony numer seryjny urządzenia zewnętrznego GNSS;

— identyfikator systemu operacyjnego urządzenia GNSS;

— numer homologacji typu urządzenia zewnętrznego GNSS;

— identyfikator elementu zabezpieczenia modułu zewnętrznego GNSS.

4.2. **Łączność między urządzeniem zewnętrznym GNSS a przyrządem rejestrującym**

4.2.1 *Protokół łączności*

GNS_14 Protokół łączności między urządzeniem zewnętrznym GNSS a przyrządem rejestrującym obsługuje trzy funkcje:

1. gromadzenie i rozpowszechnianie danych GNSS (np. położenie, czas, prędkość);
2. gromadzenie danych dotyczących konfiguracji urządzenia zewnętrznego GNSS;
3. protokół zarządzania na potrzeby obsługi powiązania, wzajemnego uwierzytelnienia i uzgadniania klucza sesji między urządzeniem zewnętrznym GNSS a VU.

GNS_15 Protokół łączności bazuje na wymogach normy ISO/IEC 7816-4:2013, przy czym bezpieczny nadajnik-odbiornik VU odgrywa rolę nadrzędną, a bezpieczny nadajnik-odbiornik GNSS – rolę podrzędną. Fizyczne połączenie między urządzeniem zewnętrznym GNSS a przyrządem rejestrującym bazuje na normie ISO/IEC 7816-12:2005 lub innej normie zgodnej z normą ISO/IEC 7816-4:2013.

GNS_16 W protokole łączności nie są obsługiwane pola o rozszerzonej długości.

GNS_17 Protokół łączności bazujący na wymogach normy ISO 7816 (zarówno *-4:2013, jak i *-12:2005) między urządzeniem zewnętrznym GNSS a VU ustawia się na wartość T=1.

GNS_18 Jeżeli chodzi o funkcje 1) gromadzenia i rozpowszechniania danych GNSS; 2) gromadzenia danych dotyczących konfiguracji urządzenia zewnętrznego GNSS; oraz 3) protokołu zarządzania, bezpieczny nadajnik-odbiornik GNSS symuluje inteligentną kartę za pomocą architektury systemu plików składającej się z pliku głównego (MF), pliku katalogowego (DF) z identyfikatorem aplikacji określonym w dodatku 1 rozdział 6.2 ('FF 44 54 45 47 4D') i z trzema plikami elementarnymi (EF) zawierającymi certyfikaty oraz jednego pojedynczego pliku elementarnego (EF.EGF) z identyfikatorem pliku równym '2F2F', jak opisano w tabeli 1.

GNS_19 Bezpieczny nadajnik-odbiornik GNSS przechowuje dane z odbiornika GNSS i konfigurację w pliku elementarnym EF.EGF. Jest to liniowy plik rekordu o zmiennej długości z identyfikatorem równym '2F2F' w formacie heksadecymalnym.

GNS_20 Bezpieczny nadajnik-odbiornik GNSS używa pamięci do przechowywania danych, która jest w stanie przeprowadzić co najmniej 20 milionów cyklów zapisu/odczytu. Poza tym aspektem o konstrukcji wewnętrznej i wdrażaniu bezpiecznego nadajnika-odbiornika GNSS decydują producenci.

Mapowanie numerów rekordów i danych przedstawiono w tabeli 1. Należy zauważyć, że istnieją cztery komunikaty GSA dotyczące czterech systemów satelitarnych i systemu wspomagającego opartego na wyposażeniu satelitarnym SBAS.

GNS_21 Strukturę plików przedstawiono w tabeli 1. Aby uzyskać informacje na temat warunków dostępu (ALW, NEV, SM-MAC), zob. dodatek 2 rozdział 3.5.

Tabela 1

Struktura plików

		Warunki dostępu		
Plik	Identyfikator pliku	Odczyt	Aktualizacja	Zaszyfrowany
Plik główny (MF)	3F00			
EF.ICC	0002	ALW	NEV (przez VU)	Nie
Plik katalogowy urządzenia GNSS	0501	ALW	NEV	Nie
EF EGF_MACertificate	C100	ALW	NEV	Nie
EF CA_Certificate	C108	ALW	NEV	Nie
EF Link_Certificate	C109	ALW	NEV	Nie
EF.EGF	2F2F	SM-MAC	NEV (przez VU)	Nie

Plik / element danych	Nr rekordu	Rozmiar (w bajtach)		Wartości domyślne
		Min.	Maks.	
Plik główny (MF)		552	1 031	
EF.ICC				
sensorGNSSSerialNumber		8	8	
Plik katalogowy urządzenia GNSS		*612*	*1 023*	
EF EGF_MACertificate		*204*	*341*	
EGFCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF.EGF				
Komunikat RMC NMEA	‘01’	85	85	
Pierwszy komunikat GSA NMEA	‘02’	85	85	
Drugi komunikat GSA NMEA	‘03’	85	85	

Plik / element danych	Nr rekordu	Rozmiar (w bajtach)		Wartości domyślne
		Min.	Maks.	
Trzeci komunikat GSA NMEA	'04'	85	85	
Czwarty komunikat GSA NMEA	'05'	85	85	
Piąty komunikat GSA NMEA	'06'	85	85	
Rozszerzony numer seryjny urządzenia zewnętrznego GNSS zdefiniowany w dodatku 1 jako „SensorGNSSSerialNumber".	'07'	8	8	
Identyfikator systemu operacyjnego bezpiecznego nadajnika-odbiornika GNSS zdefiniowany w dodatku 1 jako „SensorOSIdentifier".	'08'	2	2	
Numer homologacji typu urządzenia zewnętrznego GNSS zdefiniowany w dodatku 1 jako „SensorExternalGNSSApprovalNumber".	'09'	16	16	
Identyfikator elementu zabezpieczenia urządzenia zewnętrznego GNSS zdefiniowany w dodatku 1 jako „SensorExternalGNSSSCIdentifier".	'10'	8	8	
RFU – zastrzeżony do wykorzystania w przyszłości	Od '11' do 'FD'			

4.2.2 *Bezpieczne przesyłanie danych GNSS*

GNS_22 Bezpiecznie przesyłanie danych GNSS o położeniu jest dozwolone wyłącznie w następujących warunkach:

1. proces powiązania został przeprowadzony w sposób opisany w dodatku 11 „Wspólne mechanizmy zabezpieczenia";

2. proces okresowego wzajemnego uwierzytelniania i uzgadniania klucza sesji między VU a urządzeniem zewnętrznym GNSS, również opisany w dodatku 11 „Wspólne mechanizmy zabezpieczenia", przeprowadzono ze wskazaną częstotliwością.

GNS_23 Co T sekund, gdzie T jest wartością nie większą niż 10, chyba że trwa proces powiązania lub wzajemnego uwierzytelnienia i uzgadniania klucza sesji, VU żąda od urządzenia zewnętrznego GNSS przesłania informacji o położeniu w oparciu o poniższy schemat.

1. VU żąda od urządzenia zewnętrznego GNSS przesłania danych dotyczących lokalizacji wraz z danymi dotyczącymi rozmycia precyzji (z komunikatu NMEA GSA). Bezpieczny nadajnik-odbiornik VU stosuje zgodne z wymogami normy ISO/IEC 7816-4:2013 polecenia SELECT i READ RECORD (S) w trybie tylko uwierzytelniania bezpiecznej wymiany komunikatów, jak opisano w dodatku 11 sekcja 11.5, z identyfikatorem pliku '2F2F' i numerem zapisu „01" w przypadku komunikatu NMEA RMC oraz '02','03','04','05','06' w przypadku komunikatu NMEA GSA.

2. Dane dotyczące lokalizacji otrzymane jako ostatnie są przechowywane w pliku elementarnym z identyfikatorem '2F2F' i rekordami opisanymi w tabeli 1 w bezpiecznym nadajniku-odbiorniku GNSS, ponieważ bezpieczny nadajnik-odbiornik GNSS otrzymuje dane NMEA z częstotliwością co najmniej 1 Hz od odbiornika GNSS za pośrednictwem interfejsu danych GNSS.

3. Bezpieczny nadajnik-odbiornik GNSS wysyła odpowiedź do bezpiecznego nadajnika-odbiornika VU za pomocą komunikatu odpowiedzi APDU w trybie tylko uwierzytelniania bezpiecznej wymiany komunikatów, zgodnie z opisem przedstawionym w dodatku 11 sekcja 11.5.

4. Bezpieczny nadajnik-odbiornik VU weryfikuje autentyczność i integralność otrzymanej odpowiedzi. W przypadku pozytywnego wyniku dane dotyczące lokalizacji są przekazywane do procesora VU za pośrednictwem interfejsu danych GNSS.

5. Procesor VU sprawdza otrzymane dane, wyodrębniając informacje (np. o długości geograficznej, szerokości geograficznej, czasie) z komunikatu NMEA RMC. Komunikat RMC NMEA zawiera informację o tym, czy położenie jest prawidłowe. Jeżeli położenie nie jest prawidłowe, dane dotyczące lokalizacji nie są jeszcze dostępne i nie można ich wykorzystać w celu zarejestrowania położenia pojazdu. Jeżeli położenie jest prawidłowe, procesor VU wyodrębnia również wartości HDOP z komunikatów NMEA GSA i oblicza średnią wartość w stosunku do dostępnych systemów satelitarnych (tj. jeżeli ustalenie położenia jest możliwe).

6. Procesor VU przechowuje otrzymane i przetworzone informacje, takie jak długość geograficzna, szerokość geograficzna, czas i prędkość, w VU w formacie zdefiniowanym w słowniku danych w dodatku 1 jako współrzędne geograficzne „GeoCoordinates" wraz z wartością HDOP obliczoną jako minimum z wartości HDOP zgromadzonych w ramach dostępnych systemów GNSS.

4.2.3 *Struktura polecenia Read Record*

Poniższa sekcja zawiera szczegółowy opis struktury polecenia Read Record. Zgodnie z opisem przedstawionym w dodatku 11 „Wspólne mechanizmy zabezpieczenia" dodaje się funkcję bezpiecznej wymiany komunikatów (tryb tylko uwierzytelniania).

GNS_24 Polecenie to obsługuje tryb tylko uwierzytelniania bezpiecznej wymiany komunikatów, zob. dodatek 11.

GNS_25 Komunikat polecenia

Bajt	Długość	Wartość	Opis
CLA	1	'0Ch'	Żądanie bezpiecznej wymiany komunikatów
INS	1	'B2h'	Odczyt rekordu
P1	1	'XXh'	Numer rekordu ('00' oznacza bieżący rekord)
P2	1	'04h'	Odczytaj rekord o numerze rekordu wskazanym w P1
Le	1	'XXh'	Długość oczekiwanych danych. Liczba bajtów do odczytu

GNS_26 Rekord wskazany w P1 staje się rekordem bieżącym.

Bajt	Długość	Wartość	Opis
#1-#X	X	'XX..XXh'	Odczyt danych
SW	2	'XXXXh'	Słowo stanu (SW1, SW2)

— jeżeli wykonanie polecenia zakończyło się pomyślnie, bezpieczny nadajnik-odbiornik GNSS zwraca komunikat '**9000**',

— jeżeli bieżący plik nie jest ukierunkowany na rekord, bezpieczny nadajnik-odbiornik GNSS zwraca komunikat **'6981'**,

— jeżeli stosuje się polecenie z P1= '00', lecz nie ma żadnego bieżącego pliku elementarnego, bezpieczny nadajnik-odbiornik GNSS zwraca komunikat **'6986'** (polecenie niedozwolone),

— jeżeli nie znaleziono rekordu, bezpieczny nadajnik-odbiornik GNSS zwraca komunikat '**6A 83**',

— jeżeli urządzenie zewnętrzne GNSS wykryje manipulowanie, zwraca słowa stanu „**66 90**".

GNS_27 Bezpieczny nadajnik-odbiornik GNSS obsługuje następujące polecenia tachografów 2. generacji, wyszczególnione w dodatku 2:

Polecenie	Odniesienie
Select	Dodatek 2 rozdział 3.5.1
Read Binary	Dodatek 2 rozdział 3.5.2
Get Challenge	Dodatek 2 rozdział 3.5.4
PSO: Verify Certificate	Dodatek 2 rozdział 3.5.7
External Authenticate	Dodatek 2 rozdział 3.5.9
General Authenticate	Dodatek 2 rozdział 3.5.10
MSE:SET	Dodatek 2 rozdział 3.5.11

4.3. **Powiązanie, wzajemne uwierzytelnienie i uzgodnienie klucza sesji między urządzeniem zewnętrznym GNSS a przyrządem rejestrującym**

Proces powiązania, wzajemnego uwierzytelniania i uzgadniania klucza sesji między urządzeniem zewnętrznym GNSS a przyrządem rejestrującym opisano w rozdziale 11 dodatku 11 „Wspólne mechanizmy zabezpieczenia".

4.4. **Obsługa błędów**

W niniejszej sekcji opisano sposób obsługi potencjalnych warunków błędów przez urządzenie zewnętrzne GNSS oraz ich rejestrowania w VU.

4.4.1 *Błąd komunikacji z urządzeniem zewnętrznym GNSS*

GNS_28 Jeżeli VU nie jest nawiązać połączenia z powiązanym urządzeniem zewnętrznym GNSS przez dłużej niż 20 minut ciągłej pracy, przyrząd generuje i rejestruje zdarzenie typu „EventFaultType" z wartością enum '53'H *Usterka komunikacji z urządzeniem zewnętrznym GNSS* oraz ze znacznikiem czasu ustawionym na bieżącą godzinę. Zdarzenie zostanie wygenerowane, wyłącznie jeżeli spełnione będą następujące dwa warunki: a) tachograf inteligentny nie znajduje się w trybie kalibracyjnym; oraz b) pojazd jest w ruchu. W tym kontekście występuje błąd połączenia, gdy bezpieczny nadajnik-odbiornik VU nie otrzyma komunikatu odpowiedzi po wysłaniu komunikatu żądania, jak opisano w pkt 4.2.

4.4.2 *Naruszenie integralności fizycznej urządzenia zewnętrznego GNSS*

GNS_29 W przypadku naruszenia integralności fizycznej urządzenia zewnętrznego GNSS bezpieczny nadajnik-odbiornik GNSS kasuje całą swoją pamięć, w tym materiał kryptograficzny. Jak opisano w GNS_25 i GNS_26, VU wykrywa manipulowanie, jeżeli odpowiedź ma status '6690'. Następnie VU generuje zdarzenie typu „EventFaultType" z wartością enum '*55'H Wykrywanie manipulowania GNSS*.

4.4.3 *Brak informacji o położeniu z odbiornika GNSS*

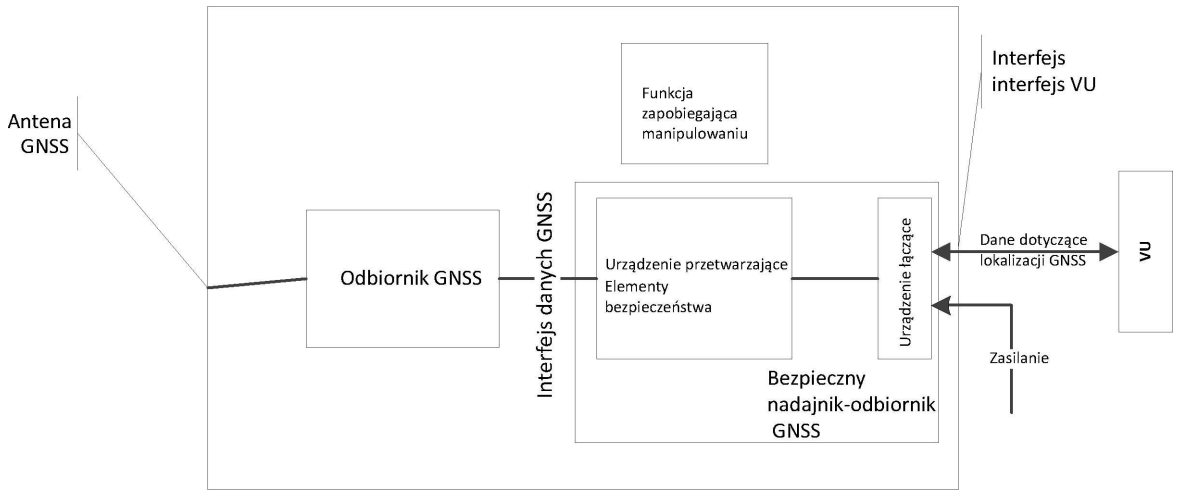
GNS_30 Jeżeli bezpieczny nadajnik-odbiornik GNSS nie otrzymuje danych z odbiornika GNSS przez dłużej niż 3 godziny ciągłej pracy, urządzenie to generuje komunikat odpowiedzi na polecenie READ RECORD z numerem rekordu '01' i polem danych o rozmiarze 12 bajtów, wszystkich ustawionych na 0xFF. Po otrzymaniu komunikatu odpowiedzi z określoną wartością pola danych VU generuje i rejestruje zdarzenie typu „EventFaultType" z wartością enum '52'H *Usterka zewnętrznego odbiornika GNSS* ze znacznikiem czasu o bieżącej wartości czasu, wyłącznie jeżeli spełnione będą następujące dwa warunki: a) tachograf inteligentny nie znajduje się w trybie kalibracyjnym; oraz b) pojazd jest w ruchu.

4.4.1 *Wygaśnięcie certyfikatu urządzenia zewnętrznego GNSS*

GNS_31 Jeżeli VU wykryje, że certyfikat EGF wykorzystywany do celów wzajemnego uwierzytelniania stracił ważność, przyrząd generuje i rejestruje usterkę urządzenia rejestrującego typu „EventFaultType" z wartością enum *'56'H Wygaśnięcie certyfikatu urządzenia zewnętrznego GNSS* ze znacznikiem czasu o bieżącej wartości czasu. VU nadal wykorzystuje otrzymane dane GNSS o położeniu.

Rys. 4

Schemat urządzenia zewnętrznego GNSS



5. PRZYRZĄD REJESTRUJĄCY BEZ URZĄDZENIA ZEWNĘTRZNEGO GNSS

5.1. Konfiguracja

W tej konfiguracji odbiornik GNSS znajduje się wewnątrz przyrządu rejestrującego, jak przedstawiono na rys. 1.

GNS_32 Odbiornik GNSS pełni funkcję nadajnika i przesyła komunikaty NMEA do procesora VU, który pełni funkcję odbiornika o częstotliwości 1/10 Hz lub większej dla zdefiniowanego wcześniej zbioru komunikatów NMEA, który musi obejmować co najmniej komunikaty RMC i GSA.

GNS_33 Do VU musi być podłączona zewnętrzna antena GNSS zainstalowana na pojeździe lub wewnętrzna antena GNSS.

5.2. Obsługa błędów

5.2.1 *Brak informacji o położeniu z odbiornika GNSS*

GNS_34 Jeżeli VU nie otrzymuje danych z odbiornika GNSS przez dłużej niż 3 godziny ciągłej pracy, przyrząd ten generuje i rejestruje zdarzenie typu „EventFaultType" z wartością enum '51'H *Usterka wewnętrznego odbiornika GNSS* ze znacznikiem czasu o bieżącej wartości czasu, wyłącznie jeżeli spełnione będą następujące dwa warunki: a) tachograf inteligentny nie znajduje się w trybie kalibracyjnym; oraz b) pojazd jest w ruchu.

6. KONFLIKT CZASOWY GNSS

Jeżeli VU wykryje rozbieżność wynoszącą ponad 1 minutę między czasem funkcji pomiaru czasu przyrządu rejestrującego a czasem z odbiornika GNSS, przyrząd zarejestruje zdarzenie typu „EventFaultType" z wartością enum *'0B'H Konflikt czasowy (GNSS a wewnętrzny zegar VU)*. Zdarzenie to jest rejestrowane wraz z wartością wyświetlaną na wewnętrznym zegarze przyrządu rejestrującego i wiąże się z automatyczną korektą czasu. Po wywołaniu zdarzenia dotyczącego konfliktu czasowego VU nie weryfikuje rozbieżności czasu przez następne 12 godzin. Zdarzenie nie zostanie wywołane w przypadkach, w których odbiornik GNSS nie mógł wykryć prawidłowego sygnału GNSS przez ostatnie 30 dni. Jeżeli jednak informacje o położeniu z odbiornika GNSS będą ponownie dostępne, następuje automatyczna korekta czasu.

7. KONFLIKT RUCHU POJAZDU

GNS_35 VU wyzwala i rejestruje zdarzenie *Konflikt ruchu pojazdu* (zob. w wymaganiu 84 w niniejszym załączniku) znacznikiem czasu o bieżącej wartości czasu, jeżeli informacje o ruchu z czujnika ruchu są sprzeczne z informacjami o ruchu obliczonymi z wewnętrznego odbiornika GNSS lub urządzenia zewnętrznego GNSS. W celu wykrycia takich sprzeczności wartość mediany różnicy prędkości pochodzących z tych źródeł należy stosować w sposób określony poniżej:

— maksymalnie co 10 sekund należy obliczać wartość bezwzględną różnicy między różnicą prędkości pojazdu szacowaną na podstawie danych z odbiornika GNSS a różnicą szacowaną na podstawie danych z czujnika ruchu,

— wartość mediany oblicza się wykorzystując wszystkie obliczone wartości w oknie czasu obejmującym pięć ostatnich minut ruchu,

— wartość mediany oblicza się jako średnią 80 % wartości pozostałych po wyeliminowaniu najwyższych wartości bezwzględnych,

zdarzenie *Konflikt ruchu pojazdu* jest wyzwalane jeżeli wartość mediany jest wyższa niż 10 km/h przez pięć nieprzerwanych minut ruchu pojazdu. Opcjonalnie można wykorzystać inne niezależne źródła wykrywania ruchu pojazdu, aby zapewnić skuteczniejsze wykrywanie manipulacji związanych z tachografem. (Uwaga: medianę z ostatnich 5 minut stosuje się aby zmniejszyć ryzyko związane z wartościami skrajnymi pomiaru i wartościami chwilowymi). Zdarzenie takie nie uruchamia się w następujących warunkach: a) podczas przeprawy promowej / przejazdu kolejowego; b) jeżeli informacje o położeniu z odbiornika GNSS nie są dostępne; oraz c) podczas trwania trybu kalibracyjnego.

Dodatek 13

INTERFEJS ITS

SPIS TREŚCI

1. WPROWADZENIE

W niniejszym dodatku określono strukturę oraz procedury, które należy zastosować w celu wdrożenia interfejsu do inteligentnych systemów transportowych (ITS) zgodnie z art. 10 rozporządzenia (UE) nr 165/2014 („*Rozporządzenie*").

W *Rozporządzeniu* określono, że tachografy pojazdów mogą być wyposażone w znormalizowane interfejsy pozwalające na wykorzystywanie przez urządzenie zewnętrzne danych rejestrowanych lub generowanych przez tachograf w trybie operacyjnym, z zastrzeżeniem spełnienia następujących warunków:

a) interfejs nie ma wpływu na autentyczność i integralność danych tachografu;

b) interfejs spełnia wymogi szczegółowych przepisów art. 11 *Rozporządzenia*;

c) urządzenie zewnętrzne podłączone do interfejsu uzyskuje dostęp do danych osobowych, w tym do danych geopozycyjnych, dopiero po udzieleniu przez kierowcę, którego te dane dotyczą, podlegającej weryfikacji zgody.

2. ZAKRES

Celem niniejszego dodatku jest określenie sposobu, w jaki aplikacje zainstalowane na urządzeniach zewnętrznych mogą uzyskiwać dane (*Dane*) z tachografu poprzez połączenie Bluetooth®.

Dane dostępne za pośrednictwem tego interfejsu są opisane w załączniku 1 do niniejszego dokumentu. Stosowanie przedmiotowego interfejsu nie uniemożliwia wdrożenia innych interfejsów (np. za pośrednictwem szyny CAN) do celów przekazywania danych z VU do innych jednostek przetwarzania pojazdu.

W niniejszym dodatku określa się:

— *Dane* dostępne za pośrednictwem interfejsu ITS;

— profil Bluetooth® wykorzystywany do przesyłania danych;

— procedury zapytywania i pobierania oraz sekwencję operacji;

— mechanizm parowania między tachografem a urządzeniem zewnętrznym;

— mechanizm udzielania zgody udostępniony kierowcy.

W tym miejscu należy wyjaśnić, że w niniejszym załączniku nie określa się:

— operacji gromadzenia *Danych* i zarządzania tym procesem w ramach VU (co jest określone w innym miejscu w *Rozporządzeniu* lub w przeciwnym razie stanowi funkcję projektu produktu);

— formy przedstawienia zgromadzonych danych w aplikacji zainstalowanej na urządzeniu zewnętrznym;

— przepisów dotyczących bezpieczeństwa danych wykraczających poza zabezpieczenia zapewniane przez Bluetooth® (takie jak szyfrowanie) w odniesieniu do treści *Danych* (które zostaną określone w innym miejscu w *Rozporządzeniu* [dodatek 10 „Wspólne mechanizmy zabezpieczenia"]);

— protokołów Bluetooth® wykorzystywanych przez interfejs ITS.

2.1. **Skróty, definicje i oznaczenia**

W niniejszym dodatku stosuje się następujące skróty i definicje właściwe dla tego dodatku:

Łączność	wymiana informacji/danych między jednostką centralną (tj. tachografem) a jednostką zewnętrzną poprzez interfejs ITS za pośrednictwem połączenia Bluetooth®
Dane	zbiory danych określone w załączniku 1
Rozporządzenie	rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 165/2014 z dnia 4 lutego 2014 r. w sprawie tachografów stosowanych w transporcie drogowym i uchylające rozporządzenie Rady (EWG) nr 3821/85 w sprawie urządzeń rejestrujących stosowanych w transporcie drogowym oraz zmieniające rozporządzenie (WE) nr 561/2006 Parlamentu Europejskiego i Rady w sprawie harmonizacji niektórych przepisów socjalnych odnoszących się do transportu drogowego
BR	podstawowa szybkość
EDR	zwiększona szybkość danych
GNSS	globalny system nawigacji satelitarnej
IRK	klucz do ustalania tożsamości
ITS	inteligentny system transportowy
LE	niski poziom energii
PIN	osobisty numer identyfikacyjny
PUC	osobisty szyfr odblokowujący
SID	identyfikator usługi
SPP	profil portu szeregowego
SSP	bezpieczne i łatwe parowanie
TRTP	parametr żądania przesłania danych
TREP	parametr odpowiedzi na przesłanie danych
VU	przyrząd rejestrujący

3. PRZYWOŁANE ROZPORZĄDZENIA I NORMY

Specyfikacje określone w niniejszym dodatku odnoszą się do wszystkich lub części wskazanych poniżej rozporządzeń i norm i są od nich zależne. W ramach zapisów niniejszego dodatku wskazano odnośne normy lub odnośne przepisy norm. W razie jakichkolwiek sprzeczności zapisy niniejszego dodatku są nadrzędne.

W niniejszym dodatku przywołano następujące rozporządzenia i normy:

— rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 165/2014 z dnia 4 lutego 2014 r. w sprawie tachografów stosowanych w transporcie drogowym i uchylające rozporządzenie Rady (EWG) nr 3821/85 w sprawie urządzeń rejestrujących stosowanych w transporcie drogowym oraz zmieniające rozporządzenie (WE) nr 561/2006 Parlamentu Europejskiego i Rady w sprawie harmonizacji niektórych przepisów socjalnych odnoszących się do transportu drogowego;

— rozporządzenie (WE) nr 561/2006 Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie harmonizacji niektórych przepisów socjalnych odnoszących się do transportu drogowego oraz zmieniające rozporządzenia Rady (EWG) nr 3821/85 i (WE) nr 2135/98, jak również uchylające rozporządzenie Rady (EWG) nr 3820/85;

— normę ISO 16844 – 4: Pojazdy drogowe – Systemy tachograficzne – Część 4: Interfejs CAN;

— normę ISO 16844 – 7: Pojazdy drogowe – Systemy tachograficzne – Część 7: Parametry;

— Bluetooth® – Profil portu szeregowego – V1.2 (Bluetooth® – Serial Port Profile – V1.2);

— Bluetooth® – Wersja podstawowa 4.2 (Bluetooth® – Core Version 4.2);

— protokół NMEA 0183 V4.1.

4. ZASADY DZIAŁANIA INTERFEJSU

4.1. **Warunki wstępne dotyczące przesyłania danych za pośrednictwem interfejsu ITS**

Przyrząd rejestrujący odpowiada za aktualizowanie i utrzymywanie danych, które mają być przechowywane w VU, bez żadnego udziału interfejsu ITS. Środki umożliwiające osiągnięcie tego celu znajdują się wewnątrz VU i są określone w innym miejscu w rozporządzeniu, a nie w niniejszym dodatku.

4.1.1 *Dane dostarczane za pośrednictwem interfejsu ITS*

Przyrząd rejestrujący odpowiada za aktualizowanie danych, które będą dostępne za pośrednictwem interfejsu ITS z częstotliwością ustaloną w procedurach VU, bez żadnego udziału interfejsu ITS. Dane VU stosuje się jako podstawę do wypełniania i aktualizowania *Danych*, przy czym środki umożliwiające osiągnięcie tego celu określono w innym miejscu w *Rozporządzeniu*, lub w przypadku braku takiego wyszczególnienia stanowią funkcję projektu produktu i nie są określone w niniejszym dodatku.

4.1.2 *Zawartość Danych*

Zawartość *Danych* pokrywa się z zawartością określoną w załączniku 1 do niniejszego dodatku.

4.1.3 *Aplikacje ITS*

Aplikacje ITS będą wykorzystywały dane udostępnione za pośrednictwem interfejsu ITS na przykład w celu zoptymalizowania zarządzania czynnościami kierowcy przy jednoczesnym przestrzeganiu przepisów rozporządzenia, w celu wykrywania możliwych usterek tachografu lub w celu stosowania danych GNSS. Specyfikacje dotyczące aplikacji nie są objęte zakresem niniejszego dodatku.

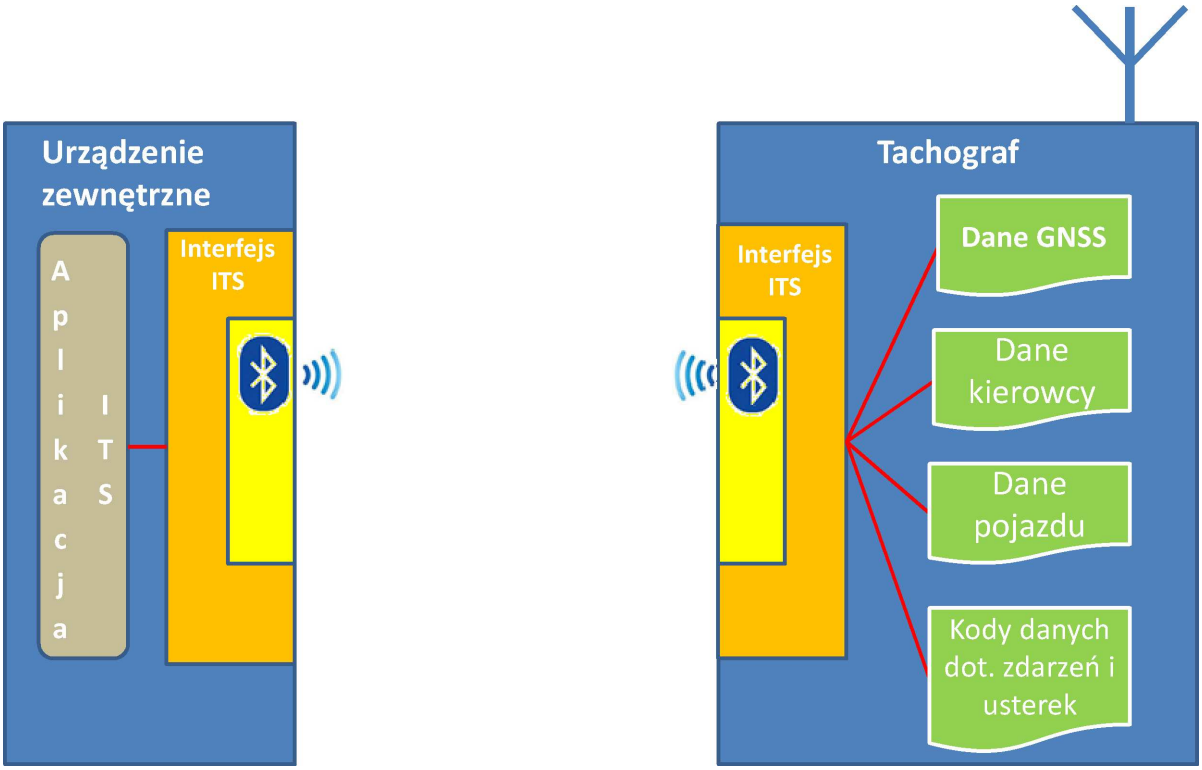
4.2. **Technologia łączności**

Wymiana *Danych* za pomocą interfejsu ITS jest prowadzona za pośrednictwem interfejsu Bluetooth® kompatybilnego z wersją 4.2 lub późniejszą. Bluetooth® funkcjonuje w nielicencjonowanym paśmie 2,4–2,485 GHz przeznaczonym do zastosowań przemysłowych, naukowych i medycznych (ISM). Bluetooth® 4.2 oferuje ulepszone mechanizmy ochrony prywatności i zabezpieczenia oraz zwiększoną prędkość i niezawodność przesyłów danych. Do celów poniższej specyfikacji wykorzystuje się urządzenie radiowe Bluetooth® klasy 2 zapewniające zasięg do 10 metrów. Więcej informacji na temat Bluetooth® 4.2 można znaleźć na stronie internetowej www.bluetooth.com (https://www.bluetooth.org/en-us/specification/adopted-specifications?_ga=1.215147412.2083380574.1435305676).

Łączność jest nawiązywana z urządzeniami do łączności po zakończeniu procesu parowania przez autoryzowane urządzenie. Ponieważ Bluetooth® wykorzystuje model urządzeń nadrzędnych/podrzędnych w celu kontrolowania, kiedy i gdzie urządzenia mogą przesyłać dane, tachograf będzie odgrywał rolę urządzenia nadrzędnego, natomiast urządzenie zewnętrzne będzie pełniło funkcję urządzenia podrzędnego.

W momencie gdy urządzenie zewnętrzne pojawi się po raz pierwszy w zakresie działania VU, można rozpocząć proces parowania Bluetooth® (zob. również załącznik 2). Urządzenia wymieniają adresy, nazwy, profile i wspólny klucz tajny, który pozwala im się łączyć, ilekroć znajdą się w pobliżu siebie w przyszłości. Po zakończeniu tego etapu urządzenie zewnętrzne uzyskuje status urządzenia zaufanego i jest w stanie inicjować żądania pobrania danych z tachografu. Nie przewiduje się możliwości dodawania mechanizmów szyfrowania poza mechanizmami zapewnianymi przez Bluetooth®. Jeżeli jednak dodatkowe mechanizmy zabezpieczeń są konieczne, zostaną one dodane zgodnie z dodatkiem 10 „Wspólne mechanizmy zabezpieczenia”.

Ogólna zasada łączności jest opisana na poniższym rysunku.



Profil SPP (profil portu szeregowego) Bluetooth® wykorzystuje się do przesyłania danych z VU do urządzenia zewnętrznego.

4.3. **Autoryzacja za pomocą kodu PIN**

Ze względów bezpieczeństwa VU wprowadza system autoryzacji za pomocą kodu PIN działający oddzielnie od systemu parowania Bluetooth. Każdy VU musi być w stanie generować kody PIN służące do uwierzytelniania, składające się z co najmniej 4 cyfr. Za każdym razem gdy urządzenie zewnętrzne paruje się z VU, musi wprowadzić poprawny kod PIN, zanim otrzyma jakiekolwiek dane.

Pomyślne wprowadzenie kodu PIN skutkuje umieszczeniem urządzenia na tzw. białej liście. Biała lista zawiera co najmniej 64 urządzenia sparowane z danym VU.

Wprowadzenie błędnego kodu PIN trzy razy pod rząd skutkuje czasowym umieszczeniem danego urządzenia na tzw. czarnej liście. Gdy urządzenie trafi na czarną listę, każda ponowna próba nawiązania połączenia przez to urządzenie jest odrzucana. Dalsze wprowadzanie błędnego kodu PIN trzy razy pod rząd skutkuje nałożeniem blokady dostępu obowiązującej przez dłuższy okres (zob. tabela 1). Wprowadzenie poprawnego kodu PIN usuwa blokadę i zeruje liczbę prób. Rysunek 1 w załączniku 2 przedstawia diagram sekwencji próby autoryzacji kodu PIN.

Tabela 1

Czas trwania blokady w zależności od liczby kolejnych nieudanych prób wprowadzenia poprawnego kodu PIN

Liczba kolejnych błędnych prób	Czas trwania blokady
3	30 sekund
6	5 minut
9	1 godzina
12	24 godziny
15	Stała

Wprowadzenie błędnego kodu PIN piętnaście razy (5x3) skutkuje umieszczeniem na stałe danego urządzenia ITS na czarnej liście. Usunięcie takiej stałej blokady jest możliwe wyłącznie poprzez wprowadzenie poprawnego kodu PUC.

Kod PUC składa się z 8 cyfr i jest dostarczany przez producenta wraz z VU. Wprowadzenie błędnego kodu PUC dziesięć razy pod rząd będzie skutkowało nieodwołalnym umieszczeniem danego urządzenia ITS na czarnej liście.

Podczas gdy producent może zapewnić możliwość zmiany kodu PIN bezpośrednio przez VU, kodu PUC nie można zmienić. Zmiana kodu PIN, o ile jest możliwa, wymaga wprowadzenia obecnego kodu PIN bezpośrednio w VU.

Ponadto wszelkie urządzenia znajdujące się na białej liście pozostają na niej do momentu ich ręcznego usunięcia przez użytkownika (np. za pośrednictwem interfejsu człowiek-maszyna VU lub w inny sposób). W ten sposób z białej listy można usunąć zgubione lub skradzione urządzenia ITS. Ponadto każde urządzenie ITS opuszczające zasięg połączenia Bluetooth na ponad 24 godziny zostaje automatycznie usunięte z białej listy VU, a przy kolejnej próbie nawiązania połączenia konieczne jest ponowne wprowadzenie poprawnego kodu PIN.

Format komunikatów między interfejsem VU a VU nie jest określony i decyzję w tej sprawie podejmuje producent. Wspomniany producent zapewnia jednak, aby stosowano określony format komunikatów wymienianych między urządzeniem ITS a interfejsem VU (zob. specyfikacje ASN.1).

Każdemu żądaniu przesłania danych towarzyszy zatem odpowiednia weryfikacja tożsamości wysyłającego, zanim zostanie ono w jakikolwiek sposób rozpatrzone. Rysunek 2 w załączniku 2 przedstawia diagram sekwencji dotyczący tej procedury. Każde urządzenie umieszczone na czarnej liście automatycznie zostanie odrzucone, a każde urządzenie nieumieszczone na czarnej ani białej liście otrzyma żądanie wprowadzenia kodu PIN, które musi spełnić, zanim ponownie wyśle swoje żądanie przesłania danych.

4.4. **Format komunikatu**

Wszystkie komunikaty wymieniane między urządzeniem ITS a interfejsem VU mają strukturę złożoną z następujących trzech części: nagłówka obejmującego bajt docelowy (TGT), bajt źródłowy (SRC) i bajt długości (LEN).

Pole danych zawiera bajt identyfikatora usługi (SID) i zmienną liczbę bajtów z danymi (maksymalnie 255).

Bajt sumy kontrolnej to 1-bajtową sumą serii modulo 256 wszystkich bajtów komunikatu, z wyłączeniem samego CS.

Komunikat zapisuje się w formacie Big Endian.

Tabela 2

Ogólny format komunikatu

Nagłówek			Pole danych					Suma kontrolna
TGT	SRC	LEN	SID	TRTP	CC	CM	DANE	CS
3 bajty			Maks. 255 bajtów					1 bajt

Nagłówek

TGT i SRC: ID docelowych (TGT) i źródłowych (SRC) urządzeń, których dotyczy dany komunikat. Interfejs VU posiada domyślne ID „EE". Nie można zmienić tego ID. Urządzenie ITS używa domyślnego ID „A0" na potrzeby swojego pierwszego komunikatu sesji łączności. Następnie interfejs VU przypisuje temu urządzeniu ITS unikatowy ID i powiadamia go o tym ID na potrzeby przyszłych komunikatów podczas sesji.

Bajt LEN uwzględnia tylko część „DANE" pola danych (zob. tabela 2), 4 pierwsze bajty są niejawne.

Interfejs VU potwierdza autentyczność wysyłającego komunikat poprzez weryfikację krzyżową własnej IDList z danymi Bluetooth, sprawdzając, czy urządzenie ITS umieszczone na liście z podanym ID znajduje się obecnie w zasięgu połączenia Bluetooth.

Pole danych

Poza SID pole danych zawiera również inne parametry: parametr żądania przesłania danych (TRTP) i bajty licznika.

Jeżeli dane, które muszą zostać przesłane, nie mieszczą się w jednym komunikacie, zostaną podzielone na kilka podkomunikatów. Każdy podkomunikat ma taki sam nagłówek i SID, ale zawiera dwubajtowy licznik, bieżący licznik (Counter Current, CC) i maksymalny licznik (Counter Max, CM), w celu wskazania numeru podkomunikatu. Aby umożliwić kontrolę błędów i przerwanie przesyłania, urządzenie przyjmujące zatwierdza każdy podkomunikat. Urządzenie przyjmujące może przyjąć podkomunikat, zażądać ponownego przesłania podkomuniaktu, zażądać od urządzenia wysyłającego ponownego rozpoczęcia transmisji lub jej przerwania.

Jeżeli CC i CM nie są używane, przyznaje się im wartość 0xFF.

Przykładowo poniższy komunikat

NAGŁÓWEK	SID	TRTP	CC	CM	DANE	CS
3 bajty	Dłuższy niż 255 bajtów					1 bajt

zostanie przesłany w następujący sposób:

NAGŁÓWEK	SID	TRTP	01	n	DANE	CS
3 bajty	255 bajtów					1 bajt

NAGŁÓWEK	SID	TRTP	02	n	DANE	CS
3 bajty	255 bajtów					1 bajt

...

NAGŁÓWEK	SID	TRTP	N	N	DANE	CS
3 bajty	Maks. 255 bajtów					1 bajt

Tabela 3 zawiera komunikaty, jakie VU i urządzenie ITS powinny być w stanie wymieniać. Zawartość każdego parametru podano w zapisie heksadecymalnym. CC i CM nie są podane w tabeli w celu zapewnienia przejrzystości, kompletny format przedstawiono powyżej.

Tabela 3

Szczegółowa treść komunikatu

Komunikat	Nagłówek			DANE			Suma kontrolna
	TGT	SRC	LEN	SID	TRTP	DANE	
RequestPIN	*ITSID*	EE	00	01	FF		
SendITSID	*ITSID*	EE	01	02	FF	*ITSID*	
SendPIN	EE	*ITSID*	04	03	FF	4*INTEGER (0..9)	
PairingResult	*ITSID*	EE	01	04	FF	BOOLEAN (T/F)	
SendPUC	EE	*ITSID*	08	05	FF	8*INTEGER (0..9)	
BanLiftingResult	*ITSID*	EE	01	06	FF	BOOLEAN (T/F)	
RequestRejected	*ITSID*	EE	08	07	FF	Godzina	
RequestData							
standardTachData	EE	*ITSID*	01	08	01		
personalTachData	EE	*ITSID*	01	08	02		
gnssData	EE	*ITSID*	01	08	03		
standardEventData	EE	*ITSID*	01	08	04		
personalEventData	EE	*ITSID*	01	08	05		
standardFaultData	EE	*ITSID*	01	08	06		
manufacturerData	EE	*ITSID*	01	08	07		

Komunikat	Nagłówek			DANE			Suma kontrolna
	TGT	SRC	LEN	SID	TRTP	DANE	
ResquestAccepted	*ITSID*	EE	Len	09	TREP	Dane	
DataUnavailable							
Brak danych	*ITSID*	EE	02	0A	TREP	10	
Dane osobowe nie podlegają wymianie	*ITSID*	EE	02	0A	TREP	11	
NegativeAnswer							
Generalne odrzucenie	*ITSID*	EE	02	0B	SID Req	10	
Usługa nieobsługiwana	*ITSID*	EE	02	0B	SID Req	11	
Podfunkcja nieobsługiwana	*ITSID*	EE	02	0B	SID Req	12	
Nieprawidłowa długość komunikatu	*ITSID*	EE	02	0B	SID Req	13	
Nieprawidłowe warunki lub błąd kolejności żądań	*ITSID*	EE	02	0B	SID Req	22	
Żądanie poza zakresem	*ITSID*	EE	02	0B	SID Req	31	
Oczekiwanie na odpowiedź	*ITSID*	EE	02	0B	SID Req	78	
Rozbieżność ID ITS	*ITSID*	EE	02	0B	SID Req	FC	
Nie znaleziono ID ITS	*ITSID*	EE	02	0B	SID Req	FB	

RequestPIN (SID 01)

Interfejs VU wysyła ten komunikat w odpowiedzi na żądanie przesłania danych przesłane przez urządzenie ITS, które nie znajduje się ani na czarnej liście, ani na białej liście.

SendITSID (SID 02)

Interfejs VU wysyła ten komunikat za każdym razem, gdy nowe urządzenie przesyła żądanie. Takie urządzenie stosuje domyślne ID „A0”, zanim otrzyma przypisane unikatowe ID na potrzeby sesji łączności.

SendPIN (SID 03)

Komunikat ten wysyła urządzenie ITS, aby trafić na białą listę interfejsu VU. Treść tego komunikatu to kod zawierający 4 liczby całkowite z przedziału od 0 do 9.

PairingResult (SID 04)

Interfejs VU wysyła ten komunikat, aby poinformować urządzenie ITS, czy przesłany przez nie kod PIN był poprawny. Treść tego komunikatu to wartość logiczna „Prawda” (True), jeżeli kod PIN jest poprawny, i „Fałsz” (False), jeżeli PIN jest niepoprawny.

SendPUC (SID 05)

Komunikat ten wysyła urządzenie ITS w celu usunięcia go z czarnej listy interfejsu VU. Treść tego komunikatu to kod zawierający 8 liczb całkowitych z przedziału od 0 do 9.

BanLiftingResult (SID 06)

Interfejs VU wysyła ten komunikat, aby poinformować urządzenie ITS, czy przesłany przez nie kod PUC był poprawny. Treść tego komunikatu to wartość logiczna „Prawda" (True), jeżeli kod PUC jest poprawny, i „Fałsz" (False), jeżeli PIN jest niepoprawny.

RequestRejected (SID 07)

Interfejs VU wysyła ten komunikat w odpowiedzi na każdy komunikat urządzenia ITS umieszczonego na czarnej liście poza komunikatem „SendPUC". Komunikat ten zawiera czas, przez jaki dane urządzenie ITS ma pozostać na czarnej liście, zgodnie z formatem sekwencji „Time" (Czas) określonym w załączniku 3.

RequestData (SID 08)

Komunikat ten dotyczący uzyskania dostępu do danych wysyła urządzenie ITS. Jednobajtowy parametr żądania przesłania danych (TRTP) wskazuje typ żądanych danych. Rozróżnia się kilka typów danych:

— standardTachData (TRTP 01): dane dostępne z tachografu sklasyfikowane jako nieosobowe;

— personalTachData (TRTP 02): dane dostępne z tachografu sklasyfikowane jako osobowe;

— gnssData (TRTP 03): dane GNSS, zawsze osobowe;

— standardEventData (TRTP 04): dane dotyczące zarejestrowanego zdarzenia sklasyfikowane jako nieosobowe;

— personalEventData (TRTP 05): dane dotyczące zarejestrowanego zdarzenia sklasyfikowane jako osobowe;

— standardFaultData (TRTP 06): dane dotyczące zarejestrowanych usterek sklasyfikowane jako nieosobowe;

— manufacturerData (TRTP 07): dane udostępnione przez producenta.

Aby uzyskać więcej informacji na temat zawartości każdego typu danych, zob. załącznik 3 do niniejszego dodatku.

Aby uzyskać więcej informacji o formacie i zawartości danych GNSS, zob. dodatek 12.

Więcej informacji na temat kodów danych dotyczących zdarzeń i usterek można znaleźć w załącznikach IB i IC.

ResquestAccepted (SID 09)

Komunikat ten wysyła interfejs VU w przypadku zaakceptowania komunikatu „RequestData" przesłanego przez urządzenie ITS. Komunikat ten zawiera 1-bajtowy TREP, który stanowi bajt TRTP powiązanego komunikatu „RequestData", oraz wszystkie dane żądanego typu.

DataUnavailable (SID 0A)

Komunikat ten wysyła interfejs VU, jeżeli, z określonego powodu, żądane dane, które mają być wysłane do umieszczonego na białej liście urządzenia ITS, nie są dostępne. Komunikat ten zawiera 1-bajtowy TREP, który stanowi TRTP żądanych danych oraz 1-bajtowy kod błędu określony w tabeli 3. Dozwolone są następujące kody:

— brak danych (10): interfejs VU nie może uzyskać dostępu do danych VU z nieokreślonych powodów;

— dane osobowe nie podlegają wymianie (11): urządzenie ITS usiłuje pobrać dane osobowe, w przypadku gdy nie podlegają one wymianie.

NegativeAnswer (SID 0B)

Interfejs VU wysyła takie komunikaty, jeżeli żądanie nie może zostać zrealizowane z każdego powodu innego niż brak dostępności danych. Komunikaty takie są zazwyczaj przesyłane w odpowiedzi na nieprawidłowy format żądania (długość, SID, ID ITS itd.), lecz nie tylko. TRTP w polu danych zawiera SID żądania. Pola danych zawiera kod identyfikujący powód uzyskania negatywnej odpowiedzi. Dozwolone są następujące kody:

— Generalne odrzucenie (kod: 10)

— Czynność nie może zostać zrealizowana z powodu nieokreślonego poniżej ani w sekcji (wprowadzić numer sekcji *DataUnavailable)*.

— Usługa nieobsługiwana (kod: 11)

— SID żądania jest niezrozumiały.

— Podfunkcja nieobsługiwana (kod: 12)

— TRTP żądania jest niezrozumiały. Może go np. brakować lub jego wartość może znajdować się poza dopuszczalnym zakresem.

— Nieprawidłowa długość komunikatu (kod: 13)

— Długość otrzymanego komunikatu jest nieprawidłowa (rozbieżność między bajtem LEN a faktyczną długością komunikatu).

— Nieprawidłowe warunki lub błąd kolejności żądań (kod: 22)

— Żądana usługa nie jest aktywna lub sekwencja komunikatów żądań nie jest prawidłowa.

— Żądanie poza zakresem (kod: 33)

— Żądany rekord parametru (pole danych) nie jest prawidłowy.

— Oczekiwanie na odpowiedź (kod: 78)

— Żądanej czynności nie można zakończyć na czas, a VU nie jest gotowy do przyjęcia kolejnego żądania.

— Rozbieżność *ID ITS* (kod: FB)

— *ID ITS* SRC nie odpowiada powiązanemu urządzeniu po dokonaniu porównania z informacjami o Bluetooth.

— Nie znaleziono *ID ITS* (kod: FC)

— *ID ITS* SRC nie jest powiązane z żadnym urządzeniem.

Wiersze 1–72 (**FormatMessageModule**) kodu ASN.1 w załączniku 3 określają format komunikatów opisany w tabeli 3. Poniżej przedstawiono więcej informacji szczegółowych na temat treści komunikatów.

4.5. **Zgoda kierowcy**

Wszystkie dostępne dane są klasyfikowane jako standardowe albo osobowe. Dostęp do danych osobowych jest możliwy wyłącznie po uzyskaniu zgody kierowcy na to, aby dotyczące go dane osobowe z tachografu mogły opuścić sieć pojazdu do celów wykorzystania tych danych przez osoby trzecie.

Kierowca udziela zgody w momencie, gdy przy pierwszym włożeniu danej karty kierowcy lub karty warsztatowej nieznanej jeszcze przyrządowi rejestrującemu właściciel karty zostanie poproszony o wyrażenie zgody na udostępnianie danych osobowych związanych z tachografem za pośrednictwem opcjonalnego interfejsu ITS (zob. również pkt 3.6.2 w załączniku IC).

Status zgody (aktywny/nieaktywny) jest zapisywany w pamięci tachografu.

W przypadku wielu kierowców wymianie z interfejsem ITS podlegają wyłącznie dane osobowe dotyczące kierowców, którzy wyrazili na to zgodę. Przykładowo jeżeli w pojeździe znajduje się dwóch kierowców i tylko pierwszy z nich zgodził się na udostępnienie swoich danych osobowych, dane osobowe dotyczące drugiego kierowcy nie podlegają wymianie.

4.6. **Pobieranie danych standardowych**

Rysunek 3 w załączniku 2 przedstawia diagramy sekwencji prawidłowego żądania wysłanego przez urządzenie ITS w celu uzyskania dostępu do danych standardowych. Urządzenie ITS zostało prawidłowo umieszczone na białej liście i nie żąda dostępu do danych osobowych, zatem nie jest wymagana dalsza weryfikacja. W ramach schematów założono, że zastosowano już odpowiednią procedurę przedstawioną na rys. 2 w załączniku 2. Można je przyrównać do szarej ramki „REQUEST TREATMENT" na rys. 2.

Spośród dostępnych danych następujące dane uznaje się za standardowe:

— standardTachData (TRTP 01)

— StandardEventData (TRTP 04)

— standardFaultData (TRTP 06)

4.7. **Pobieranie danych osobowych**

Rysunek 4 w załączniku 2 przedstawia diagram sekwencji dotyczący przetwarzania żądania dostępu do danych osobowych. Jak wspomniano wcześniej, interfejs VU wysyła dane osobowe, wyłącznie jeżeli kierowca wyraźnie wyraził na to zgodę (zob. również pkt 4.5). W przeciwnym razie żądanie musi zostać automatycznie odrzucone.

Spośród dostępnych danych następujące dane uznaje się za osobowe:

— personalTachData (TRTP 02)

— gnssData (TRTP 03)

— personalEventData (TRTP 05)

— manufacturerData (TRTP 07)

4.8. **Pobieranie danych dotyczących zdarzeń i usterek**

Urządzenia ITS muszą być w stanie żądać dostępu do danych dotyczących zdarzeń zawierających wykaz wszystkich nieoczekiwanych zdarzeń. Tego rodzaju dane klasyfikuje się jako standardowe lub osobowe, zob. załącznik 3. Zawartość każdego zdarzenia jest zgodna z dokumentami przedstawionymi w załączniku 1 do niniejszego dodatku.

ZAŁĄCZNIK 1

WYKAZ DANYCH DOSTĘPNYCH ZA POŚREDNICTWEM INTERFEJSU ITS

Data	Source	Data classification (personal/ not personal)
VehicleIdentificationNumber	Vehicle Unit	**not personal**
CalibrationDate	Vehicle Unit	**not personal**
TachographVehicleSpeed speed instant t	Vehicle Unit	personal
Driver1WorkingState Selector driver	Vehicle Unit	personal
Driver2WorkingState	Vehicle Unit	personal
DriveRecognize Speed Threshold detected	Vehicle Unit	**not personal**
Driver1TimeRelatedStates Weekly day time	Driver Card	personal
Driver2TimeRelatedStates	Driver Card	personal
DriverCardDriver1	Vehicle Unit	**not personal**
DriverCardDriver2	Vehicle Unit	**not personal**
OverSpeed	Vehicle Unit	personal
TimeDate	Vehicle Unit	**not personal**
HighResolutionTotalVehicleDistance	Vehicle Unit	**not personal**
ServiceComponentIdentification	Vehicle Unit	**not personal**
ServiceDelayCalendarTimeBased	Vehicle Unit	**not personal**
Driver1Identification	Driver Card	personal
Driver2Identification	Driver Card	personal
NextCalibrationDate	Vehicle Unit	**not personal**
Driver1ContinuousDrivingTime	Driver Card	personal
Driver2ContinuousDrivingTime	Driver Card	personal
Driver1CumulativeBreakTime	Driver Card	personal
Driver2CumulativeBreakTime	Driver Card	personal
Driver1CurrentDurationOfSelectedActivity	Driver Card	personal
Driver2CurrentDurationOfSelectedActivity	Driver Card	personal

Data	Source	Data classification (personal/ not personal)
SpeedAuthorised	Vehicle Unit	**not personal**
TachographCardSlot1	Driver Card	**not personal**
TachographCardSlot2	Driver Card	**not personal**
Driver1Name	Driver Card	personal
Driver2Name	Driver Card	personal
OutOfScopeCondition	Vehicle Unit	**not personal**
ModeOfOperation	Vehicle Unit	**not personal**
Driver1CumulatedDrivingTimePreviousAndCurrentWeek	Driver Card	personal
Driver2CumulatedDrivingTimePreviousAndCurrentWeek	Driver Card	personal
EngineSpeed	Vehicle Unit	personal
RegisteringMemberState	Vehicle Unit	**not personal**
VehicleRegistrationNumber	Vehicle Unit	**not personal**
Driver1EndOfLastDailyRestPeriod	Driver Card	personal
Driver2EndOfLastDailyRestPeriod	Driver Card	personal
Driver1EndOfLastWeeklyRestPeriod	Driver Card	personal
Driver2EndOfLastWeeklyRestPeriod	Driver Card	personal
Driver1EndOfSecondLastWeeklyRestPeriod	Driver Card	personal
Driver2EndOfSecondLastWeeklyRestPeriod	Driver Card	personal
Driver1CurrentDailyDrivingTime	Driver Card	personal
Driver2CurrentDailyDrivingTime	Driver Card	personal
Driver1CurrentWeeklyDrivingTime	Driver Card	personal
Driver2CurrentWeeklyDrivingTime	Driver Card	personal
Driver1TimeLeftUntilNewDailyRestPeriod	Driver Card	personal
Driver2TimeLeftUntilNewDailyRestPeriod	Driver Card	personal
Driver1CardExpiryDate	Driver Card	personal

Data	Source	Data classification (personal/ not personal)
Driver2CardExpiryDate	Driver Card	personal
Driver1CardNextMandatoryDownloadDate	Driver Card	personal
Driver2CardNextMandatoryDownloadDate	Driver Card	personal
TachographNextMandatoryDownloadDate	Vehicle Unit	**not personal**
Driver1TimeLeftUntilNewWeeklyRestPeriod	Driver Card	personal
Driver2TimeLeftUntilNewWeeklyRestPeriod	Driver Card	personal
Driver1NumberOfTimes9hDailyDrivingTimesExceeded	Driver Card	personal
Driver2NumberOfTimes9hDailyDrivingTimesExceeced	Driver Card	personal
Driver1CumulativeUninterruptedRestTime	Driver Card	personal
Driver2CumulativeUninterruptedRestTime	Driver Card	personal
Driver1MinimumDailyRest	Driver Card	personal
Driver2MinimumDailyRest	Driver Card	personal
Driver1MinimumWeeklyRest	Driver Card	personal
Driver2MinimumWeeklyRest	Driver Card	personal
Driver1MaximumDailyPeriod	Driver Card	personal
Driver2MaximumDailyPeriod	Driver Card	personal
Driver1MaximumDailyDrivingTime	Driver Card	personal
Driver2MaximumDailyDrivingTime	Driver Card	personal
Driver1NumberOfUsedReducedDailyRestPeriods	Driver Card	personal
Driver2NumberOfUsedReducedDailyRestPeriods	Driver Card	personal
Driver1RemainingCurrentDrivingTime	Driver Card	personal
Driver2RemainingCurrentDrivingTime	Driver Card	personal
GNSS position	Vehicle Unit	personal

2) STAŁY DOSTĘP DO DANYCH GNSSPO UZYSKANIU ZGODY KIEROWCY

Zobacz dodatek 12 – GNSS.

3) KODY ZDARZEŃ DOSTĘPNE BEZ ZGODY KIEROWCY

Zdarzenie	Zasady gromadzenia danych	Dane rejestrowane dla zdarzenia
Włożenie karty nieważnej	— 10 ostatnich zdarzeń	— data i godzina wystąpienia zdarzenia, — typ karty, numer karty i państwo członkowskie, które wydało kartę, oraz generacja karty powodującej zdarzenie, — liczba podobnych zdarzeń w tym dniu.
Konflikt kart	— 10 ostatnich zdarzeń	— data i godzina rozpoczęcia zdarzenia, — data i godzina zakończenia zdarzenia, — typ karty, numer karty i państwo członkowskie, które wydało kartę, oraz generacja obu kart powodujących konflikt.
Sesja ostatniej karty niezamknięta prawidłowo	— 10 ostatnich zdarzeń	— data i godzina włożenia karty, — typ karty, numer karty i państwo członkowskie, które wydało kartę, oraz generacja karty, — dane dotyczące ostatniej sesji odczytane z karty: — data i godzina włożenia karty, — numer VRN, państwo członkowskie rejestracji oraz generacja VU.
Przerwa w zasilaniu (2)	— najdłuższe zdarzenie w każdym z ostatnich 10 dni ich występowania, — 5 najdłużej trwających zdarzeń w ciągu ostatnich 365 dni.	— data i godzina rozpoczęcia zdarzenia, — data i godzina zakończenia zdarzenia, — typ karty, numer karty i państwo członkowskie, które wydało kartę, oraz generacja każdej karty włożonej na początku lub po zakończeniu zdarzenia, — liczba podobnych zdarzeń w tym dniu.
Błąd łączności z urządzeniem do łączności na odległość	— najdłuższe zdarzenie w każdym z ostatnich 10 dni ich występowania, — 5 najdłużej trwających zdarzeń w ciągu ostatnich 365 dni.	— data i godzina rozpoczęcia zdarzenia, — data i godzina zakończenia zdarzenia, — typ karty, numer karty i państwo członkowskie, które wydało kartę, oraz generacja każdej karty włożonej na początku lub po zakończeniu zdarzenia, — liczba podobnych zdarzeń w tym dniu.
Brak informacji o położeniu z odbiornika GNSS	— najdłuższe zdarzenie w każdym z ostatnich 10 dni ich występowania, — 5 najdłużej trwających zdarzeń w ciągu ostatnich 365 dni.	— data i godzina rozpoczęcia zdarzenia, — data i godzina zakończenia zdarzenia, — typ karty, numer karty i państwo członkowskie, które wydało kartę, oraz generacja każdej karty włożonej na początku lub po zakończeniu zdarzenia, — liczba podobnych zdarzeń w tym dniu.
Błąd danych dotyczących ruchu	— najdłuższe zdarzenie w każdym z ostatnich 10 dni ich występowania, — 5 najdłużej trwających zdarzeń w ciągu ostatnich 365 dni.	— data i godzina rozpoczęcia zdarzenia, — data i godzina zakończenia zdarzenia, — typ karty, numer karty i państwo członkowskie, które wydało kartę, oraz generacja każdej karty włożonej na początku lub po zakończeniu zdarzenia, — liczba podobnych zdarzeń w tym dniu.

Zdarzenie	Zasady gromadzenia danych	Dane rejestrowane dla zdarzenia
Konflikt ruchu pojazdu	— najdłuższe zdarzenie w każdym z ostatnich 10 dni ich występowania, — 5 najdłużej trwających zdarzeń w ciągu ostatnich 365 dni.	— data i godzina rozpoczęcia zdarzenia, — data i godzina zakończenia zdarzenia, — typ karty, numer karty i państwo członkowskie, które wydało kartę, oraz generacja każdej karty włożonej na początku lub po zakończeniu zdarzenia, — liczba podobnych zdarzeń w tym dniu.
Próba naruszenia zabezpieczenia	10 ostatnich zdarzeń wg typu zdarzenia.	— data i godzina rozpoczęcia zdarzenia, — data i godzina zakończenia zdarzenia (o ile dotyczy), — typ karty, numer karty i państwo członkowskie, które wydało kartę, oraz generacja każdej karty włożonej na początku lub po zakończeniu zdarzenia, — typ zdarzenia.
Konflikt czasowy	— najdłuższe zdarzenie w każdym z ostatnich 10 dni ich występowania, — 5 najdłużej trwających zdarzeń w ciągu ostatnich 365 dni.	— data i godzina na urządzeniu rejestrującym, — data i godzina na odbiorniku GNSS, — typ karty, numer karty i państwo członkowskie, które wydało kartę, oraz generacja każdej karty włożonej na początku lub po zakończeniu zdarzenia, — liczba podobnych zdarzeń w tym dniu.

4) KODY ZDARZENIA DOSTĘPNE BEZ ZGODY KIEROWCY

Zdarzenie	Zasady gromadzenia danych	Dane rejestrowane dla zdarzenia
Prowadzenie bez prawidłowej karty	— najdłuższe zdarzenie w każdym z ostatnich 10 dni ich występowania, — 5 najdłużej trwających zdarzeń w ciągu ostatnich 365 dni.	— data i godzina rozpoczęcia zdarzenia, — data i godzina zakończenia zdarzenia, — typ karty, numer karty i państwo członkowskie, które wydało kartę, oraz generacja każdej karty włożonej na początku lub po zakończeniu zdarzenia, — liczba podobnych zdarzeń w tym dniu.
Włożenie karty podczas prowadzenia pojazdu	— ostatnie zdarzenie dla każdego z 10 ostatnich dni od zaistnienia zdarzenia.	— data i godzina zdarzenia, — typ karty, numer karty i państwo członkowskie, które wydało kartę, oraz generacja karty, — liczba podobnych zdarzeń w tym dniu.
Przekroczenie prędkości (1)	— najpoważniejsze zdarzenie dla każdego z 10 ostatnich dni od zaistnienia zdarzenia (tzn. zdarzenie o najwyższej, przeciętnej prędkości), — 5 najpoważniejszych zdarzeń w okresie ostatnich 365 dni, — pierwsze zdarzenie zaistniałe po ostatniej kalibracji.	— data i godzina rozpoczęcia zdarzenia, — data i godzina zakończenia zdarzenia, — maksymalna prędkość zmierzona w czasie zdarzenia, — średnia arytmetyczna prędkość zmierzona w czasie zdarzenia, — typ karty, numer karty i państwo członkowskie, które wydało kartę, oraz generacja karty kierowcy (o ile dotyczy), — liczba podobnych zdarzeń w tym dniu.

5) KODY DANYCH DOTYCZĄCYCH USTEREK DOSTĘPNE BEZ ZGODY KIEROWCY

Usterka	Zasady gromadzenia danych	Dane rejestrowane dla usterki
Usterka karty	— 10 ostatnich usterek karty kierowcy,	— data i godzina rozpoczęcia usterki, — data i godzina zakończenia usterki, — typ karty, numer karty i państwo członkowskie, które wydało kartę, oraz generacja karty.
Usterki urządzenia rejestrującego	— 10 ostatnich usterek dla każdego typu usterki, — pierwsza usterka po ostatniej kalibracji.	— data i godzina rozpoczęcia usterki, — data i godzina zakończenia usterki, — typ usterki, — typ karty, numer karty i państwo członkowskie, które wydało kartę, oraz generacja każdej karty włożonej na początku lub po zakończeniu usterki.

Usterkę tę uruchamia dowolna z następujących usterek, z wyłączeniem pracy w trybie kalibracyjnym:

— usterka wewnętrzna VU

— usterka drukarki

— usterka wyświetlacza

— usterka pobierania danych

— usterka czujnika

— usterka odbiornika GNSS lub urządzenia zewnętrznego GNSS

— usterka urządzenia do łączności na odległość

6) ZDARZENIA I USTERKI DOTYCZĄCE KONKRETNEGO PRODUCENTA BEZ ZGODY KIEROWCY

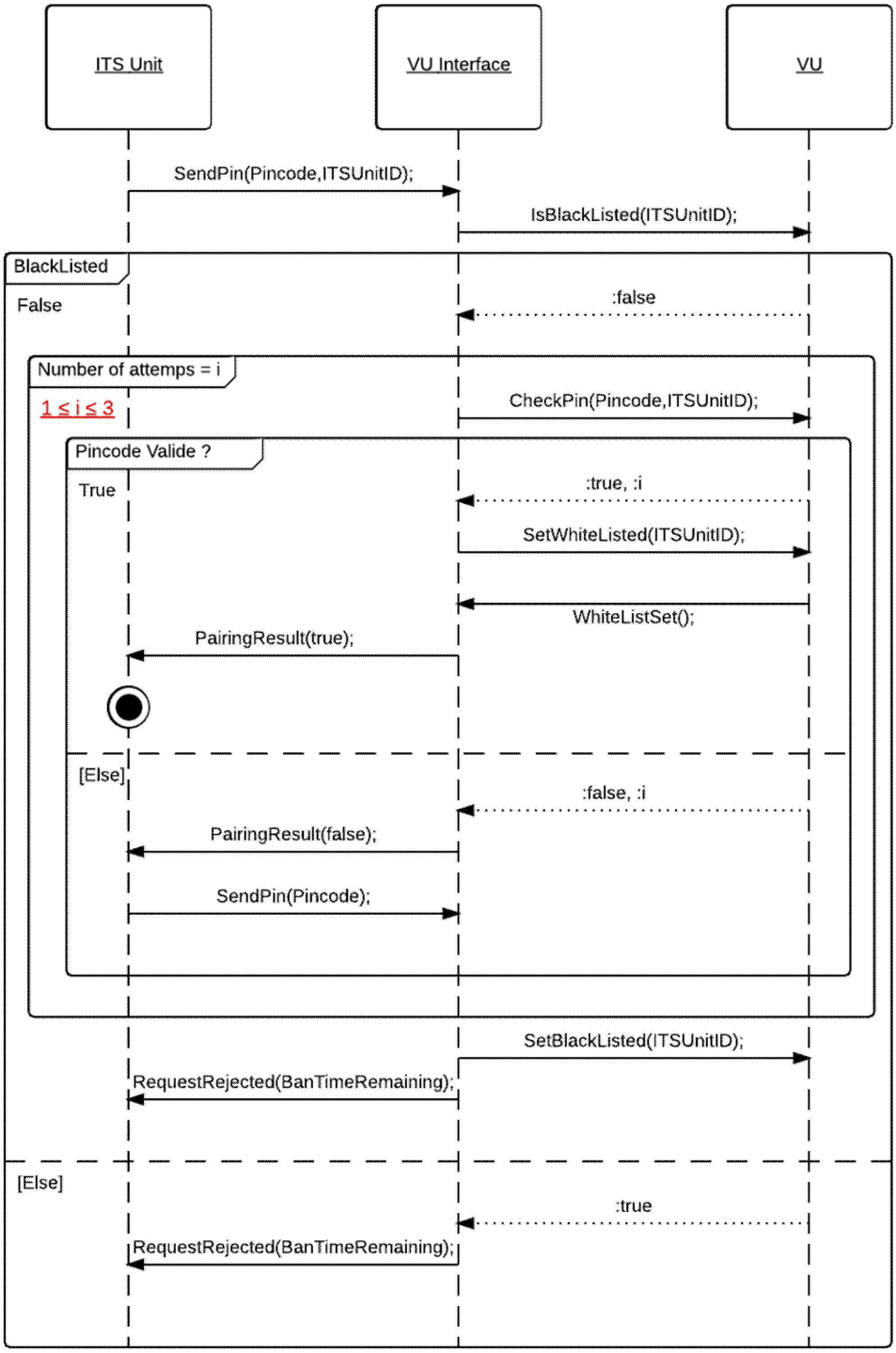
Zdarzenie lub usterka	Zasady gromadzenia danych	Dane rejestrowane dla zdarzenia
Określi producent	Określi producent	Określi producent

ZAŁĄCZNIK 2

DIAGRAMY SEKWENCJI WYMIANY KOMUNIKATÓW Z URZĄDZENIEM ITS.

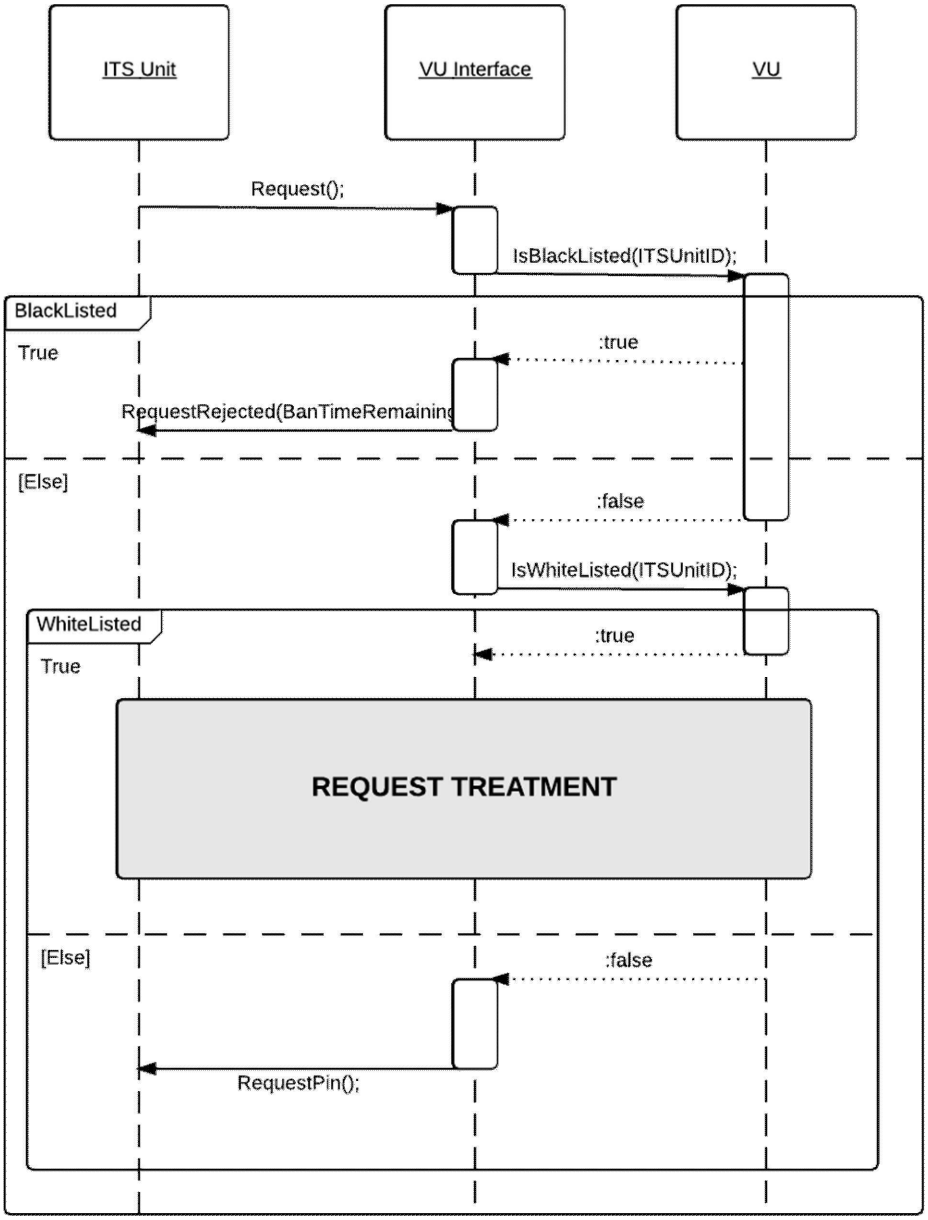
Rys. 1

Diagram sekwencji próby autoryzacji kodu PIN



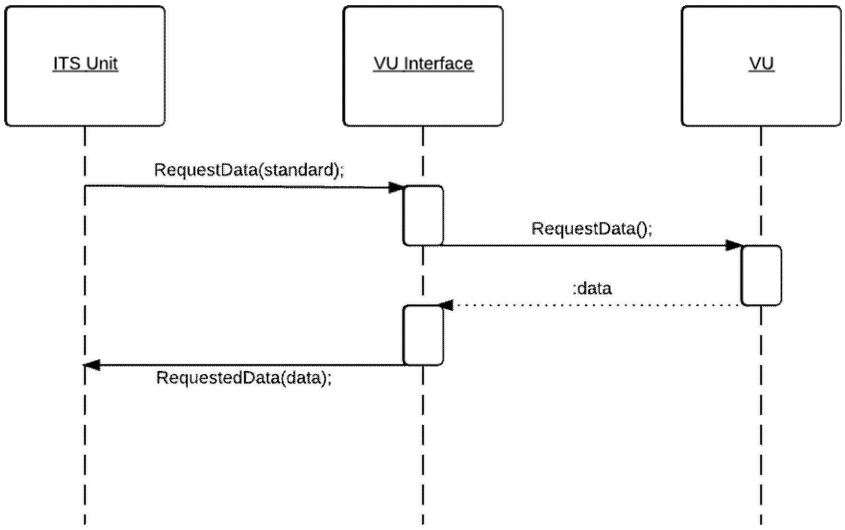
Rys. 2

Diagram sekwencji weryfikacji autoryzacji urządzenia ITS



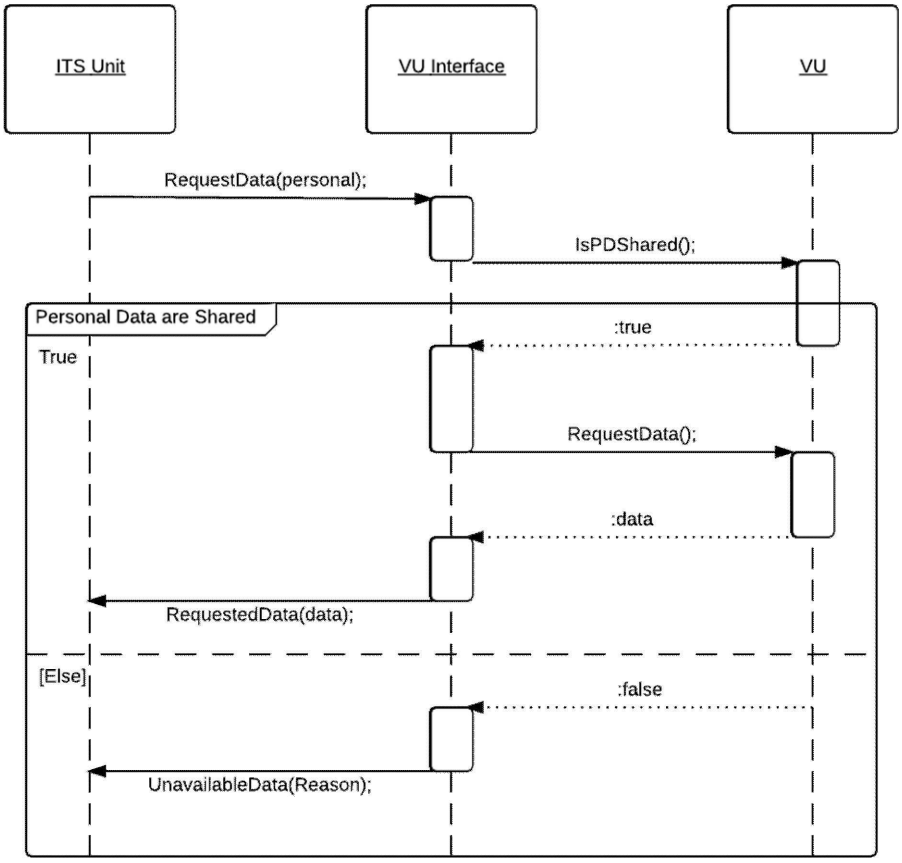
Rys. 3

Diagram sekwencji przetworzenia żądania przedstawienia danych zaklasyfikowanych jako nieosobowe (po poprawnym uzyskaniu dostępu za pomocą kodu PIN)



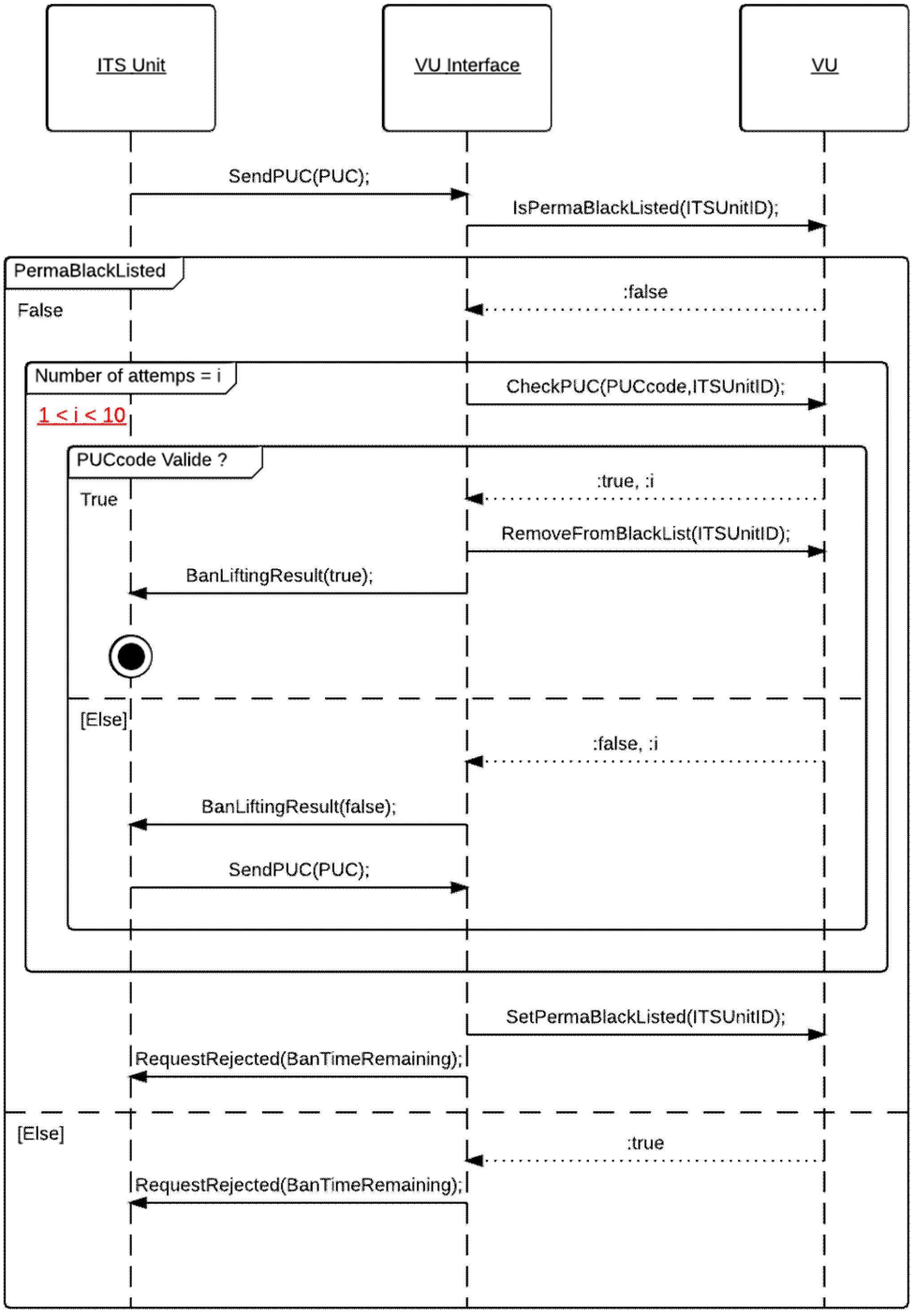
Rys. 4

Diagram sekwencji przetworzenia żądania przedstawienia danych zaklasyfikowanych jako osobowe (po poprawnym uzyskaniu dostępu za pomocą kodu PIN)



Rys. 5

Diagram sekwencji próby autoryzacji kodu PIN



ZAŁĄCZNIK 3

SPECYFIKACJE ASN.1

```
FormatMessageModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS ;
IMPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
        BanLiftingResult FROM PINPUCDataFieldsModule
        RequestAccepted,RequestData, DataUnavailable FROM
        RequestDataFieldsModule
        SendITSID, NegativeAnswer FROM OtherDataFieldsModule;

      CompleteMessage ::=SEQUENCE{
            header Header,
            data DataField,
            checksum Checksum
      }

      ----------------
      --HEADER TYPES--
      ----------------


      Header::=SEQUENCE{
            tgt IDList,
            src IDList,
            len BIT STRING (1..255)
      }

      vuID BIT STRING ::= 'EE'H
      IDList ::=CHOICE{
            vu BIT STRING (vuID),
            itsUnits SEQUENCE OF BIT STRING,
                  --Default hex Value:A0, redefined after first message exchange--
                  --Each ID will be linked to the Bluetooth ID of the device--
            ...
      }

      --------------------
      --DATAFIELDS TYPES--
      --------------------
      DataField ::=SEQUENCE{
            sid BIT STRING,
            trtp BIT STRING,
            subMBytes SubMessageBytes,
            dataField Content,
            ...
      }

      SubMessageBytes ::= SEQUENCE{
            currentSubM BIT STRING,
            totalSubM BIT STRING
      }

      Content ::= CHOICE{
            requestPIN RequestPIN,
            sendITSID SendITSID,
            sendPin SendPIN,
```

```
55                pairRslt PairingResult,
56                sendPUC SendPUC,
57                banlift BanLiftingResult,
58                requestRejected RequestRejected,
59                requestData RequestData,
60                requestOK RequestAccepted,
61                dataUnavailable DataUnavailable,
62                negAns NegativeAnswer
63          }
64
65          ------------------
66          --CHECKSUM TYPES--
67          ------------------
68
69          Checksum ::= SEQUENCE{
70                --SHA2 checksum
71          }
72    END
73
```

```
PINPUCDataFieldsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
BanLiftingResult;
IMPORTS ;

	----------
	---Utils--
	----------

	PUC ::= SEQUENCE (SIZE(8)) OF
	INTEGER (SIZE(0..9))

	PIN ::=	SEQUENCE (SIZE(4)) OF
		INTEGER (SIZE(0..9))

	--------------------------
	--Messages From ITS Unit--
	--------------------------

	SendPIN {PIN:pin} ::= SEQUENCE {
		sid BIT STRING ('03'H),
		pin PIN (pin)
	}

	SendPUC {PUC:puc} ::= SEQUENCE {
		sid BIT STRING ('05'H),
		puc PUC (puc)
	}
	--------------------
	--Messages From VU--
	--------------------

	PairingResult ::= SEQUENCE{
		sid BIT STRING ('04'H),
		result BOOLEAN
	}

	RequestPIN {MType:receivedRequest}::= SEQUENCE{
		sid BIT STRING ('01'H)
	}

	RequestRejected ::= SEQUENCE{
		sid BIT STRING ('07'H),
		banTimeRemaining GeneralizedTime, --PermaBan == 1k years-- }

	BanLiftingResult ::= SEQUENCE{
		sid BIT STRING ('06'H),
		result BOOLEAN
	}
END
```

```
RequestDataFields DEFINITIONS AUTOMATIC TAGS ::= BEGIN
	EXPORTS RequestAccepted,RequestData, DataUnavailable ;
	IMPORTS StandardEvent, PersonalEvent, StandardFault FROM EventsModule;

	------------------
	---From ITS Unit--
	------------------
	RequestData ::= SEQUENCE{
		sid BIT STRING ('08'H),
		requestedData DataTypeCode,
		...
	}

	-----------
	--From VU--
	-----------
	RequestAccepted ::=SEQUENCE{
		sid BIT STRING ('09'H),
		trtp DataTypeCode,
		dataSheet CHOICE{
			standardData StandardTachDataContent,
			personalData PersonalTachDataContent,
			gnss GNSSDataContent,
			standardEvent StandardEventContent,
			personalEvent PersonalEventContent,
			standardFault StandardFaultContent,
			manufacturerdata ManufacturerDataContent,
			...
		}
	}

	DataTypeCode ::=CHOICE{
		standardTachData BIT STRING ('01'H),
		personalTachData BIT STRING ('02'H),
		gnssData BIT STRING ('03'H),
		standardEventData BIT STRING ('04'H),
		personalEventData BIT STRING ('05'H),
		standardFaultData BIT STRING ('06'H),
		manufacturerData BIT STRING ('07'H),
		...
	}

	DataUnavailable ::=SEQUENCE{
		sid BIT STRING ('0A'H),
		trtp DataTypeCode,
		reason UnavailableDataCodes
	}

	UnavailableDataCodes ::= CHOICE{
		noDataAvailable BIT STRING ('10'H),
		personalDataNotShared BIT STRING ('11'H),
		...
	}
	----------------------------
	--Complete Tachograph Data--
	----------------------------
	--The format of the data was taken from the ISO16844-7 norm, more information
available in this ISO document—

```

```
Time ::= SEQUENCE{
	seconds INTEGER (0..59.75), --increment: 0.25s--
	minutes INTEGER (0..59), --increment: 1min--
	hours INTEGER (0..23), --increment: 1h--
	day INTEGER (0.25.. 31.75), --increment: 0.25d--
	month INTEGER (1..12), --increment: 1month--
	year INTEGER (1985..2235), --increment: 1year--
	locMinOffset INTEGER (-59..59), --increment: 1min--
	locHouroffset INTEGER (-23..23)--increment: 1h--
}

Date ::= SEQUENCE{
	month INTEGER (1..12), --increment: 1month--
	day INTEGER (0.25.. 31.75), --increment: 0.25d--
	year INTEGER (1985..2235) --increment: 1year--
}

DriverName ::=SEQUENCE{
	codePageSurname UTF8String, --See ISO/IEC 8859--
	surname UTF8String,
	codePageFirstname UTF8String, --See ISO/IEC 8859--
	firstname UTF8String,
}

--------------------
--Message Content--
--------------------

StandardTachDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&standardTachData),
	personal BOOLEAN (FALSE),
	data StandardTachyDataSheet,
}

PersonalTachDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&personalTachData),
	personal BOOLEAN (TRUE),
	data PersonalTachyDataSheet
}

GNSSDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&gnssData),
	personal BOOLEAN (TRUE),
	data GNSSDataSheet
}

StandardEventContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&standardEventData),
	personal BOOLEAN (FALSE),
	data StandardEventDataSheet
}

PersonalEventContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&personalEventData),
	personal BOOLEAN (TRUE),
	data PersonalEventDataSheet
}

StandardFaultContent ::= SEQUENCE{
```

```
243                 trtp DataTypeCode (DataTypeCode.&standardFaultData),
244                 personal BOOLEAN (FALSE),
245                 data StandardFault
246         }
247
248         ManufacturerDataContent ::= SEQUENCE{
249                 trtp DataTypeCode (DataTypeCode.&manufacturerData),
250                 personal BOOLEAN (TRUE),
251                 ...
252         }
253
254         ---------------
255         --DATA SHEETS--
256         ---------------
257
258         --Data sheet format follows ISO 16844-7.--
259         StandardTachyDataSheet ::= SEQUENCE{
260                 vin UTF8String (SIZE(17)),
261                 calibrationDate Date,
262                 driveRecognize INTEGER (2 UNION 12),
263                 driverCardDriver1 INTEGER (2 UNION 12),
264                 driverCardDriver2 INTEGER (2 UNION 12),
265                 timeDate Time,
266                 highResolutionTotalVehicleDistance INTEGER (0..21055406), --increment:
267   5m--
268                 serviceComponentIdentification INTEGER (0..255),
269                 serviceDelayCalendarTimeBased INTEGER (-125..125), --increment: 1week-
270   -
271                 nextCalibrationDate Date,
272                 speedAuthorised INTEGER (0..250.996), --increment 1/256km/h--
273                 tachographCardSlot1 INTEGER (0..4...), --Maximum 250--
274                 tachographCardSlot2 INTEGER (0..4...), --Maximum 250--
275                 outOfScopeCondition INTEGER(2 UNION 12),
276                 modeOfOperation INTEGER (0..4...), --Maximum 250--
277                 registeringMemberState UTF8String,
278         vehicleRegistrationNumber SEQUENCE {
279                         codePageVRN INTEGER (0..255),
280                         vrn OCTET STRING (SIZE(13)),
281                 },
282                 tachographNextMandatoryDownloadDate Date,
283                 ...
284         }
285
286         PersonalTachyDataSheet ::= SEQUENCE{
287                 tachographVehicleSpeed INTEGER (0..250.996), --increment 1/256km/h--
288                 driver1WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
289   UNION 1012...),
290                 driver2WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
291   UNION 1012...),
292
293                 driver1TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
294   1002 UNION
295                                                  1012 UNION 1102 UNION 1112 UNION
296   10002 UNION 10012 UNION
297                                                  10102 UNION 10112 UNION 11002 UNION
298   11012...),
299                 driver2TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
300   1002 UNION
```

```
                                                    1012 UNION 1102 UNION 1112 UNION
10002 UNION 10012 UNION
                                                    10102 UNION 10112 UNION 11002 UNION
11012...),

             overSpeed INTEGER (2 UNION 12),
             driver1Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
FROM TACHO REGULATION--
             driver2Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
FROM TACHO REGULATION--
             driver1ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
             driver2ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
             driver1CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
increment: 1min--
             driver2CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
increment: 1min--
             driver1Name DriverName,
             driver2Name DriverName,
             driver1CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
--increment: 1min--
             driver2CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
--increment: 1min--
             engineSpeed INTEGER(0..8031.875), --increment: 0,125r/min--
             driver1EndOfLastDailyRestPeriod Time,
             driver2EndOfLastDailyRestPeriod Time,
             driver1EndOfLastWeeklyRestPeriod Time,
             driver2EndOfLastWeeklyRestPeriod Time,
             driver1EndOfSecondLastWeeklyRestPeriod Time,
             driver2EndOfSecondLastWeeklyRestPeriod Time,
             driver1CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
-
             driver2CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
-
             driver1CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
1min--
             driver2CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
1min--
             driver1TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver2TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver1CardExpiryDate Date,
             driver2CardExpiryDate Date,
             driver1CardNextMandatoryDownloadDate Date,
             driver2CardNextMandatoryDownloadDate Date,
             driver1TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver2TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver1NumberOfTimes9hDailyDrivingTimesExceeded INTEGER (0..13),
             driver2NumberOfTimes9hDailyDrivingTimesExceeced INTEGER (0..13),
             driver1CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
increment: 1min--
             driver2CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
increment: 1min--
             driver1MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
             driver2MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
             driver1MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
             driver2MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
```

```
360                driver1MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
361                driver2MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
362                driver1MaximumDailyDrivingTime INTEGER (910 UNION 1010),
363                driver2MaximumDailyDrivingTime INTEGER (910 UNION 1010),
364                driver1NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
365                driver2NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
366                driver1RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
367   1min--
368                driver2RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
369   1min--
370                ...
371          }
372
373          GNSSDataSheet ::=  SEQUENCE {
374          gnssPosition GeoCoordinates
375                --See Appendix 1 for definition of GeoCoordinates--
376          }
377
378          StandardEventDataSheet ::= SEQUENCE{
379                events SEQUENCE OF StandardEvent
380          }
381
382          PersonalEventDataSheet ::= SEQUENCE{
383                events SEQUENCE OF PersonalEvent
384          }
385   END
386
387   EventsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
388          EXPORTS ALL;
389          IMPORTS NationAlpha FROM Appendix1; --See Appendix 1 for more information
390   about NationAlpha--
391
392                SecurityBreachEvent ::=SEQUENCE{
393                      --See Annex 1B for more information--
394                }
395
396                RecordingEquipmentFaultType ::= SEQUENCE{
397                      --See Annex 1B for more information--
398                }
399
400                StandardEvent::= CHOICE{
401                      insertionInvalidCard InsertionOfANonValidCard,
402                      cardConflict CardConflict,
403                      timeOverlap TimeOverlap,
404                      previousSessionNotClosed LastCardSessionNotCorrectlyClosed,
405                      overSpeeding OverSpeeding,
406                      powerSupplyInterruption PowerSupplyInterruption,
407                      comErrorWithRemoteFacility
408   CommunicationErrorWithTheRemoteCommunicationFacility,
409                      absenceGNSSPosition
410   AbsenceOfPositionInformationFromGNSSReceiver,
411                      positionDataError PositionDataError,
412                      motionDataError MotionDataError,
413                      vehicleMotionConflict VehicleMotionConflict,
414                      securityBreachAttempt SecurityBreachAttempt,
415                      timeConflict TimeConflict,
416                      ...
417                }
418
```

```
PersonalEvent ::= CHOICE{
	lackOfAppropriateCard DrivingWithoutAnAppropriateCard,
	cardInsertionWhileDriving CardInsertionWhileDriving,
	overSpeeding OverSpeeding,
	...
}

StandardFault ::= CHOICE{
	cardFault CardFault,
	recordingEquipementFault RecordingEquipmentFault,
...
}

---------------
--EVENTS LIST--
---------------

InsertionOfANonValidCard::=SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER
}

CardConflict ::= SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER
}

TimeOverlap ::=SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER,
	numberSimilarEvent INTEGER
}

DrivingWithoutAnAppropriateCard ::= SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER,
	numberOfSimilarEvent INTEGER
}

CardInsertionWhileDriving ::= SEQUENCE{
	date GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
```

```
478                     issuingMemberState SEQUENCE OF NationAlpha,
479                     numberOfSimilarEvents INTEGER
480             }
481
482             LastCardSessionNotCorrectlyClosed ::=SEQUENCE{
483                     beginDate GeneralizedTime,
484                     endDate GeneralizedTime,
485                     carsdType SEQUENCE OF UTF8String,
486                     cardsNumber SEQUENCE OF INTEGER,
487                     issuingMemberState SEQUENCE OF NationAlpha,
488                     cardsGeneration SEQUENCE OF INTEGER,
489                     oldSession SEQUENCE{
490                             beginDate GeneralizedTime,
491                             endDate GeneralizedTime,
492                             vrn UTF8String,
493                             issuingMemberState NationAlpha,
494                             cardsGeneration INTEGER,
495                     }
496             }
497
498             OverSpeeding ::=SEQUENCE{
499                     beginDate GeneralizedTime,
500                     endDate GeneralizedTime,
501                     maximumSpeed INTEGER,
502                     averageSpeed INTEGER,
503                     cardType UTF8String,
504                     cardNumber INTEGER,
505                     issuingMemberState NationAlpha,
506                     cardGeneration INTEGER,
507                     numberOfSimilarEvents INTEGER
508             }
509
510             PowerSupplyInterruption ::=SEQUENCE{
511                     beginDate GeneralizedTime,
512                     endDate GeneralizedTime,
513                     carsdType SEQUENCE OF UTF8String,
514                     cardsNumber SEQUENCE OF INTEGER,
515                     issuingMemberState SEQUENCE OF NationAlpha,
516                     cardsGeneration SEQUENCE OF INTEGER,
517                     numberOfSimilarEvent INTEGER
518             }
519
520             CommunicationErrorWithTheRemoteCommunicationFacility ::=SEQUENCE{
521                     beginDate GeneralizedTime,
522                     endDate GeneralizedTime,
523                     carsdType SEQUENCE OF UTF8String,
524                     cardsNumber SEQUENCE OF INTEGER,
525                     issuingMemberState SEQUENCE OF NationAlpha,
526                     cardsGeneration SEQUENCE OF INTEGER,
527                     numberOfSimilarEvent INTEGER
528             }
529
530             AbsenceOfPositionInformationFromGNSSReceiver ::= SEQUENCE{
531                     beginDate GeneralizedTime,
532                     endDate GeneralizedTime,
533                     carsdType SEQUENCE OF UTF8String,
534                     cardsNumber SEQUENCE OF INTEGER,
535                     issuingMemberState SEQUENCE OF NationAlpha,
536                     cardsGeneration SEQUENCE OF INTEGER,
```

```
537                     numberOfSimilarEvent INTEGER
538             }
539
540             PositionDataError ::= SEQUENCE{
541                     beginDate GeneralizedTime,
542                     endDate GeneralizedTime,
543                     carsdType SEQUENCE OF UTF8String,
544                     cardsNumber SEQUENCE OF INTEGER,
545                     issuingMemberState SEQUENCE OF NationAlpha,
546                     cardsGeneration SEQUENCE OF INTEGER,
547                     numberOfSimilarEvent INTEGER
548             }
549
550             MotionDataError ::= SEQUENCE{
551                     beginDate GeneralizedTime,
552                     endDate GeneralizedTime,
553                     carsdType SEQUENCE OF UTF8String,
554                     cardsNumber SEQUENCE OF INTEGER,
555                     issuingMemberState SEQUENCE OF NationAlpha,
556                     cardsGeneration SEQUENCE OF INTEGER,
557                     numberOfSimilarEvent INTEGER
558             }
559
560             VehicleMotionConflict ::= SEQUENCE{
561                     beginDate GeneralizedTime,
562                     endDate GeneralizedTime,
563                     carsdType SEQUENCE OF UTF8String,
564                     cardsNumber SEQUENCE OF INTEGER,
565                     issuingMemberState SEQUENCE OF NationAlpha,
566                     cardsGeneration SEQUENCE OF INTEGER,
567                     numberOfSimilarEvent INTEGER
568             }
569
570             SecurityBreachAttempt ::= SEQUENCE{
571                     beginDate GeneralizedTime,
572                     endDate GeneralizedTime OPTIONAL,
573                     carsdType SEQUENCE OF UTF8String,
574                     cardsNumber SEQUENCE OF INTEGER,
575                     issuingMemberState SEQUENCE OF NationAlpha,
576                     numberOfSimilarEvent INTEGER,
577                     typeOfEvent SecurityBreachEvent
578             }
579
580
581             TimeConflict ::= SEQUENCE{
582                     beginDate GeneralizedTime,
583                     endDate GeneralizedTime,
584                     carsdType SEQUENCE OF UTF8String,
585                     cardsNumber SEQUENCE OF INTEGER,
586                     issuingMemberState SEQUENCE OF NationAlpha,
587                     cardsGeneration SEQUENCE OF INTEGER,
588                     numberOfSimilarEvent INTEGER
589             }
590
591             ---------------
592             --FAULTS LIST--
593             ---------------
594
595             CardFault ::= SEQUENCE{
```

```
596                     beginDate GeneralizedTime,
597                     endDate GeneralizedTime,
598                     carsdType SEQUENCE OF UTF8String,
599                     cardsNumber SEQUENCE OF INTEGER,
600                     issuingMemberState SEQUENCE OF NationAlpha,
601                     cardsGeneration SEQUENCE OF INTEGER,
602             }
603
604             RecordingEquipmentFault ::= SEQUENCE{
605                     beginDate GeneralizedTime,
606                     endDate GeneralizedTime,
607                     faultType RecordingEquipmentFaultType,
608                     carsdType SEQUENCE OF UTF8String,
609                     cardsNumber SEQUENCE OF INTEGER,
610                     issuingMemberState SEQUENCE OF NationAlpha,
611                     cardsGeneration SEQUENCE OF INTEGER,
612             }
613 END
```

Dodatek 14

FUNKCJA ŁĄCZNOŚCI NA ODLEGŁOŚĆ

SPIS TREŚCI

1 WPROWADZENIE

W niniejszym dodatku określono strukturę oraz procedury, które należy zastosować w celu wykonania funkcji łączności na odległość („łączność") zgodnie z art. 9 rozporządzenia (UE) nr 165/2014 („rozporządzenie").

DSC_1 Zgodnie z rozporządzeniem (UE) nr 165/2014 tachograf musi być wyposażony w funkcję łączności na odległość, aby zapewnić przedstawicielom właściwych organów kontrolnych możliwość odczytywania informacji przekazywanych przez tachograf zainstalowany w przejeżdżających pojazdach za pomocą urządzeń zdalnej kontroli („czytnik wczesnego wykrywania na odległość" (REDCR)), a w szczególności w urządzenia kontroli łączące się bezprzewodowo za pośrednictwem interfejsów dedykowanej łączności krótkiego zasięgu (DSRC) pracujących na częstotliwości CEN 5,8 GHz.

Należy pamiętać, że opisana funkcja jest wykorzystywana wyłącznie w celu wstępnej selekcji pojazdów, które zostaną wybrane do bardziej szczegółowej kontroli; nie zastępuje ona formalnego przeglądu przeprowadzanego zgodnie z przepisami rozporządzenia (UE) nr 165/2014. Zobacz motyw 9 w preambule do tego rozporządzenia, w którym stwierdza się, że łączność na odległość między tachografem a organami kontrolnymi na potrzeby kontroli drogowych usprawnia ukierunkowane kontrole drogowe.

DSC_2 *Dane* wymienia się za pomocą *Łączności*, tj. bezprzewodowej wymiany informacji za pośrednictwem systemu łączności bezprzewodowej DSRC operującego na częstotliwości 5,8 GHz prowadzonej zgodnie z niniejszym dodatkiem, która jest sprawdzana pod kątem zgodności z odpowiednimi parametrami przewidzianymi w normie 300 674-1 {Kwestie dotyczące kompatybilności elektromagnetycznej i widma radiowego (ERM); telematyka transportu i ruchu drogowego (RTTT); dedykowana łączność krótkiego zasięgu (DSRC) utrzymywana za pośrednictwem urządzeń transmisyjnych (500 kbit/s / 250 kbit/s) działających na częstotliwości 5,8 GHz w paśmie przeznaczonym do zastosowań przemysłowych, naukowych i medycznych (ISM); Część 1: Charakterystyka ogólna przyrządów instalowanych na poboczu (RSU) oraz przyrządów instalowanych w pojeździe (OBU) i metody kontrolowania tych przyrządów}.

DSC_3 *Łączność* nawiązuje się za pośrednictwem urządzeń do łączności wyłącznie po otrzymaniu sygnału wyemitowanego przez urządzenia właściwego organu kontrolnego przy wykorzystaniu zgodnych środków łączności radiowej (*„czytnik wczesnego wykrywania na odległość" (REDCR)*).

DSC_4 *Dane* zabezpiecza się w celu zapewnienia ich integralności.

DSC_5 Dostęp do przesyłanych *Danych* jest ograniczony do właściwych organów kontrolnych upoważnionych do kontroli naruszeń rozporządzenia (WE) nr 561/2006 i rozporządzenia (UE) nr 165/2014 oraz do warsztatów w zakresie niezbędnym do sprawdzenia poprawnego funkcjonowania tachografu.

DSC_6 *Dane* przesyłane w trakcie utrzymywania *Łączności* ograniczają się do danych niezbędnych na potrzeby ukierunkowanych kontroli drogowych pojazdów wyposażonych w tachografy, które mogły zostać niewłaściwie użyte lub stać się przedmiotem manipulacji.

DSC_7 Integralność i bezpieczeństwo *Danych* zapewnia się, zabezpieczając *Dane* przechowywane w przyrządzie rejestrującym (VU) i przekazując wyłącznie zabezpieczone dane ładunku i dane dotyczące zabezpieczeń za pośrednictwem urządzeń bezprzewodowej łączności na odległość DSRC działających na częstotliwości 5,8 GHz (zob. pkt 5.4.4), co oznacza, że tylko upoważnieni pracownicy właściwych organów kontrolnych są w stanie zrozumieć dane przekazywane w trakcie utrzymywania *Łączności* i są w stanie zweryfikować ich autentyczność. Zob. Dodatek 11 – Wspólne mechanizmy zabezpieczenia.

DSC_8 *Dane* muszą zawierać znacznik czasu określający datę i godzinę ich ostatniej aktualizacji.

DSC_9 Treść danych zabezpieczających jest znana wyłącznie właściwym organom kontrolnym i tym stronom, którym organy udostępniają te informacje, oraz pozostaje pod ich kontrolą; treść takich danych wykracza poza zakres przepisów dotyczących *Łączności* będących przedmiotem niniejszego dodatku z wyjątkiem zakresu, w jakim *Łączność* zabezpiecza przesyłanie pakietu danych zabezpieczających z każdym pakietem danych ładunku.

DSC_10 Należy zapewnić możliwość wykorzystania tej samej architektury i tych samych urządzeń do uzyskania innych koncepcji danych (jak np. ważenie w pojeździe) z zastosowaniem architektury określonej w niniejszym dodatku.

DSC_11 W tym miejscu należy wyjaśnić, że zgodnie z przepisami rozporządzenia (UE) nr 165/2014 (art. 7) dane dotyczące tożsamości kierowcy nie mogą być przekazywane w ramach *Łączności*.

2 ZAKRES

Celem niniejszego dodatku jest określenie, w jaki sposób przedstawiciele właściwych organów kontrolnych mają korzystać z dedykowanego systemu łączności bezprzewodowej DSRC działającego w paśmie 5,8 GHz, aby zdalnie pozyskiwać z pojazdu docelowego dane („*Dane*") wskazujące, że taki pojazd może potencjalnie naruszać przepisy rozporządzenia (UE) nr 165/2014 i że w związku z tym należy rozważyć możliwość jego zatrzymania do bardziej szczegółowej kontroli.

Zgodnie z wymogiem ustanowionym w rozporządzeniu (UE) nr 165/2014 gromadzone *Dane* muszą ograniczać się do danych lub dotyczyć danych potwierdzających, że mogło dojść do naruszenia praw, zgodnie z definicją przedstawioną w art. 9 rozporządzenia (UE) nr 165/2014.

W takim przypadku czas dostępny na nawiązanie łączności jest ograniczony, ponieważ *Łączność* ma ukierunkowany charakter i cechuje się krótkim zasięgiem. Ponadto właściwe organy kontrolne mogą korzystać ze środków łączności wykorzystywanych do celów zdalnego monitorowania tachografu również do innych celów (np. do przekazywania informacji dotyczących maksymalnych obciążeń i wymiarów pojazdów ciężarowych określonych w dyrektywie 2015/719/WE), przy czym działania w tym zakresie mogą być podejmowane oddzielnie lub sekwencyjnie według uznania właściwych organów kontrolnych.

W niniejszym dodatku określa się:

— urządzenia do łączności oraz procedury i protokoły, które należy stosować do celów *Łączności*;

— normy i przepisy, z którymi urządzenia radiowe muszą być zgodne;

— sposób przekazywania *Danych* za pośrednictwem urządzeń do *Łączności*;

— procedury zapytywania i pobierania oraz sekwencję operacji;

— *Dane*, które mają być przekazywane;

— Możliwe interpretacje *Danych* przesyłanych w ramach *Łączności*;

— przepisy w zakresie danych zabezpieczających dotyczących *Łączności*;

— dostępność *Danych* dla właściwych organów kontrolnych;

— sposób, w jaki *Czytnik wczesnego wykrywania na odległość* może żądać przekazania różnych koncepcji danych dotyczących ładunku i floty.

W tym miejscu należy wyjaśnić, że w niniejszym dodatku nie określa się:

— operacji gromadzenia *Danych* i zarządzania tym procesem w ramach VU (co stanowi funkcję projektu produktu, chyba że zostało określone w innym miejscu w rozporządzeniu (UE) nr 165/2014);

— formy, w jakiej należy przedstawić zgromadzone dane przedstawicielowi właściwych organów kontrolnych ani kryteriów, z których właściwe organy kontrolne muszą korzystać przy podejmowaniu decyzji o ewentualnym zatrzymaniu pojazdu (co stanowi funkcję projektu produktu, chyba że zostało określone w innym miejscu w rozporządzeniu (UE) nr 165/2014 lub zależy od decyzji politycznej właściwych organów kontrolnych). W tym miejscu należy wyjaśnić, że za pośrednictwem *Łączności* udostępnia się *Dane* właściwym organom kontrolnym, wyłącznie aby zapewnić im możliwość podejmowania świadomych decyzji;

— Przepisów w zakresie bezpieczeństwa danych (takich jak przepisy w zakresie szyfrowania) dotyczących treści *Danych* (które zostaną określone w dodatku 11 – Wspólne mechanizmy zabezpieczenia);

— szczegółowych informacji dotyczących wszelkich koncepcji danych innych niż RTM, które można pozyskać z zastosowaniem tej samej architektury i tych samych urządzeń;

— szczegółowych informacji dotyczących zachowania i zarządzania pomiędzy VU i DSRC-VU ani dotyczących zachowania w ramach DSRC-VU (poza przekazywaniem *Danych* na żądanie REDCR).

3 SKRÓTY, DEFINICJE I OZNACZENIA

W niniejszym dodatku używa się następujących skrótów i definicji właściwych dla tego dodatku:

Antena	urządzenie elektryczne przekształcające energię elektryczną w fale radiowe i *vice versa*, wykorzystywane w połączeniu z nadajnikiem radiowym lub odbiornikiem radiowym. W trakcie pracy nadajnik radiowy generuje drgania elektryczne o częstotliwości fal radiowych, które trafiają do gniazd antenowych, a antena emituje energię pozyskiwaną z prądu w formie fal elektromagnetycznych (fal radiowych). Przyjmując fale radiowe, antena przechwytuje część energii z fali elektromagnetycznej i wytwarza niewielkie napięcie w gniazdach antenowych, które jest następnie przesyłane do odbiornika w celu wzmocnienia;
Łączność	wymiana informacji/danych między *DSRC-REDCR* a DSRC-VU zgodnie z przepisami sekcji 5 w trybie nadrzędny-podrzędny prowadzona w celu pozyskania *Danych*;
Dane	zabezpieczone dane o określonym formacie (zob. pkt 5.4.4) żądane przez *DSRC–REDCR* i przekazane przez *DSR-VU* za pośrednictwem DSRC działającego na częstotliwości 5,8 GHz określonego w pkt 5 poniżej;
Rozporządzenie (WE) nr 165/2014	Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 165/2014 z dnia 4 lutego 2014 r. w sprawie tachografów stosowanych w transporcie drogowym i uchylające rozporządzenie Rady (EWG) nr 3821/85 w sprawie urządzeń rejestrujących stosowanych w transporcie drogowym oraz zmieniające rozporządzenie (WE) nr 561/2006 Parlamentu Europejskiego i Rady w sprawie harmonizacji niektórych przepisów socjalnych odnoszących się do transportu drogowego;
AID	identyfikator aplikacji
BLE	Bluetooth Low Energy (łączność Bluetooth przy znikomym poborze prądu)
BST	tabela usług sygnału

CIWD	włożenie karty podczas prowadzenia pojazdu
CRC	cykliczna kontrola nadmiarowa
DSC (n)	identyfikator wymogu związanego z określonym dodatkiem dotyczącym DSRC
DSRC	dedykowana łączność krótkiego zasięgu
DSRC-REDCR	DSRC–czytnik wczesnego wykrywania na odległość
DSRC-VU	DSRC–przyrząd rejestrujący. Jest to „urządzenie wczesnego wykrywania na odległość" zdefiniowana w załączniku 1C
DWVC	prowadzenie pojazdu bez ważnej karty
EID	identyfikator elementu
LLC	sterowanie połączeniem logicznym
LPDU	jednostka danych protokołu LLC
OWS	system ważenia zainstalowany w pojeździe
PDU	jednostka danych protokołu
REDCR	czytnik wczesnego wykrywania na odległość. Jest to „urządzenie służące jako czytnik wczesnego wykrywania na odległość" zdefiniowane w załączniku 1C
RTM	zdalne monitorowanie tachografu
SM-REDCR	moduł zabezpieczeń–czytnik wczesnego wykrywania na odległość
TARV	aplikacje telematyczne dla pojazdów regulowanych (seria norm ISO 15638)
VU	przyrząd rejestrujący
VUPM	pamięć ładunku przyrządu rejestrującego
VUSM	moduł zabezpieczeń przyrządu rejestrującego
VST	tabela usług pojazdu
WIM	ważenie w ruchu
WOB	ważenie w pojeździe

Specyfikacje określone w niniejszym dodatku odnoszą się do wszystkich lub części wskazanych poniżej rozporządzeń i norm i są od nich zależne. W ramach zapisów niniejszego dodatku wskazano odnośne normy lub odnośne przepisy norm. W razie jakichkolwiek sprzeczności zapisy niniejszego dodatku są nadrzędne. W sytuacji wystąpienia jakichkolwiek sprzeczności, w przypadku których nie istnieją specyfikacje wyraźnie określone w niniejszym dodatku, należy w pierwszej kolejności zastosować procedury przewidziane w ERC 70-03 (i sprawdzić zgodność z odpowiednimi parametrami przewidzianymi w normie EN 300 674-1), a następnie procedury przewidziane kolejno w normach EN 12795, EN 12253, EN 12834 i EN 13372 pkt 6.2, 6.3, 6.4 oraz 7.1.

W niniejszym dodatku przywołano następujące rozporządzenia i normy:

[1] rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 165/2014 z dnia 4 lutego 2014 r. w sprawie tachografów stosowanych w transporcie drogowym i uchylające rozporządzenie Rady (EWG) nr 3821/85 w sprawie urządzeń rejestrujących stosowanych w transporcie drogowym oraz zmieniające rozporządzenie (WE) nr 561/2006 Parlamentu Europejskiego i Rady w sprawie harmonizacji niektórych przepisów socjalnych odnoszących się do transportu drogowego;

[2] rozporządzenie (WE) nr 561/2006 Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie harmonizacji niektórych przepisów socjalnych odnoszących się do transportu drogowego oraz zmieniające rozporządzenia Rady (EWG) nr 3821/85 i (WE) nr 2135/98, jak również uchylające rozporządzenie Rady (EWG) nr 3820/85 (tekst mający znaczenie dla EOG);

[3] dokument ERC 70-03 CEPT „Zalecenie ECC 70-03 dotyczące korzystania z urządzeń bliskiego zasięgu (SRD)";

[4] normę ISO 15638 Inteligentne systemy transportowe – Ramy wspólnych aplikacji telematycznych dla regulowanych komercyjnych samochodów ciężarowych (TARV);

[5] normę EN 300 674-1 „Kwestie dotyczące kompatybilności elektromagnetycznej i widma radiowego (ERM); telematyka transportu i ruchu drogowego (RTTT); dedykowana łączność krótkiego zasięgu (DSRC) utrzymywana za pośrednictwem urządzeń transmisyjnych (500 kbit/s / 250 kbit/s) działających na częstotliwości 5,8 GHz w paśmie przeznaczonym do zastosowań przemysłowych, naukowych i medycznych (ISM); Część 1: Charakterystyka ogólna przyrządów instalowanych na poboczu (RSU) oraz przyrządów instalowanych w pojeździe (OBU) i metody kontrolowania tych przyrządów";

[6] normę EN 12253 „Telematyka transportu i ruchu drogowego – Wydzielona komunikacja krótkiego zasięgu – Warstwa fizyczna wykorzystująca częstotliwość 5,8 GHz";

[7] normę EN 12795 „Telematyka transportu i ruchu drogowego – Wydzielona komunikacja krótkiego zasięgu (DSRC) – Warstwa łącza danych DSRC: sterowanie dostępem nośnika i łączem logicznym";

[8] normę EN 12834 „Telematyka transportu i ruchu drogowego – Wydzielona komunikacja krótkiego zasięgu (DSRC) – Warstwa aplikacyjna DSRC";

[9] normę EN 13372 „Telematyka transportu i ruchu drogowego (RTTT) – Wydzielona komunikacja krótkiego zasięgu – Profile zastosowań RTTT";

[10] normę ISO 14906 „Elektroniczny system pobierania opłat – Określenie interfejsu zastosowań dla wydzielonej komunikacji krótkiego zasięgu".

4 SCENARIUSZE OPERACYJNE

4.1 **Informacje ogólne**

W rozporządzeniu (UE) nr 165/2014 wskazano konkretne i kontrolowane scenariusze określające sposób stosowania *Łączności*.

Do scenariuszy objętych wsparciem należą:

„Profil łączności 1: Kontrole drogowe przeprowadzane przy wykorzystaniu czytnika wczesnego wykrywania na odległość opartego na technologii łączności bezprzewodowej krótkiego zasięgu dające podstawy do wszczęcia fizycznej kontroli drogowej (relacja nadrzędny-podrzędny)

Profil czytnika 1a: Kontrole przeprowadzane przy wykorzystaniu ręcznego urządzenia wczesnego wykrywania na odległość lub urządzenia wczesnego wykrywania na odległość zainstalowanego tymczasowo na poboczu

Profil czytnika 1b: Kontrole przeprowadzane przy wykorzystaniu ukierunkowanego czytnika wczesnego wykrywania na odległość zainstalowanego w pojeździe".

4.1.1 *Warunki wstępne dotyczące przesyłania danych za pośrednictwem interfejsu DSRC działającego na częstotliwości 5,8 GHz*

UWAGA: w celu zrozumienia kontekstu warunków wstępnych warto zapoznać się z rys. 14.3 poniżej.

4.1.1.1 Dane przechowywane w VU

DSC_12 Przyrząd rejestrujący odpowiada za aktualizowanie co 60 sekund danych, które mają być przechowywane w VU, bez żadnego udziału funkcji łączności DSRC oraz za utrzymywanie tych danych. Środki umożliwiające osiągnięcie tego celu znajdują się wewnątrz VU i są określone w sekcji 3.19 „Łączność na odległość na potrzeby ukierunkowanych kontroli drogowych" załącznika 1C do rozporządzenia (UE) nr 165/2014, a nie w niniejszym dodatku.

4.1.1.2 Dane przesyłane do funkcji DSRC-VU

DSC_13 Przyrząd rejestrujący odpowiada za aktualizowanie danych gromadzonych przez tachograf DSRC (*Dane*) za każdym razem, gdy następuje aktualizacja danych przechowywanych w VU w odstępach czasu określonych w pkt 4.1.1.1 (DSC_12), bez żadnego udziału funkcji łączności DSRC.

DSC_14 Dane VU stosuje się jako podstawę do wypełniania i aktualizowania *Danych*, przy czym środki umożliwiające osiągnięcie tego celu określono w sekcji 3.19 „Łączność na odległość na potrzeby ukierunkowanych kontroli drogowych" załącznika 1C lub w przypadku braku takiego wyszczególnienia stanowią funkcję projektu produktu i nie są określone w niniejszym dodatku. Informacje na temat struktury połączenia między funkcją DSRC-VU a VU można znaleźć w sekcji 5.6.

4.1.1.3 Zawartość Danych

DSC_15 Treść i format *Danych* powinny pozwalać na to, aby po ich odszyfrowaniu zachowały one odpowiednią strukturę i pozostały dostępne w formie i formacie określonych w pkt 5.4.4 niniejszego dodatku (struktury *Danych*).

4.1.1.4 Przedstawienie Danych

DSC_16 *Dane*, który były regularnie aktualizowane zgodnie z procedurami przewidzianymi w pkt 4.1.1.1, zabezpiecza się przed ich przedstawieniem *DSRC-VU*, a następnie przedstawia jako wartość koncepcji danych zabezpieczonych w celu ich tymczasowego przechowania w *DSRC-VU* jako aktualną wersję *Danych*. Dane te przekazuje się z *VUSM* do funkcji DSRC *VUPM*. *VUSM* i *VUPM* to funkcje, które niekoniecznie muszą mieć postać fizyczną. Forma fizycznej konkretyzacji służącej wykonywaniu tych funkcji jest kwestią projektu produktu, chyba że została określona w innym miejscu w rozporządzeniu (UE) nr 165/2014.

4.1.1.5 Dane zabezpieczające

DSC_17 Dane zabezpieczające (*securityData*) obejmujące żądane przez *REDCR* dane niezbędne do zapewnienia mu możliwości odszyfrowania *Danych* przekazuje się zgodnie z przepisami dodatku 11 „Wspólne mechanizmy zabezpieczenia", po czym przedstawia się je jako wartość koncepcji danych w celu ich tymczasowego przechowania w *DSRC-VU* jako aktualną wersję *SecurityData* w formie określonej w sekcji 5.4.4 niniejszego dodatku.

4.1.1.6 Dane VUPM dostępne do przekazywania za pośrednictwem interfejsu DSRC

DSC_18 Koncepcja danych, która musi być zawsze dostępna w ramach funkcji DSRC VUPM do celów natychmiastowego przekazania na żądanie *REDCR*, została zdefiniowana w sekcji 5.4.4 w odniesieniu do pełnej specyfikacji modułu ASN.1.

Informacje ogólne na temat profilu łączności 1

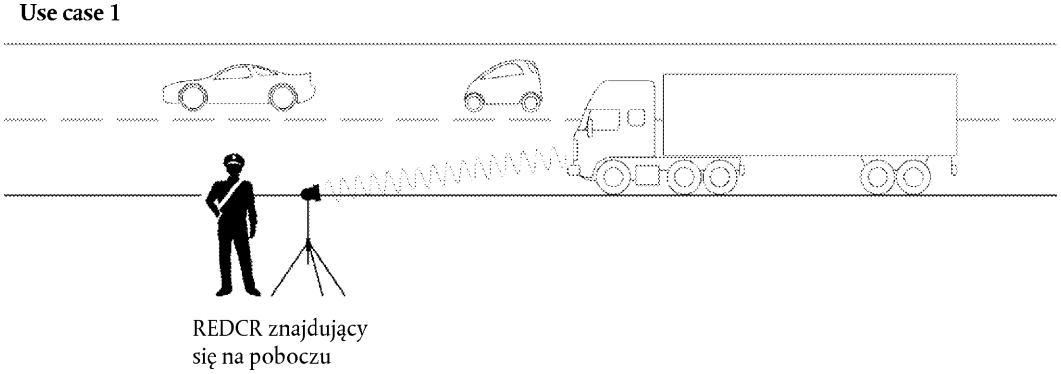
Profil ten obejmuje przypadek wykorzystania, w którym przedstawiciel właściwego organu kontrolnego używa czytnika wczesnego wykrywania na odległość (bazującego na interfejsach DSRC działających na częstotliwości 5,8 GHz w ramach ERC 70-03 i sprawdzonego pod kątem zgodności z odpowiednimi parametrami przewidzianymi w normie EN 300 674-1, jak opisano w sekcji 5) (*REDCR*) w celu zdalnego zidentyfikowania pojazdu, który może potencjalnie naruszać przepisy rozporządzenia (UE) nr 165/2014. Po zidentyfikowaniu pojazdu przedstawiciel właściwego organu kontrolnego przeprowadzający kontrolę podejmuje o ewentualnym zatrzymaniu pojazdu.

4.1.2 *Profil 1a: Kontrole przeprowadzane przy wykorzystaniu ręcznego czytnika wczesnego wykrywania na odległość lub czytnika wczesnego wykrywania na odległość zainstalowanego tymczasowo na poboczu*

W ramach tego przypadku wykorzystania przedstawiciel właściwego organu kontrolnego znajduje się na poboczu i nakierowuje ręczny *REDCR*, *REDCR* ustawiony na statywie trójnożnym lub innego rodzaju przenośny *REDCR* w kierunku środka szyby przedniej wybranego pojazdu. Kontrolę przeprowadza się przy wykorzystaniu interfejsów DSRC działających na częstotliwości 5,8 GHz w ramach ERC 70-03 i sprawdza pod kątem zgodności z odpowiednimi parametrami przewidzianymi w normie EN 300 674-1, jak opisano w sekcji 5. Zob. rys. 14.1 (przypadek wykorzystania 1).

Rysunek 14.1

Kontrola drogowa przeprowadzana przy wykorzystaniu interfejsów DSRC działających na częstotliwości 5,8 GHz

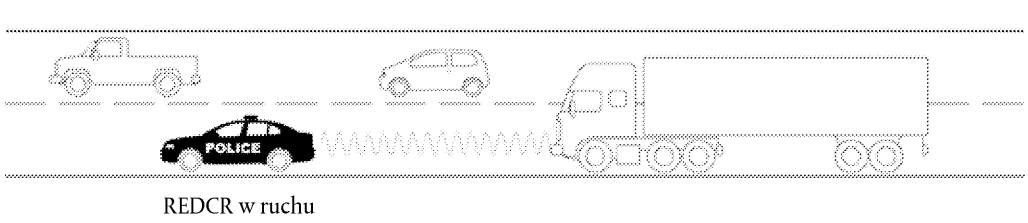


4.1.3 *Profil 1b: Kontrole przeprowadzane przy wykorzystaniu ukierunkowanego czytnika wczesnego wykrywania na odległość (REDCR) zainstalowanego w pojeździe*

W przedmiotowym przypadku wykorzystania przedstawiciel właściwego organu kontrolnego znajduje się w pojeździe będącym w ruchu i nakierowuje ręczny, przenośny *REDCR* znajdujący się wewnątrz pojazdu w kierunku środka szyby przedniej wybranego pojazdu albo *REDCR* jest zainstalowany w pojeździe lub na nim w taki sposób, by był skierowany w kierunku środka szyby przedniej wybranego pojazdu w momencie, gdy pojazd, w którym znajduje się czytnik wczesnego wykrywania na odległość, znajduje się w określonym położeniu względem wybranego pojazdu (na przykład bezpośrednio przed tym pojazdem w strumieniu ruchu). Kontrolę przeprowadza się przy wykorzystaniu interfejsów DSRC działających na częstotliwości 5,8 GHz w ramach ERC 70-03 i sprawdza pod kątem zgodności z odpowiednimi parametrami przewidzianymi w normie EN 300 674-1, jak opisano w sekcji 5. Zob. rys. 14.2. (przypadek wykorzystania 2).

Rysunek 14.2

Kontrola przeprowadzana z pojazdu korzystającego z interfejsów DSRC działających na częstotliwości 5,8 GHz



4.2 **Bezpieczeństwo/integralność**

Aby umożliwić weryfikację autentyczności i integralności danych pobranych w ramach łączności na odległość, zabezpieczone *Dane* są weryfikowane i deszyfrowane zgodnie z dodatkiem 11 Wspólne mechanizmy zabezpieczenia.

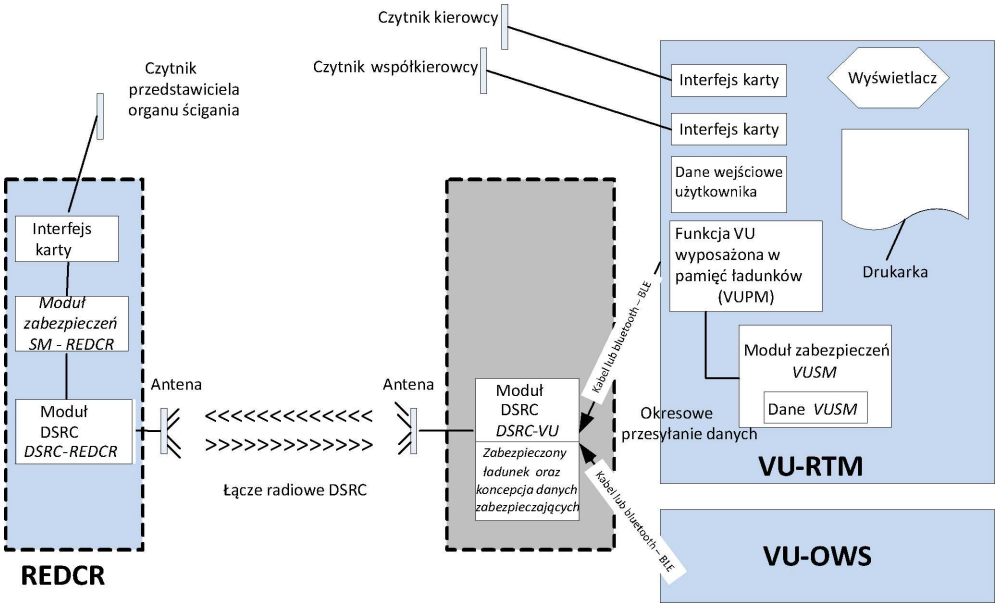
5 PROJEKT I PROTOKOŁY ŁĄCZNOŚCI NA ODLEGŁOŚĆ

5.1 **Projekt**

Projekt funkcji łączności na odległość w tachografie inteligentnym przedstawiono na rys. 14.3.

Rys. 14.3

Projekt funkcji łączności na odległość



DSC_19 W VU zlokalizowane są następujące funkcje:

— moduł zabezpieczeń (*VUSM*). Ta funkcja występująca w VU jest odpowiedzialna za zabezpieczanie *Danych* przesyłanych z *DSRC-VU* do przedstawiciela właściwych organów kontrolnych za pośrednictwem łączności na odległość;

— zabezpieczone dane są przechowywane w pamięci VUSM. W odstępach czasu określonych w pkt 4.1.1.1 (DSC_12) VU szyfruje i uzupełnia koncepcję RTMdata (która obejmuje wartości koncepcji danych ładunku i danych zabezpieczających określone poniżej w tym dodatku) przechowywaną w pamięci DSRC-VU. Działanie modułu zabezpieczeń jest zdefiniowane w dodatku 11 „Wspólne mechanizmy zabezpieczenia" i wykracza poza zakres niniejszego dodatku, z zastrzeżeniem konieczności zapewnienia aktualizacji urządzenia do łączności VU za każdym razem, gdy zmieniają się dane VUSM;

— łączność między VU a DSRC-VU może być łącznością przewodową lub łącznością opartą na technologii Bluetooth Low Energy (BLE), a jeżeli chodzi o fizyczną lokalizację DSRC-VU, może być ono zintegrowane z anteną umieszczoną na szybie przedniej pojazdu, może znajdować się wewnątrz VU lub może być umieszczone gdzieś pomiędzy;

— DSRC-VU posiada niezawodne źródło energii dostępne w każdej chwili. Sposób zasilania energią zależy od projektu;

— pamięć DSRC-VU jest pamięcią trwałą w celu utrzymania danych w DSRC-VU, nawet gdy zapłon pojazdu jest wyłączony;

— jeżeli łączność między VU a DSRC-VU odbywa się za pośrednictwem technologii BLE, a źródłem zasilania jest akumulator, którego nie można ponownie naładować, źródło zasilania DSRC-VU zastępuje się podczas każdego przeglądu okresowego, a producent urządzenia DSRC-VU jest odpowiedzialny za zapewnienie odpowiedniego zasilania energią między jednym przeglądem okresowym a drugim, utrzymując normalny dostęp do danych przez REDCR przez cały okres bez awarii lub przerwania dostaw;

— funkcja VU umożliwiająca zdalne monitorowanie tachografu i wyposażona w „pamięć na temat ładunków" (*VUPM*). Ta funkcja występująca w VU jest odpowiedzialna za dostarczanie i aktualizację *Danych*. Treść *Danych* („TachographPayload") jest zdefiniowana w pkt 5.4.4/5.4.5 poniżej i jest aktualizowana w odstępach czasu określonych w pkt 4.1.1.1 (DSC_12);

— DSRC-VU. Jest to funkcja w obrębie anteny lub połączona z anteną i nawiązująca łączność z VU za pośrednictwem połączenia przewodowego lub bezprzewodowego (BLE), które posiada aktualne dane (*dane VUPM*) i zarządza odpowiedziami na kontrolę prowadzoną przez nośnik DSRC działający na częstotliwości 5,8 GHz. Odłączenie urządzenia DSRC lub zakłócenie jego funkcjonowania podczas normalnej eksploatacji pojazdu z działającym urządzeniem DSRC interpretuje się jako naruszenie przepisów rozporządzenia (UE) nr 165/2014;

— moduł zabezpieczeń (REDCR) (*SM-REDCR*) to funkcja wykorzystywana do deszyfrowania i sprawdzania integralności danych pochodzących z VU. Środki umożliwiające osiągnięcie tego celu określono w dodatku 11 Wspólne mechanizmy zabezpieczenia, a nie w niniejszym dodatku;

— urządzenie DSRC (REDCR) (*DSRC-REDCR*) obejmuje nadajnik-odbiornik działający na częstotliwości 5,8 GHz i powiązane oprogramowanie wbudowane i oprogramowanie zwykłe, które zarządza *Łącznością* z *DSRC-VU* zgodnie z niniejszym dodatkiem;

— *DSRC-REDCR* wysyła zapytania do *DSRC-VU* w docelowym pojeździe i pozyskuje *Dane* (bieżące *dane VUPM* docelowego pojazdu) za pośrednictwem łącza DSRC oraz przetwarza i przechowuje otrzymane dane w swoim *SM-REDCR*;

— antenę *DSRC-VU* umieszcza się w miejscu, w którym zapewnia optymalną łączność DSRC między pojazdem a anteną drogową (zwykle w środkowej części szyby przedniej pojazdu lub blisko tej pozycji …). W przypadku pojazdów lekkich odpowiednie jest zainstalowanie anteny w górnej części szyby przedniej.

— Przed anteną lub w pobliżu anteny nie mogą znajdować się żadne metalowe przedmioty (np. identyfikatory, naklejki, antyodblaskowe (barwione) paski z folii, osłony przeciwsłoneczne, wycieraczki szyby przedniej w stanie spoczynku), które mogą zakłócać łączność.

— Antena musi być zamontowana tak, aby jej obszar pokrycia był mniej więcej równoległy do powierzchni drogi.

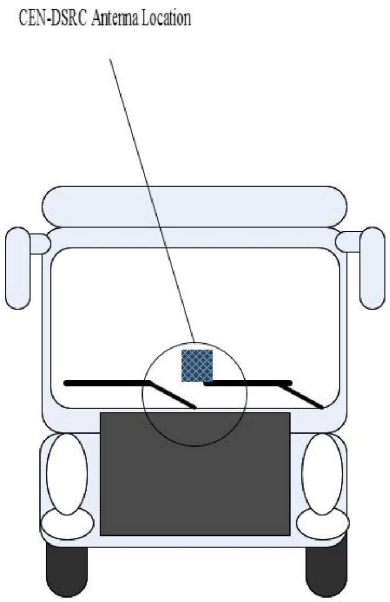
DSC_20 Antena i Łączność działają w ramach ERC 70-03, są sprawdzane pod kątem zgodności z odpowiednimi parametrami przewidzianymi w normie EN 300 674-1, jak opisano w sekcji 5. W odniesieniu do anteny i Łączności można wdrożyć techniki ograniczania ryzyka wystąpienia zakłóceń bezprzewodowych, jak opisano w sprawozdaniu ECC nr 228, przy użyciu np. filtrów w łączności CEN DSRC 5.8 GHz.

DSC_21 Antena DSRC jest połączona z funkcją DSRC-VU bezpośrednio w obrębie modułu zamontowanego na szybie przedniej lub blisko szyby przedniej lub poprzez dedykowany przewód zbudowany w taki sposób, aby utrudnić nielegalne odłączenie. Odłączenie lub zakłócenie funkcjonowania anteny stanowi naruszenie przepisów rozporządzenia (UE) nr 165/2014. Zamierzone maskowanie lub inne szkodliwe oddziaływanie na funkcjonowanie anteny interpretuje się jako naruszenie przepisów rozporządzenia (UE) nr 165/2014.

DSC_22 Współczynnik kształtu anteny nie został zdefiniowany i stanowi przedmiot decyzji handlowej, dopóki wbudowany DSRC-VU spełnia wymagania zgodności określone w sekcji 5 poniżej. Antena jest umieszczona w miejscu określonym w DSC_19 i przedstawionym na rys. 14.4 (linia owalna) i skutecznie wspomaga przypadki wykorzystania opisane w pkt 4.1.2 i 4.1.3.

Rys. 14.4

Przykładowe umieszczenie anteny DSRC działającej na częstotliwości 5,8 GHz na szybie przedniej pojazdów regulowanych



Współczynnik kształtu *REDCR* i jego anteny może różnić się w zależności od położenia czytnika (zamontowany statyw, urządzenie ręczne, zamontowany w pojeździe itd.) i trybu działania przyjętego przez przedstawiciela właściwych organów kontrolnych.

Funkcję wyświetlania lub powiadamiania wykorzystuje się do przedstawienia przedstawicielowi właściwych organów kontrolnych wyników funkcji łączności na odległość. Wyniki mogą być wyświetlane na ekranie, w formie wydruku, sygnału audio lub połączenia takich powiadomień. Forma takiego wyświetlenia lub powiadomienia jest kwestią wymogów przedstawicieli właściwych organów kontrolnych i projektu urządzenia i nie jest określona w niniejszym dodatku.

DSC_23 Współczynnik projektu i kształtu *REDCR* stanowi funkcję projektu komercyjnego, funkcjonującego w ramach ERC 70-03, oraz specyfikacji projektu i eksploatacji określonej w niniejszym dodatku (sekcja 5.3.2), tym samym zapewniając maksymalną elastyczność rynku w zakresie zaprojektowania i zapewnienia urządzenia mającego na celu zrealizowanie określonych scenariuszy kontroli dowolnego właściwego organu kontrolnego.

DSC_24 Współczynnik projektu i kształtu *DSRC-VU* i jego pozycjonowanie wewnątrz lub na zewnątrz VU stanowią funkcję projektu komercyjnego, funkcjonującego w ramach ERC 70-03, oraz specyfikacji projektu i eksploatacji określonej w niniejszym dodatku (sekcja 5.3.2) i w obrębie tej klauzuli (5.1).

DSC_25 W rozsądnym stopniu *DSRC-VU* musi być jednak w stanie zaakceptować wartości koncepcji danych z innego inteligentnego urządzenia rejestrującego za pomocą otwartego standardowego połączenia branżowego i protokołów (na przykład z urządzenia służącego do ważenia w pojeździe), dopóki takie koncepcje danych są określone unikatowymi i znanymi identyfikatorami aplikacji / nazwami plików, zaś instrukcje obsługi takich protokołów są udostępniane Komisji Europejskiej i są dostępne bezpłatnie dla producentów odpowiednich urządzeń.

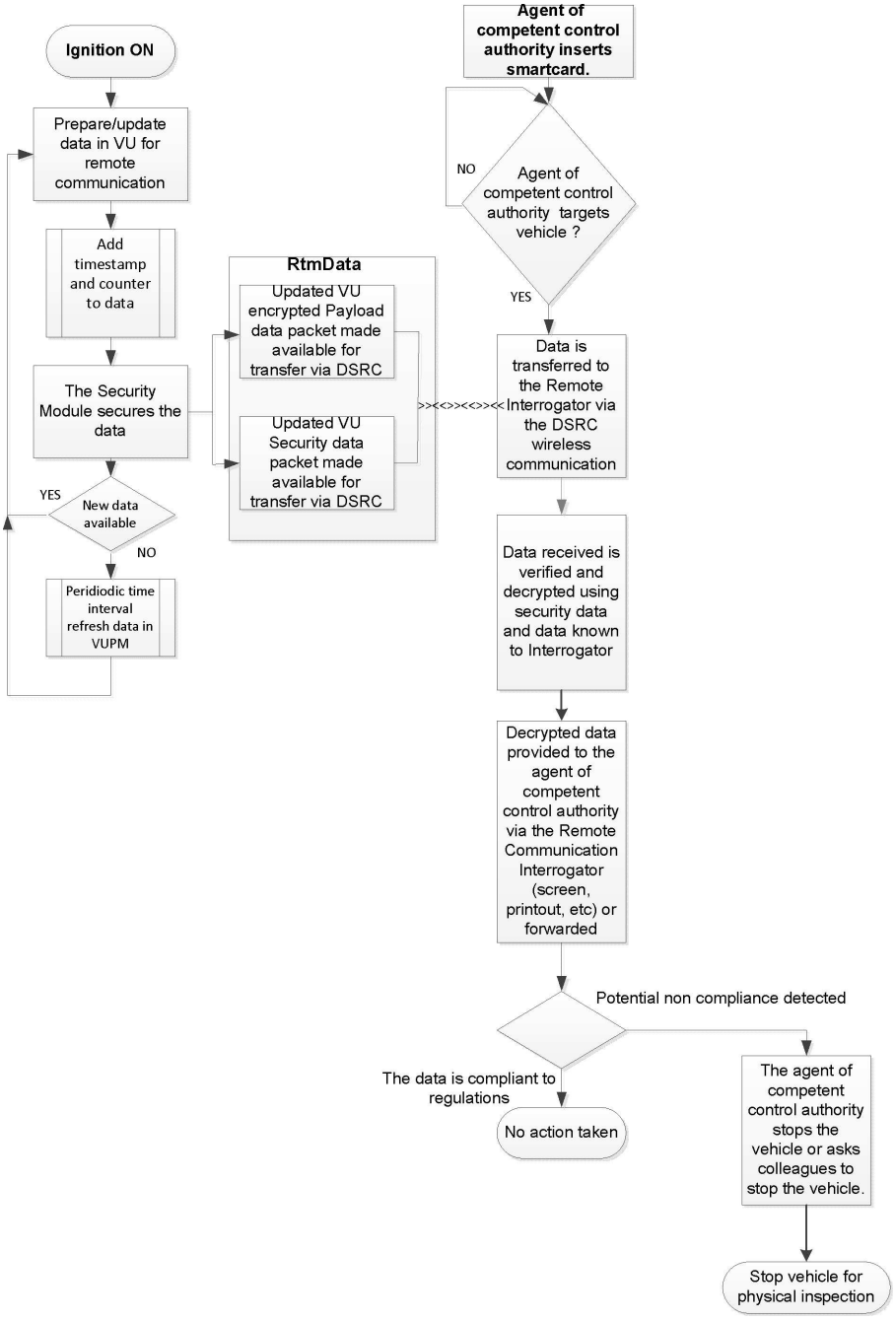
5.2 **Przepływ pracy**

5.2.1 *Operacje*

Na rys. 14.5 przedstawiono przepływ pracy w odniesieniu do operacji.

Rys. 14.5

Przepływ pracy w odniesieniu do funkcji łączności na odległość



Poszczególne kroki opisano poniżej:

a. ilekroć pojazd jest w ruchu (włączony zapłon), tachograf przekazuje dane funkcji VU. Funkcja VU przygotowuje *Dane* na potrzeby funkcji łączności na odległość (zaszyfrowane) i aktualizuje *VUPM* przechowywane w pamięci *DSRC-VU* (jak określono w pkt 4.1.1.1–4.1.1.2). Zebrane *Dane* formatuje się w sposób określony w pkt 5.4.4–5.4.5 poniżej;

b. przy każdej aktualizacji *Danych* aktualizuje się znacznik czasu określony w koncepcji danych zabezpieczających;

c. funkcja *VUSM* zabezpiecza dane zgodnie z procedurami określonymi w dodatku 11;

d. przy każdej aktualizacji *Danych* (zob. pkt 4.1.1.1–4.1.1.2) *Dane* przesyła się do DSRC-VU, gdzie zastępują one wszystkie poprzednie dane, aby w razie kontroli prowadzonej przez *REDCR* zawsze były dostępne zaktualizowane bieżące dane (*Dane*). W przypadku dostarczania *Danych* DSRC-VU przez VU *Dane* są identyfikowane po nazwie pliku *RTMData* lub ApplicationID i identyfikatorach atrybutu;

e. jeżeli przedstawiciel właściwych organów kontrolnych chce zgromadzić *Dane* z wybranego pojazdu docelowego, najpierw umieszcza swoją kartę elektroniczną w *REDCR* w celu umożliwienia *Łączności* i pozwolenia *SM-REDCR* na weryfikację autentyczności karty i deszyfrowanie danych;

f. przedstawiciel właściwego organu kontrolnego wybiera następnie pojazd i żąda przekazania danych za pośrednictwem łączności na odległość. *REDCR* otwiera sesję interfejsu DSRC działającego na częstotliwości 5,8 GHz z *DSRC-VU* pojazdu docelowego i żąda przekazania *Danych*. *Dane* są przesyłane do *REDCR* za pośrednictwem systemu łączności bezprzewodowej jako atrybut DSRC korzystający z usługi aplikacyjnej GET, jak określono w 5.4. Atrybut zawiera zaszyfrowane wartości danych ładunku oraz dane zabezpieczające DSCR;

g. dane są analizowane przez urządzenie *REDCR* i przekazywane przedstawicielowi właściwego organu kontrolnego;

h. przedstawiciel właściwego organu kontrolnego wykorzystuje dane do podjęcia decyzji o ewentualnym zatrzymaniu pojazdu do szczegółowej kontroli lub zwrócenia się do innego przedstawiciela właściwego organu kontrolnego o zatrzymanie pojazdu.

5.2.2 *Interpretacja danych otrzymanych za pośrednictwem łączności DSRC*

DSC_26 Dane otrzymywane przez interfejs działający na częstotliwości 5,8 GHz niosą tylko i wyłącznie znaczenie i import zdefiniowane w pkt 5.4.4 i 5.4.5 poniżej i są rozumiane zgodnie z celami określonymi w tych punktach. Zgodnie z przepisami rozporządzenia (UE) nr 165/2014 *Dane* wykorzystuje się jedynie w celu przekazania odpowiednich informacji właściwemu organowi kontrolnemu, aby pomóc mu w ustaleniu, czy należy zatrzymać pojazd do kontroli fizycznej, a następnie *Dane* te są niszczone zgodnie z art. 9 rozporządzenia (UE) nr 165/2014.

5.3 **Parametry interfejsu fizycznego DSRC w odniesieniu do łączności na odległość**

5.3.1 *Ograniczenia dotyczące lokalizacji*

DSC_27 Zdalnej kontroli pojazdów korzystających z interfejsu DSRC działającego na częstotliwości 5,8 GHz nie należy prowadzić w odległości do 200 metrów od uruchomionej suwnicy bramowej DSRC działającej na częstotliwości 5,8 GHz.

5.3.2 *Parametry łącza odbiorczego (downlink) i łącza nadawczego (uplink)*

DSC_28 Urządzenia wykorzystywane do zdalnego monitorowania tachografu muszą być zgodne z ERC70-03 i parametrami określonymi w tabelach 14.1 i 14.2 poniżej oraz muszą działać w ramach ERC70-03 i tych parametrów.

DSC_29 Ponadto aby zapewnić zgodność z parametrami operacyjnymi innych standardowych systemów DSRC działających na częstotliwości 5,8 GHz, urządzenie wykorzystywane do zdalnego monitorowania tachografu musi być zgodne z parametrami określonymi w normach EN 12253 i EN 13372.

Mianowicie:

Tabela 14.1

Parametry łącza odbiorczego

Nr pozycji	Parametr	Wartości	Uwagi
D1	Częstotliwości nośne łącza odbiorczego	Istnieją cztery alternatywne częstotliwości, których może używać REDCR: 5,7975 GHz 5,8025 GHz 5,8075 GHz 5,8125 GHz	W ramach ERC 70-03. Częstotliwości nośne mogą zostać wybrane przez podmiot wdrażający system przydrożny i nie muszą być znane w DSRC-VU. (zgodnie z normami EN 12253 i EN 13372)
D1a (*)	Tolerancja częstotliwości nośnych	w ramach ± 5 ppm	(zgodnie z normą EN 12253)
D2 (*)	Maska zakresu nadajnika RSU (REDCR)	W ramach ERC 70-03. REDCR jest zgodny z klasą B,C, jak określono w normie 12253. Brak innych szczególnych wymogów określonych w tym załączniku	Parametr stosowany do kontrolowania zakłóceń pomiędzy interrogatorami znajdującymi się blisko siebie (jak określono w normach EN 12253 i EN 13372).
D3	OBU(DSRC-VU) Minimalny zakres częstotliwości	5,795–5,815 GHz	(zgodnie z normą EN 12253)
D4 (*)	Maksymalna EIRP	W ramach ERC 70-03 (nielicencjonowanego) i rozporządzenia krajowego Maksymalna wartość + 33 dBm	(zgodnie z normą EN 12253)
D4a	Maska kątowa EIRP	Zgodnie z zadeklarowaną i opublikowaną specyfikacją projektanta interrogatora	(zgodnie z normą EN 12253)
D5	Polaryzacja	Lewostronna kołowa	(zgodnie z normą EN 12253)
D5a	Polaryzacja krzyżowa	XPD: Na obszarze pokrycia: (REDCR) RSU t ≥ 15 dB (DSRC-VU) OBU r ≥ 10 dB Na obszarze -3 dB: (REDCR) RSU t ≥ 10 dB (DSRC-VU) OBU r ≥ 6 dB	(zgodnie z normą EN 12253)
D6 (*)	Modulacja	Dwupoziomowa modulacja amplitudy	(zgodnie z normą EN 12253)
D6a (*)	Indeks modulacji	0,5 … 0,9	(zgodnie z normą EN 12253)

Nr pozycji	Parametr	Wartości	Uwagi
D6b	Wzorzec ruchu gałek ocznych	≥90 % (czas) / ≥85 % (amplituda)	
D7 (*)	Kodowanie danych	FM0 Bit „1” posiada przejścia jedynie na początku i końcu interwału bitowego. Bit „0” posiada dodatkowe przejście w środku interwału bitowego w porównaniu z bitem „1”.	(zgodnie z normą EN 12253)
D8 (*)	Szybkość transmisji bitów	500 kBit/s	(zgodnie z normą EN 12253)
D8a	Tolerancja zegara częstotliwości	wyższa niż ± 100 ppm	(zgodnie z normą EN 12253)
D9 (*)	Bitowa stopa błędów (BER) w odniesieniu do łączności	≤ 10^{-6}, gdy moc padająca w przyrządzie instalowanym w pojeździe (DSRC-VU) mieści się w zakresie podanym w pkt [D11a–D11b].	(zgodnie z normą EN 12253)
D10	Czynnik uruchamiający OBU (DSRC-VU)	OBU (DSRC-VU) uruchamia się po otrzymaniu dowolnej ramki zawierającej co najmniej 11 oktetów (w tym preambułę)	Nie jest konieczny żaden specjalny wzór uruchamiania. DSRC-VU może uruchomić się po otrzymaniu ramki zawierającej mniej niż 11 oktetów (zgodnie z normą EN 12253)
D10a	Maksymalna godzina rozpoczęcia	≤5 ms	(zgodnie z normą EN 12253)
D11	Strefa łączności	Region przestrzenny, w którym osiąga się BER zgodną z D9a	(zgodnie z normą EN 12253)
D11a (*)	Limit zasilania w odniesieniu do łączności (górna)	– 24 dBm	(zgodnie z normą EN 12253)
D11b (*)	Limit zasilania w odniesieniu do łączności (dolna)	Moc zdarzenia: – 43 dBm (obszar pokrycia) – 41 dBm (w przedziale – 45° ± 45° odpowiadającym płaszczyźnie równoległej do powierzchni drogi, gdy DSRC-VU jest później instalowany w pojeździe (azymut))	(zgodnie z normą EN 12253) Rozszerzony wymóg w odniesieniu do kątów poziomych do ±45°, ze względu na przypadki wykorzystania zdefiniowane w niniejszym załączniku.
D12 (*)	Poziom odcięcia zasilania (DSRC-VU)	– 60 dBm	(zgodnie z normą EN 12253)
D13	Preambuła	Preambuła jest obowiązkowa.	(zgodnie z normą EN 12253)
D13a	Długość i wzór preambuły	16 bitów ± 1 bit FM0 zakodowany jako bity „1”	(zgodnie z normą EN 12253)

Nr pozycji	Parametr	Wartości	Uwagi
D13b	Kształt fali preambuły	Sekwencja naprzemienna o niskim i wysokim poziomie z czasem trwania impulsu równym 2 μs. Tolerancja podana w D8a	(zgodnie z normą EN 12253)
D13c	Bity pomocnicze	RSU (REDCR) może przesłać maksymalnie 8 bitów po fladze końcowej. Od OBU (DSRC-VU) nie wymaga się, aby uwzględniał te dodatkowe bity.	(zgodnie z normą EN 12253)

(*) – Parametry łącza odbiorczego z zastrzeżeniem sprawdzenia pod kątem zgodności z odpowiednim testem parametrów przewidzianym w normie EN 300 674-1.

Tabela 14.2

Parametry łącza nadawczego

Nr pozycji	Parametr	Wartości	Uwagi
U1 (*)	Częstotliwości podnośne	OBU (DSRC-VU) obsługuje częstotliwości 1,5 MHz i 2,0 MHz RSU (REDCR) obsługuje częstotliwość 1,5 MHz lub 2,0 MHz lub obie. U1-0: 1,5 MHz U1-1: 2,0 MHz	Wybór częstotliwości podnośnej (1,5 MHz lub 2,0 MHz) zależy od wybranego profilu określonego w normie EN 13372.
U1a (*)	Tolerancja częstotliwości podnośnych	w ramach ± 0,1 %	(zgodnie z normą EN 12253)
U1b	Wykorzystanie wstęg bocznych	Takie same dane po obu stronach	(zgodnie z normą EN 12253)
U2 (*)	Maska zakresu nadajnika OBU (DSRC-VU)	Zgodnie z EN 12253 1) Moc poza pasmem zob. ETSI EN 300674-1 2) Moc na paśmie: [U4a] dBm w 500 kHz 3) Emisja na dowolnym innym kanale łącza nadawczego: U2(3)-1 = -35 dBm w 500 kHz	(zgodnie z normą EN 12253)
U4a (*)	Maksymalna modulacja jednowstęgowa EIRP (obszar pokrycia)	Dwie opcje: U4a-0: – 14 dBm U4a-1: – 21 dBm	Zgodnie z zadeklarowaną i opublikowaną specyfikacją projektanta urządzenia
U4b (*)	Maksymalna modulacja jednowstęgowa EIRP (35°)	Dwie opcje: — Nie dotyczy — – 17 dBm	Zgodnie z zadeklarowaną i opublikowaną specyfikacją projektanta urządzenia
U5	Polaryzacja	Lewostronna kołowa	(zgodnie z normą EN 12253)

Nr pozycji	Parametr	Wartości	Uwagi
U5a	Polaryzacja krzyżowa	XPD: Na obszarze pokrycia: (REDCR) RSU r ≥ 15 dB (DSRC-VU) OBU t ≥ 10 dB Na obszarze – 3 dB: (REDCR) RSU r ≥ 10 dB (DSRC-VU) OBU t ≥ 6 dB	(zgodnie z normą EN 12253)
U6	Modulacja podnośna	2-PSK Zakodowane dane zsynchronizowane z częstotliwością podnośną: przejścia zakodowanych danych zbieżne z przejściami częstotliwości podnośnej.	(zgodnie z normą EN 12253)
U6b	Cykl roboczy	Cykl roboczy: 50 % ± α, α ≤5 %	(zgodnie z normą EN 12253)
U6c	Modulacja na nośniku	Mnożenie modulowanej częstotliwości podnośnej przez częstotliwość nośną.	(zgodnie z normą EN 12253)
U7 (*)	Kodowanie danych	NRZI (Brak przejścia na początku bitu „1”, przejście na początku bitu „0”, brak przejścia w ramach bitu)	(zgodnie z normą EN 12253)
U8 (*)	Szybkość transmisji bitów	250 kBit/s	(zgodnie z normą EN 12253)
U8a	Tolerancja zegara częstotliwości	w ramach ± 1 000 ppm	(zgodnie z normą EN 12253)
U9	Bitowa stopa błędów (B. E.R.) w odniesieniu do łączności	$\leq 10^{-6}$	(zgodnie z normą EN 12253)
U11	Strefa łączności	Region przestrzenny, w którym zlokalizowany jest DSRC-VU, tak że jego transmisje są odbierane przez REDCR przy BER mniejszej niż ta podana w pkt U9a.	(zgodnie z normą EN 12253)
U12a (*)	Zysk z konwersji (dolna granica)	1 dB dla każdej wstęgi bocznej Zakres kątowy: kołowo-symetryczny pomiędzy obszarem pokrycia a ± 35° oraz	
		w przedziale – 45° ± 45° odpowiadającym płaszczyźnie równoległej do powierzchni drogi, gdy DSRC-VU jest później instalowany w pojeździe (azymut)	Większy niż określony zakres wartości dla kątów poziomych do ± 45° ze względu na przypadki wykorzystania zdefiniowane w niniejszym załączniku.
U12b (*)	Zysk z konwersji (górna granica)	10 dB dla każdej wstęgi bocznej	Niższy niż określony zakres wartości dla każdej wstęgi bocznej w obrębie stożka kołowego wokół obszaru pokrycia ± 45° kąta otwarcia.
U13	Preambuła	Preambuła jest obowiązkowa.	(zgodnie z normą EN 12253)

Nr pozycji	Parametr	Wartości	Uwagi
U13a	Długość i wzór preambuły	32–36 µs modulowane jedynie przy użyciu częstotliwości podnośnej, a następnie 8 bitów „0" zakodowanych jako NRZI.	(zgodnie z normą EN 12253)
U13b	Bity pomocnicze	DSRC-VU może przesłać maksymalnie 8 bitów po fladze końcowej. Od RSU (REDCR) nie wymaga się, aby uwzględniał te dodatkowe bity.	(zgodnie z normą EN 12253)

(*) – Parametry łącza nadawczego z zastrzeżeniem sprawdzenia zgodności z odpowiednim testem parametrów przewidzianym w normie EN 300 674-1.

5.3.3 *Projekt anteny*

5.3.3.1 Antena REDCR

DSC_30 Projekt anteny *REDCR* stanowi funkcję projektu komercyjnego, funkcjonującego w granicach określonych w pkt 5.3.2, który dostosowano, aby zoptymalizować wydajność odczytu *DSRC-REDCR* w określonym celu oraz aby odczytać okoliczności, w których w założeniu *REDCR* ma funkcjonować.

5.3.3.2 Antena VU

DSC_31 Projekt anteny *DSRC-VU* stanowi funkcję projektu komercyjnego, funkcjonującego w granicach określonych w pkt 5.3.2, które dostosowano, aby zoptymalizować wydajność odczytu *DSRC-REDCR* w określonym celu oraz aby odczytać okoliczności, w których w założeniu *REDCR* ma funkcjonować.

DSC_32 Antena VU jest zamontowana na szybie przedniej pojazdu lub blisko szyby przedniej, jak określono w pkt 5.1 powyżej.

DSC_33 W środowisku testowym w warsztacie (zob. sekcja 6.3) antena DSRC-VU, umieszczona zgodnie z pkt 5.1 powyżej, powinna skutecznie połączyć się za pomocą standardowej łączności testowej i skutecznie zapewnić transakcję RTM, jak określono w tym dodatku, na odległość od 2 do 10 m, z wynikiem lepszym niż 99 % przypadków, uśrednionym do 1 000 kontroli odczytów.

5.4 **Wymogi protokołu DSRC w odniesieniu do zdalnego monitorowania tachografu**

5.4.1 *Informacje ogólne*

DSC_34 Protokół transakcji służący do pobierania *Danych* za pomocą połączenia interfejsu DSRC działającego na częstotliwości 5,8 GHz przebiega zgodnie z następującymi krokami. W niniejszej sekcji opisuje się przepływ transakcji w warunkach idealnych, bez retransmisji czy zakłóceń łączności.

UWAGA: celem etapu inicjacji (krok 1) jest ustanowienie łączności między *REDCR* a DSRC-VU, które znalazły się w strefie transakcji DSRC w częstotliwości 5,8 GHz (tryb nadrzędny-podrzędny), ale jeszcze nie nawiązały łączności z *REDCR*, a także zgłoszenie procesów aplikacji.

— **Krok 1** Inicjacja. *REDCR* wysyła ramkę zawierającą tabelę usług sygnału (BST), która zawiera identyfikatory aplikacji (AID) w wykazie obsługiwanych usług. W aplikacji RTM będzie to po prostu usługa z wartością AID = 2 (Freight&Fleet). *DSRC-VU* dokonuje oceny otrzymanej BST i odpowiada (zob. poniżej), przekazując wykaz obsługiwanych aplikacji w ramach domeny Freight&Fleet, lub nie odpowiada, jeżeli żadne aplikacje nie są obsługiwane. Jeżeli *REDCR* nie oferuje AID=2, DSRC-VU nie odpowiada *REDCR*.

— **Krok 2** *DSRC-VU* wysyła ramkę zawierającą żądane przydzielenia okna prywatnego.

— **Krok 3** *REDCR* wysyła ramkę z przydziałem okna prywatnego.

— **Krok 4** *DSRC-VU* używa przydzielonego okna prywatnego do wysłania ramki zawierającej jego tabelę usług pojazdu (VST). Tego rodzaju VST zawiera wykaz wszystkich różnych wystąpień aplikacji obsługiwanych przez ten *DSRC-VU* w ramach AID=2. Poszczególne wystąpienia są identyfikowane za pomocą jednorazowo generowanych identyfikatorów elementu, z których każdy jest powiązany z wartością parametru znacznika kontekstowego aplikacji określającą obsługiwaną aplikację i normę.

— **Krok 5** Następnie *REDCR* analizuje oferowaną tabelę usług pojazdu i albo przerywa łączność (RELEASE), ponieważ nie jest zainteresowany niczym, co dana VST ma do zaoferowania (tj. otrzymuje VST od *DSRC-VU*, który nie obsługuje transakcji RTM), albo – jeżeli otrzymuje odpowiednią tabelę usług pojazdu – uruchamia wystąpienie aplikacji.

— **Krok 6** Aby osiągnąć ten cel, REDCR wysyła ramkę zawierającą polecenie pobrania danych dotyczących zdalnego monitorowania tachografu i identyfikującą wystąpienie aplikacji RTM poprzez wskazanie identyfikatora odpowiadającego wystąpieniu aplikacji RTM (jak określił DSRC-VU w VST) oraz przydziela okno prywatne.

— **Krok 7** *DSRC-VU* używa nowo przydzielonego okna prywatnego do wysłania ramki zawierającej adresowany identyfikator odpowiadający wystąpieniu aplikacji RTM zgodnie z VST, po którym następuje atrybut *RtmData* (element ładunku + element bezpieczeństwa).

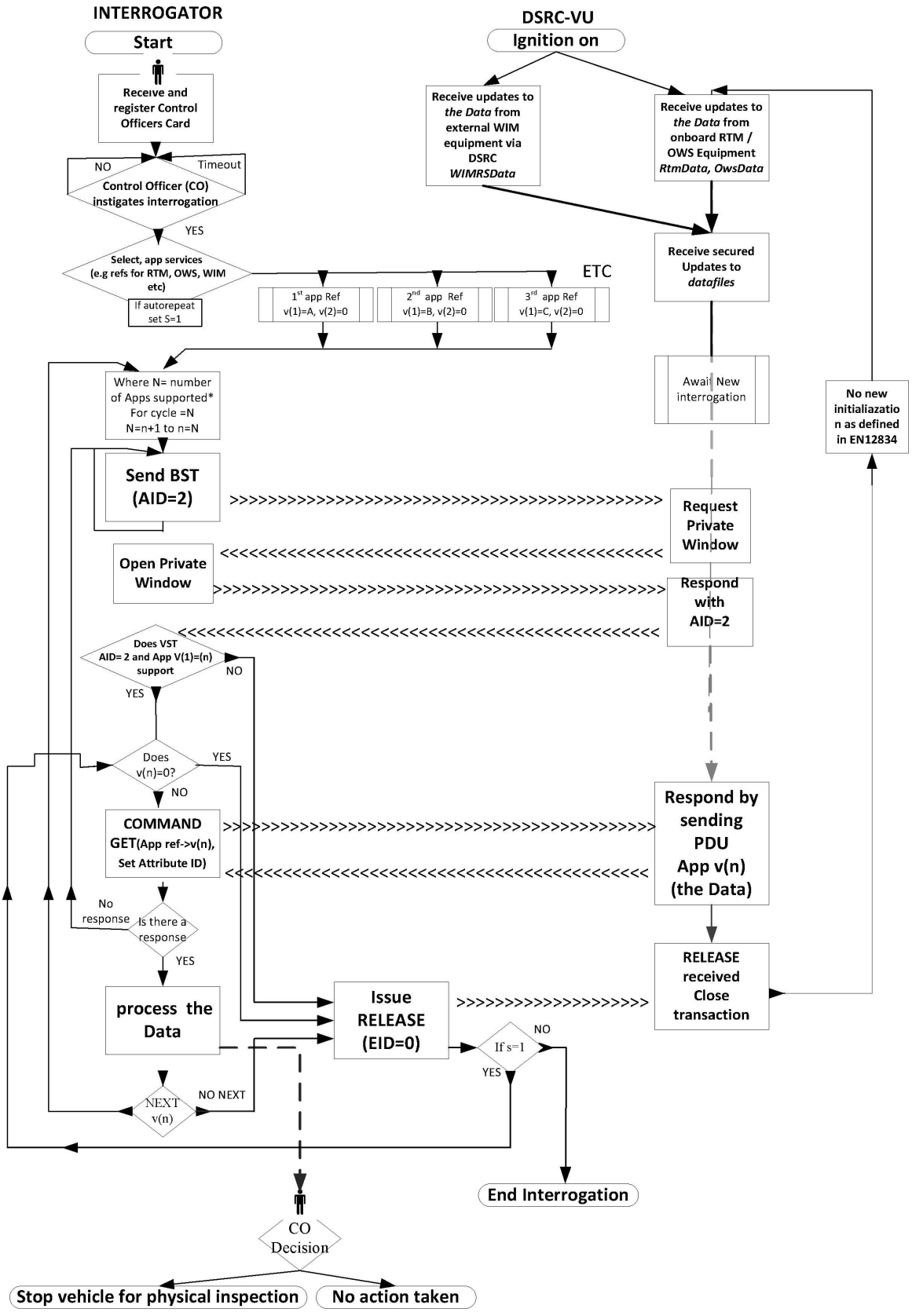
— **Krok 8** W przypadku żądania wielu usług wartość „n” zmienia się na kolejny numer referencyjny usługi i procedura zostaje powtórzona.

— **Krok 9** *REDCR* potwierdza otrzymanie danych, wysyłając do *DSRC-VU* ramkę zawierającą polecenie RELEASE w celu przerwania sesji LUB, jeżeli nie zatwierdził pomyślnego otrzymania LPDU, wraca do kroku 6.

Zob. rys. 14.6 przedstawiający graficzny opis protokołu transakcji.

Rys. 14.6

Zdalne monitorowanie tachografu w ramach przepływu procesów DSRC na częstotliwości 5,8 GHz



5.4.2 *Polecenia*

DSC_35 Poniższe polecenia stanowią jedyne funkcje stosowane na etapie transakcji RTM:

— **INITIALISATION.request**: polecenie wysyłane z REDCR w formie emisji z definicją aplikacji obsługiwanych przez ten REDCR;

— **INITIALISATION.response**: odpowiedź z DSRC-VU potwierdzająca połączenie i zawierająca wykaz obsługiwanych wystąpień aplikacji wraz z charakterystyką oraz informacjami na temat sposobu postępowania z nimi (EID);

— **GET.request**: polecenie wysyłane z *REDCR* do *DSRC-VU*, określające wystąpienie aplikacji, którym należy się zająć, za pomocą zdefiniowanego EID otrzymanego w VST, oraz nakazujące *DSRC-VU* wysłanie wybranego(-ych) atrybutu(-ów) z *Danymi*. Celem polecenia GET jest umożliwienie *REDCR* otrzymania *Danych* od *DSRC-VU*;

— **GET.response**: odpowiedź z DSRC-VU zawierająca żądane *Dane*;

— **ACTION.request ECHO**: polecenie nakazujące *DSRC-VU* odesłanie danych z *DSRC-VU* do *REDCR*. Celem polecenia ECHO jest umożliwienie warsztatom lub placówkom przeprowadzających testy na potrzeby homologacji typu zbadania, czy połączenie DSRC działa bez konieczności dostępu do poświadczeń zabezpieczenia;

— **ACTION**.response ECHO: odpowiedź z DSRC-VU na polecenie ECHO;

— **EVENT_REPORT.request** RELEASE: polecenie informujące *DSRC-VU* o zakończeniu transakcji. Celem polecenia RESEALSE jest zakończenie sesji z *DSRC-VU*. Po otrzymaniu polecenia RELEASE *DSRC-VU* nie odpowiada na żadne dalsze zapytania w ramach bieżącego połączenia. Należy zauważyć, że zgodnie z wymogami normy EN 12834 DSRC-VU nie połączy się drugi raz z tym samym interrogatorem, chyba że znajdował się poza strefą łączności przez 255 sekund lub identyfikator sygnału interrogatora został zmieniony.

5.4.3 *Sekwencja polecenia zapytania*

DSC_36 Z perspektywy sekwencji polecenia i odpowiedzi transakcję opisuje się w następujący sposób:

Sekwencja	Nadajnik		Odbiornik	Opis	Działanie
1	REDCR	>	DSRC-VU	Inicjacja łącza komunikacyjnego żądanie	REDCR emituje BST
2	*DSRC-VU*	>	*REDCR*	*Inicjacja łącza komunikacyjnego odpowiedź*	*Jeżeli BST obsługuje AID=2, to DSRC-VU żąda okna prywatnego*
3	REDCR	>	DSRC-VU	Przyznaje okno prywatne	Wysyła ramkę zawierającą przydział okna prywatnego
4	*DSRC-VU*	>	*REDCR*	*Wysyła VST*	*Wysyła ramkę zawierającą VST*
5	REDCR	>	DSRC-VU	Wysyła GET.request w odniesieniu do danych zawartych w Atrybucie dotyczącym konkretnego EID	
6	*DSRC-VU*	>	*REDCR*	*Wysyła GET.response z żądanym atrybutem dotyczącym konkretnego EID*	*Wysyła Atrybut (RTMData, OWS-Data….) zawierający dane dotyczące konkretnego EID*

Sekwencja	Nadajnik		Odbiornik	Opis	Działanie
7	REDCR	>	DSRC-VU	Wysyła GET.request w odniesieniu do danych zawartych w innym Atrybucie (w razie potrzeby)	
8	*DSRC-VU*	>	*REDCR*	*Wysyła GET.response z żądanym atrybutem*	*Wysyła Atrybut zawierający dane dotyczące konkretnego EID*
9	REDCR	>	DSRC-VU	Potwierdza pomyślne otrzymanie danych	Wysyła polecenie RELEASE zamykające transakcję
10	*DSRC-VU*			*Zamyka transakcję*	

Przykład sekwencji transakcji i zawartości wymienianych ramek przedstawiono w pkt 5.4.7 i 5.4.8.

5.4.4 *Struktury danych*

DSC_37 Struktura semantyczna *Danych* przekazywanych przez interfejs DSRC działający na częstotliwości 5,8 GHz jest zgodna ze strukturą opisaną w niniejszym dodatku. Strukturę tych danych przedstawiono w tym punkcie.

DSC_38 Ładunek (dane dotyczące zdalnego monitorowania tachografu) składa się z połączenia:

1. danych EncryptedTachographPayload stanowiących zaszyfrowane dane TachographPayload określone w specyfikacji ASN.1 w sekcji 5.4.5. Metodę szyfrowania opisano w dodatku 11;
2. danych DSRCSecurityData określonych w dodatku 11.

DSC_39 Dane dotyczące zdalnego monitorowania tachografu opisuje się jako Atrybut RTM = 1 i przekazuje w kontenerze RTM = 10.

DSC_40 Znacznik kontekstowy RTM określa obsługiwaną część normy w serii norm TARV (RTM odnosi się do części 9).

Zawarta w module ASN.1 definicja danych DSRC w ramach aplikacji RTM jest następująca:

```
   TarvRtm {iso(1) standard(0) 15638 part9(9) version1(1)}
   DEFINITIONS AUTOMATIC TAGS
   ::= BEGIN
   IMPORTS
   -- Imports data attributes and elements from EFC which are used for RTM
   LPN
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Imports function parameters from the EFC Application Interface Definition
   SetMMIRq
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Imports the L7 DSRCData module data from the EFC Application Interface Definition
   Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
   Attributes,
   BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
   EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
   ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
   FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};


   -- Definitions of the RTM functions:
   RTM-InitialiseComm-Request ::= BST
   RTM-InitialiseComm-Response::= VST
   RTM-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials ABSENT,iid
   ABSENT,  attrIdList})
   RTM-DataRetrieval-Response::= Get-Response {RtmContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
   RTM-TerminateComm::= Event-Report-Request {RtmContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
   eventType (0)})

   RTM-TestComm-Request::= Action-Request {RtmContainer} (WITH COMPONENTS {..., eid (0), actionType
   (15), accessCredentials ABSENT, iid ABSENT})

   RTM-TestComm-Response::= Action-Response {RtmContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
   (0), iid ABSENT})

   -- Definitions of the RTM attributes:
   RtmData ::= SEQUENCE {
        encryptedTachographPayload OCTET STRING (SIZE(67)) (CONSTRAINED BY { -- calculated encrypting
   TachographPayload as per Appendix 11 --}),
        DSRCSecurityData OCTET STRING
        }
   TachographPayload ::= SEQUENCE {
              tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
              tp15638SpeedingEvent            BOOLEAN,  -- 1= Irregularities in speed (see Annex 1C)
              tp15638DrivingWithoutValidCard  BOOLEAN,     -- 1= Invalid card usage (see Annex 1C)
              tp15638DriverCard               BOOLEAN,-- 0= Indicates a valid driver card  (see Annex 1C)
              tp15638CardInsertion            BOOLEAN, -- 1= Card insertion while driving (see Annex 1C)
              tp15638MotionDataError          BOOLEAN, -- 1= Motion data error (see Annex 1C)
              tp15638VehicleMotionConflict    BOOLEAN, -- 1= Motion conflict (see Annex 1C)
              tp156382ndDriverCard            BOOLEAN, -- 1= Second driver card inserted (see Annex 1C)
              tp15638CurrentActivityDriving   BOOLEAN, -- 1= other activity selected;
                                                        -- 0= driving selected
              tp15638LastSessionClosed        BOOLEAN, -- 1= improperly, 0= properly, closed
              tp15638PowerSupplyInterruption  INTEGER (0..127), -- Supply interrupts in the last 10 days
              tp15638SensorFault              INTEGER (0..255),-- eventFaultType as per data dictionary
   -- All subsequent time related types as defined in Annex 1C.
              tp15638TimeAdjustment           INTEGER(0..4294967295), -- Time of the last time adjustment
              tp15638LatestBreachAttempt      INTEGER(0..4294967295), -- Time of last breach attempt
              tp15638LastCalibrationData      INTEGER(0..4294967295), -- Time of last calibration data
              tp15638PrevCalibrationData      INTEGER(0..4294967295), -- Time of previous calibration data
              tp15638DateTachoConnected       INTEGER(0..4294967295), -- Date tachograph connected
              tp15638CurrentSpeed             INTEGER (0..255), -- Last current recorded speed
              tp15638Timestamp                INTEGER(0..4294967295) -- Timestamp of current record[2]
              }
Rtm-ContextMark ::= SEQUENCE {
  standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version

  RtmCommProfile          INTEGER {
                                C1 (1),
                                C2 (2)
                                } (0..255) DEFAULT 1
  }
RtmTransferAck ::= INTEGER {
                  Ok (1),
                  NoK (2)
                  } SIZE (1..255)
```

```
StandardIdentifier ::= OBJECT IDENTIFIER
RtmContainer ::= CHOICE {
        integer                         [0]    INTEGER,
        bitstring                       [1]    BIT STRING,
        octetstring                     [2]    OCTET STRING (SIZE (0..127, ...)),
        universalString                 [3]    UniversalString,
        beaconId                        [4]    BeaconID,
        t-apdu                          [5]    T-APDUs,
        dsrcApplicationEntityId         [6]    DSRCApplicationEntityID,
        dsrc-Ase-Id                     [7]    Dsrc-EID,
        attrIdList                      [8]    AttributeIdList,
        attrList                        [9]    AttributeList{RtmContainer},
        rtmData                         [10]   RtmData,
        rtmContextmark                  [11]   Rtm-ContextMark,
        reserved12                      [12]   NULL,
        reserved13                     [13]   NULL,
        reserved14                      [14]   NULL,
        time                            [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
        }}

END
```

5.4.5 *Elementy danych dotyczących zdalnego monitorowania tachografu (RtmData), wykonywane czynności i definicje*

DSC_41 Wartości danych, które mają zostać obliczone przez VU i wykorzystane do uaktualnienia zabezpieczonych danych w DSRC-VU, oblicza się zgodnie z zasadami przedstawionymi w tabeli 14.3:

Tabela 14.3

Elementy RtmData, wykonywane czynności i definicje

(1) Element danych RTM	(2) Czynność wykonywana przez VU		(3) Definicja danych w ASN.1
RTM1 **Tablica rejestracyjna pojazdu**	VU ustala wartość *tp15638VehicleRegistrationPlate* elementu danych RTM1 na podstawie zarejestrowanej wartości typu danych *VehicleRegistrationIdentification*, jak określono w dodatku 1 *VehicleRegistrationIdentification*	Numer tablicy rejestracyjnej pojazdu wyrażony jako ciąg znaków	`tp15638VehicleRegstrationPlate LPN, --numer tablicy rejestracyjnej pojazdu zaimportowany z normy ISO 14906 z ograniczeniem określonym w normie EN 15509 stanowiący SEKWENCJĘ składającą się z kodu państwa, po którym następuje wskaźnik alfabetu , a następnie sam numer tablicy rejestracyjnej, który zawsze składa się z 14 oktetów (wypełniony zerami), tak aby długość typu LPN zgodnie z normą EN 15509 zawsze wynosiła 17 oktetów, z których 14 oktetów stanowi „faktyczny” numer`

(1) Element danych RTM	(2) Czynność wykonywana przez VU		(3) Definicja danych w ASN.1
RTM2 **Zdarzenia polegające na przekroczeniu prędkości**	VU generuje wartość logiczną w odniesieniu do elementu danych RTM2 tp15638SpeedingEvent. VU oblicza wartość tp15638SpeedingEvent na podstawie liczby zdarzeń przekroczenia prędkości zarejestrowanych w VU w ciągu ostatnich 10 dni występowania, jak określono w załączniku 1C. Jeżeli w ostatnich 10 dniach występowania zarejestrowano co najmniej jedno zdarzenie tp15638SpeedingEvent, ustawia się wartość tp15638SpeedingEvent na PRAWDA. W PRZECIWNYM WYPADKU, jeżeli w ostatnich 10 dniach występowania nie zarejestrowano żadnego zdarzenia, ustawia się wartość tp15638SpeedingEvent na FAŁSZ.	1 (PRAWDA) – wskazuje na nieprawidłowości w prędkości w ciągu 10 ostatnich dni występowania	`tp15638speedingEvent BOOLEAN,`
RTM3 **Prowadzenie pojazdu bez ważnej karty**	VU generuje wartość logiczną w odniesieniu do elementu danych RTM3. tp15638DrivingWithoutValidCard. VU przypisuje wartość PRAWDA zmiennej tp15638DrivingWithoutValidCard w przypadku zarejestrowania w danych VU w ciągu ostatnich 10 dni występowania co najmniej jednego zdarzenia typu „Prowadzenie bez prawidłowej karty", jak określono w załączniku 1C. W PRZECIWNYM WYPADKU, jeżeli w ostatnich 10 dniach występowania nie zarejestrowano żadnego zdarzenia, ustawia się wartość zmiennej tp15638DrivingWithoutValidCard na FAŁSZ.	1 (PRAWDA) = wskazuje na stosowanie nieważnej karty	`tp15638DrivingWithoutValidCard` `BOOLEAN,`
RTM4 **Ważna karta kierowcy**	VU generuje wartość logiczną w odniesieniu do elementu danych RTM4 tp15638DriverCard na podstawie danych zgromadzonych w VU i określonych w dodatku 1. W przypadku braku ważnej karty kierowcy VU ustawia wartość zmiennej na PRAWDA. W PRZECIWNYM WYPADKU, jeżeli istnieje ważna karta kierowcy, VU ustawia wartość zmiennej na FAŁSZ.	0 (FAŁSZ) = wskazuje istnienie ważnej karty kierowcy	`tp15638DriverCard BOOLEAN,`
RTM5 **Włożenie karty podczas prowadzenia pojazdu**	VU generuje wartość logiczną w odniesieniu do elementu danych RTM5. VU przypisuje wartość PRAWDA zmiennej tp15638CardInsertion w przypadku zarejestrowania w danych VU w ciągu ostatnich 10 dni występowania co najmniej jednego zdarzenia typu „włożenie karty podczas prowadzenia pojazdu", jak określono w załączniku 1C. W PRZECIWNYM WYPADKU, jeżeli w ostatnich 10 dniach występowania nie zarejestrowano żadnego takiego zdarzenia, ustawia się wartość zmiennej tp15638CardInsertion na FAŁSZ.	1 (PRAWDA) = wskazuje na wystąpienie zdarzenia polegającego na włożeniu karty podczas prowadzenia pojazdu w ciągu 10 ostatnich występowania	`tp15638CardInsertion BOOLEAN,`
RTM6 **Błąd danych dotyczących ruchu**	VU generuje wartość logiczną w odniesieniu do elementu danych RTM6. VU przypisuje wartość PRAWDA zmiennej tp15638MotionDataError w przypadku zarejestrowania w danych VU w ciągu ostatnich 10 dni występowania co najmniej jednego zdarzenia typu „błąd danych dotyczących ruchu", jak określono w załączniku 1C. W PRZECIWNYM WYPADKU, jeżeli w ostatnich 10 dniach występowania nie zarejestrowano żadnego takiego zdarzenia, ustawia się wartość zmiennej tp15638MotionDataError na FAŁSZ.	1 (PRAWDA) – wskazuje na wystąpienie zdarzenia typu „błąd danych dotyczących ruchu" w ciągu 10 ostatnich dni występowania	`tp15638motionDataError BOOLEAN,`

(1) Element danych RTM	(2) Czynność wykonywana przez VU		(3) Definicja danych w ASN.1
RTM7 **Konflikt ruchu pojazdu**	VU generuje wartość logiczną w odniesieniu do elementu danych RTM7. VU przypisuje wartość PRAWDA zmiennej tp15638vehicleMotionConflict w przypadku zarejestrowania w danych VU w ciągu ostatnich 10 dni występowania co najmniej jednego zdarzenia typu „konflikt ruchu pojazdu" (wartość '0A'H). W PRZECIWNYM WYPADKU, jeżeli w ostatnich 10 dniach występowania nie zarejestrowano żadnego zdarzenia, ustawia się wartość zmiennej tp15638vehicleMotionConflict na FAŁSZ.	1 (PRAWDA) – wskazuje na wystąpienie zdarzenia typu „konflikt ruchu pojazdu" w ciągu 10 ostatnich dni występowania	`tp15638vehicleMotionConflict` `BOOLEAN,`
RTM8 **Druga karta kierowcy**	VU generuje wartość logiczną w odniesieniu do elementu danych RTM8 na podstawie załącznika 1C („Dane dotyczące czynności kierowcy" w odniesieniu do ZAŁOGI i WSPÓŁKIEROWCY). W przypadku istnienia drugiej ważnej karty kierowcy VU ustawia wartość zmiennej na PRAWDA. W PRZECIWNYM WYPADKU, w przypadku braku drugiej ważnej karty kierowcy VU ustawia wartość zmiennej na FAŁSZ.	1 (PRAWDA) = wskazuje na włożenie drugiej karty kierowcy	`tp156382ndDriverCard` `BOOLEAN,`
RTM9 **Bieżące działania**	VU generuje wartość logiczną w odniesieniu do elementu danych RTM9. Jeżeli VU zarejestruje bieżącą czynność jako jakąkolwiek czynność inną niż „PROWADZENIE", jak określono w załączniku 1C, ustawia wartość zmiennej na PRAWDA. W PRZECIWNYM WYPADKU, jeżeli VU zarejestruje bieżącą czynność jako „PROWADZENIE", VU ustawia wartość zmiennej na FAŁSZ.	1 (PRAWDA) = inna wybrana czynność; 0 (FAŁSZ) = wybór czynności „prowadzenie".	`tp15638currentActivityDriving` `BOOLEAN`
RTM10 **Zamknięcie ostatniej sesji**	VU generuje wartość logiczną w odniesieniu do elementu danych RTM10. Jeżeli ostatnia sesja karty nie została prawidłowo zamknięta zgodnie z procedurą opisaną w załączniku 1C, VU ustawia wartość zmiennej na PRAWDA. W PRZECIWNYM WYPADKU, jeżeli ostatnia sesja karty została prawidłowo zamknięta, VU ustawia wartość zmiennej na FAŁSZ.	1 (PRAWDA) = sesja zamknięta nieprawidłowo; 0 (FAŁSZ) = sesja zamknięta prawidłowo.	`tp15638lastSessionClosed` `BOOLEAN`
RTM11 **Przerwa w zasilaniu**	VU generuje wartość całkowitą dla elementu danych RTM11. VU przypisuje zmiennej tp15638PowerSupplyInterruption wartość odpowiadającą „najdłuższej przerwie w zasilaniu" zgodnie z art. 9 rozporządzenia (UE) nr 165/2014 w odniesieniu do zdarzenia typu „przerwa w zasilaniu", jak określono w załączniku 1C. W PRZECIWNYM WYPADKU, jeżeli w ostatnich 10 dniach występowania nie zarejestrowano żadnego zdarzenia związanego z przerwą w zasilaniu, wartość liczby całkowitej ustawia się na 0.	— Liczba przerw w zasilaniu w ostatnich 10 dniach występowania	`tp15638powerSupplyInterruption` `INTEGER (0..127),`

(1) Element danych RTM	(2) Czynność wykonywana przez VU		(3) Definicja danych w ASN.1
RTM12 **Usterka czujnika**	VU generuje wartość w postaci liczby całkowitej w odniesieniu do elementu danych RTM12. VU przypisuje zmiennej sensorFault wartość: — 1 w przypadku zarejestrowania w ciągu ostatnich 10 dni zdarzenia typu '35'H związanego z usterką czujnika; — 2 w przypadku zarejestrowania w ciągu ostatnich 10 dni zdarzenia związanego z usterką odbiornika GNSS (wewnętrznego albo zewnętrznego, o wartości enum'51'H lub '52' H); — 3 w przypadku zarejestrowania w ciągu ostatnich 10 dni występowania zdarzenia typu '53'H związanego z błędem łączności z urządzeniem zewnętrznym GNSS; — 4 w przypadku zarejestrowania w ciągu ostatnich 10 dni zarówno usterki czujnika, jak i usterki odbiornika GNSS; — 5 w przypadku zarejestrowania w ciągu ostatnich 10 dni zarówno usterki czujnika, jak i błędów łączności z urządzeniem zewnętrznym GNSS; — 6 w przypadku zarejestrowania w ciągu ostatnich 10 dni zarówno usterki odbiornika GNSS, jak i błędu łączności z urządzeniem zewnętrznym GNSS; — 7 w przypadku zarejestrowania w ciągu ostatnich 10 dni występowania wszystkich trzech usterek czujnika. W PRZECIWNYM WYPADKU przypisuje wartość 0, jeżeli: w ciągu ostatnich 10 dni od wystąpienia nie zarejestrowano żadnych kolejnych zdarzeń	— usterka czujnika jeden oktet zgodnie ze słownikiem danych	`tp15638SensorFault INTEGER (0..255),`
RTM13 **Korekta czasu**	VU generuje wartość w postaci liczby całkowitej (timeReal z dodatku 1) dla elementu danych RTM13 na podstawie obecności danych dotyczących korekty czasu zdefiniowanych w załączniku 1C. VU przypisuje wartość czasu, w którym doszło do wystąpienia ostatniego zdarzenia polegającego na korekcie czasu danych. W PRZECIWNYM WYPADKU, jeżeli w danych VU nie stwierdzono wystąpienia żadnego zdarzenia typu „korekta czasu" zdefiniowanego w załączniku 1C, wartość ustala się na 0.	Czas ostatniej korekty czasu	`tp15638TimeAdjustment` `INTEGER(0..4294967295),`
RTM14 **Próba naruszenia zabezpieczenia**	VU generuje wartość w postaci liczby całkowitej (timeReal z dodatku 1) dla elementu danych RTM14 na podstawie wystąpienia zdarzenia typu „próba naruszenia zabezpieczenia" zdefiniowanego w załączniku 1C. VU ustala wartość czasu, w którym doszło do ostatniego zarejestrowanego przez VU zdarzenia związanego z próbą naruszenia zabezpieczenia. W PRZECIWNYM WYPADKU, jeżeli w danych VU nie stwierdzono wystąpienia żadnego zdarzenia typu „próba naruszenia zabezpieczenia" zdefiniowanego w załączniku 1C, wartość ustala się na 0x00FF.	Czas ostatniej próby naruszenia zabezpieczenia — Wartość domyślna = 0x00FF	`tp15638LatestBreachAttempt` `INTEGER(0..4294967295),`
RTM15 **Ostatnia kalibracja**	VU generuje wartość w postaci liczby całkowitej (timeReal z dodatku 1) dla elementu danych RTM15 na podstawie obecności danych dotyczących ostatniej kalibracji zdefiniowanych w załączniku 1C. VU ustala wartość czasu, w którym dokonano dwóch ostatnich kalibracji (RTM15 i RTM16) ustanowionych w VuCalibrationData zdefiniowanych w dodatku 1. VU ustala wartość RTM15 na timeReal zapisu ostatniej kalibracji.	Dane dotyczące czasu ostatniej kalibracji	`tp15638LastCalibrationData` `INTEGER(0..4294967295),`

(1) Element danych RTM	(2) Czynność wykonywana przez VU		(3) Definicja danych w ASN.1
RTM16 **Poprzednia kalibracja**	VU generuje wartość w postaci liczby całkowitej (timeReal z dodatku 1) dla elementu danych RTM16 z zapisu kalibracyjnego poprzedzającego zapis ostatniej kalibracji. W PRZECIWNYM WYPADKU, jeżeli poprzednia kalibracja nie miała miejsca, VU ustala wartość RTM16 na 0.	Dane dotyczące czasu poprzedniej kalibracji	`tp15638PrevCalibrationData` `INTEGER(0..4294967295),`
RTM17 **Data podłączenia tachografu**	Dla elementu danych RTM17 VU generuje wartość w postaci liczby całkowitej (timeReal z dodatku 1). VU ustala wartość czasu wstępnej instalacji VU. VU wyodrębnia te dane z VuCalibrationData (dodatek 1) znajdujących się w VuCalibrationRecords z CalibrationPurpose równym: '03'H	Data podłączenia tachografu	`tp15638DateTachoConnected` `INTEGER(0..4294967295),`
RTM18 **Prędkość bieżąca**	VU generuje wartość w postaci liczby całkowitej w odniesieniu do elementu danych RTM18. VU ustala wartość RTM16 na wartość ostatniej zarejestrowanej prędkości bieżącej w chwili dokonania ostatniej aktualizacji RtmData.	Ostatnia zarejestrowana prędkość bieżąca	`tp15638CurrentSpeed` `INTEGER (0..255),`
RTM19 **Znacznik czasu**	Dla elementu danych RTM19 VU generuje wartość w postaci liczby całkowitej (timeReal z dodatku 1). VU ustala wartość RTM19 na czas ostatniej aktualizacji RtmData.	Znacznik czasu aktualnego rekordu TachographPayload	`tp15638Timestamp` `INTEGER(0..4294967295),`

5.4.6 *Mechanizm przesyłania danych*

DSC_42 REDCR wysyła żądanie przekazania zdefiniowanych wcześniej danych ładunku po zakończeniu etapu inicjacji; następnie *DSRC-VU* przekazuje te dane w przydzielonym oknie. REDCR korzysta z polecenia GET w celu pobrania danych.

DSC_43 Wszystkie dane wymieniane w ramach DSRC koduje się zgodnie z PER (reguły upakowanego kodowania).

5.4.7 *Szczegółowy opis transakcji DSRC*

DSC_44 Inicjację przeprowadza się zgodnie z pkt DSC_44–DSC_48 oraz tabelami 14.4–14.9. Na etapie inicjacji REDCR rozpoczyna przesyłanie ramki zawierającej BST (tabelę usług sygnału) zgodnie z normami EN 12834 i EN 13372 pkt 6.2, 6.3, 6.4 i 7.1 z ustawieniami określonymi w tabeli 14.4 poniżej.

Tabela 14.4

Inicjacja – ustawienia ramki BST

Pole	Ustawienia
Identyfikator łącza	Adres emisji
Identyfikator sygnału	Zgodnie z normą EN 12834
Czas	Zgodnie z normą EN 12834
Profil	Brak rozszerzenia, należy zastosować 0 lub 1
Aplikacje obowiązkowe	Brak rozszerzenia, brak EID, brak parametru, AID = 2 Freight&Fleet
Aplikacje nieobowiązkowe	Brak
Lista profilów	Brak rozszerzenia, liczba profilów na liście = 0
Nagłówek fragmentacji	Brak fragmentacji
Ustawienia 2. warstwy	Polecenie PDU, polecenie interfejsu użytkownika

W tabeli 14.5 poniżej przedstawiono praktyczny przykład zastosowania ustawień określonych w tabeli 14.4 wraz z informacjami o kodowaniu bitowym.

Tabela 14.5

Inicjacja – przykładowa zawartość ramki BST

Oktet #	Atrybut/Pole	Bity w oktecie	Opis
1	FLAGA	0111 1110	Flaga początkowa
2	Identyfikator emisji	1111 1111	Adres emisji
3	Pole kontrolne MAC	1010 0000	Polecenie PDU
4	Pole kontrolne LLC	0000 0011	Polecenie interfejsu użytkownika
5	Nagłówek fragmentacji	1xxx x001	Brak fragmentacji

Oktet #	Atrybut/Pole	Bity w oktecie	Opis
6	BST	1000	Żądanie inicjacji
	SEQUENCE {		
	OPTION indicator BeaconID SEQUENCE { ManufacturerId INTEGER (0..65535)	0	Brak aplikacji nieobowiązkowych
		xxx	Identyfikator producenta
7		xxxx xxxx	
8		xxxx x	
	IndividualID INTEGER (0..134217727)	xxx	27-bitowy identyfikator dostępny dla producenta
9		xxxx xxxx	
10		xxxx xxxx	
11	}	xxxx xxxx	
12	Time INTEGER (0..4294967295)	xxxx xxxx	Czas rzeczywisty w 32-bitowym systemie UNIX
13		xxxx xxxx	
14		xxxx xxxx	
15		xxxx xxxx	
16	Profile NTEGER (0..127,...)	0000 0000	Brak rozszerzenia. Przykładowy profil 0
17	MandApplications SEQUENCE (SIZE (0..127,...)) OF {	0000 0001	Brak rozszerzenia, liczba aplikacji obowiązkowych = 1
18	SEQUENCE {		
	Wskaźnik WARIANTU	0	Brak EID
	Wskaźnik WARIANTU	0	Brak parametru
	AID DSRCApplicationEntityID } }	00 0010	Brak rozszerzenia. AID= 2 Freight&-Fleet

Oktet #	Atrybut/Pole	Bity w oktecie	Opis
19	ProfileList SEQUENCE (0..127,...) OF Profile }	0000 0000	Brak rozszerzenia, liczba profilów na liście = 0
20	FCS	xxxx xxxx	Sekwencja kontroli ramki
21		xxxx xxxx	
22	Flaga	0111 1110	Flaga końcowa

DSC_45 Po otrzymaniu BST *DSRC-VU* żąda przydzielenia okna prywatnego zgodnie z postanowieniami norm EN 12795 i EN 13372 pkt 7.1.1, bez określonych ustawień RTM. W tabeli 14.6 przedstawiono przykład kodowania bitowego.

Tabela 14.6

Inicjacja – zawartość ramki dotyczącej żądania przydzielenia okna prywatnego

Oktet #	Atrybut/Pole	Bity w oktecie	Opis
1	FLAGA	0111 1110	Flaga początkowa
2	Prywatny LID	xxxx xxxx	Adres łącza określonego DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	Pole kontrolne MAC	0110 0000	Żądanie przydzielenia okna prywatnego
7	FCS	xxxx xxxx	Sekwencja kontroli ramki
8		xxxx xxxx	
9	Flaga	0111 1110	Flaga końcowa

DSC_46 Następnie REDCR odpowiada, przydzielając okno prywatne zgodnie z postanowieniami norm EN 12795 i EN 13372 pkt 7.1.1, bez określonych ustawień RTM.

W tabeli 14.7 przedstawiono przykład kodowania bitowego.

Tabela 14.7

Inicjacja – zawartość ramki dotyczącej przydzielenia okna prywatnego

Oktet #	Atrybut/Pole	Bity w oktecie	Opis
1	FLAGA	0111 1110	Flaga początkowa
2	Prywatny LID	xxxx xxxx	Adres łącza określonego DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	Pole kontrolne MAC	0010 s000	Przydzielenie okna prywatnego
7	FCS	xxxx xxxx	Sekwencja kontroli ramki
8		xxxx xxxx	
9	Flaga	0111 1110	Flaga końcowa

DSC_47 Po otrzymaniu przydziału okna prywatnego *DSRC-VU* przesyła swoją VST (tabela usług pojazdu), jak określono w normach EN 12834 i EN 13372 pkt 6.2, 6.3, 6.4 i 7.1, z ustawieniami określonymi w tabeli 14.8 za pomocą przydzielonego okna transmisji.

Tabela 14.8

Inicjacja – ustawienia ramki VST

Pole	Ustawienia
Prywatny LID	Zgodnie z normą EN 12834
Parametry VST	Wypełnienie = 0; następnie dla każdej obsługiwanej aplikacji: EID występuje, parametr występuje, AID = 2; EID zgodny z wygenerowanym przez OBU
Parametr	Brak rozszerzenia, zawiera znacznik kontekstowy RTM
ObeConfiguration	Opcjonalne pole ObeStatus może być obecne, ale nie może być stosowane przez REDCR
Nagłówek fragmentacji	Brak fragmentacji
Ustawienia 2. warstwy	Polecenie PDU, polecenie interfejsu użytkownika

DSC_48 *DSRC-VU* obsługuje aplikację „Ładunek i flota" (Freight and Fleet) opatrzoną identyfikatorem aplikacji '2'. Inne identyfikatory aplikacji mogą być obsługiwane, ale nie mogą występować w tej VST, ponieważ BST wymaga wyłącznie AID=2. Pole „Aplikacje" zawiera wykaz wystąpień aplikacji obsługiwanych w ramach *DSRC-VU*. Dla każdego obsługiwanego wystąpienia aplikacji podaje się odniesienie do odpowiedniej normy w formie znacznika Rtm Context, który składa się z IDENTYFIKATORA OBIEKTU reprezentującego powiązaną normę, jej część (9 w przypadku RTM) oraz – w stosownych przypadkach – wersję, a także EID generowanego przez DSRC-VU i powiązanego z danym wystąpieniem aplikacji.

W tabeli 14.9 przedstawiono praktyczny przykład ustawień określonych w tabeli 14.8 wraz z informacjami o kodowaniu bitowym.

Tabela 14.9

Inicjacja – przykładowa zawartość ramki VST

Oktet #	Atrybut/Pole	Bity w oktecie	Opis
1	FLAGA	0111 1110	Flaga początkowa
2	Prywatny LID	xxxx xxxx	Adres łącza określonego DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	Pole kontrolne MAC	1100 0000	Polecenie PDU
7	Pole kontrolne LLC	0000 0011	Polecenie interfejsu użytkownika
8	Nagłówek fragmentacji	1xxx x001	Brak fragmentacji
9	VST SEQUENCE {	1001	Odpowiedź na inicjację
	Wypełnienie CIĄG BITÓW (ROZMIAR (4))	0000	Niewykorzystywane i ustawione na 0
10	Profil INTEGER (0..127,…) Aplikacje SEQUENCE OF {	0000 0000	Brak rozszerzenia. Przykładowy profil 0
11		0000 0001	Brak rozszerzenia, 1 aplikacja
12	SEQUENCE {		
	Wskaźnik WARIANTU	1	EID występuje
	Wskaźnik WARIANTU	1	Parametr występuje
	AID DSRCApplicationEntityID	00 0010	Brak rozszerzenia. AID= 2 Freight&-Fleet
13	EID Dsrc-EID	xxxx xxxx	Zdefiniowany przez OBU i identyfikujący wystąpienie aplikacji.

Oktet #	Atrybut/Pole	Bity w oktecie	Opis
14	Kontener parametru {	0000 0010	Brak rozszerzenia, wybór kontenera = 02, ciąg oktetowy
15		0000 1000	Brak rozszerzenia, długość znacznika kontekstowego RTM = 8
16	Rtm-ContextMark::= SEQUENCE { StandardIdentifier standardIdentifier	0000 0110	Identyfikator obiektu obsługiwanej normy, części i wersji. Przykład: ISO (1) norma (0) TARV (15638) część 9 (9) wersja 1 (1). Wartość pierwszego oktetu to 06H i stanowi identyfikator obiektu; drugi oktet to 06H, który stanowi jego długość. Kolejne 6 oktetów koduje przykładowy identyfikator obiektu Należy zauważyć, że tylko jeden element sekwencji jest obecny (pominięto opcjonalny element RtmCommProfile)
17		0000 0110	
18		0010 1000	
19		1000 0000	
20		1111 1010	
21		0001 0110	
22		0000 1001	
23		0000 0001	
24	ObeConfiguration Sequence { Wskaźnik WARIANTU	0	Brak ObeStatus
	EquipmentClass INTEGER (0..32767)	xxx xxxx	
25		xxxx xxxx	
26	ManufacturerId INTEGER (0..65535)	xxxx xxxx	Identyfikator producenta dla DSRC-VU opisany w rejestrze dotyczącym normy ISO 14816
27		xxxx xxxx	
28	FCS	xxxx xxxx	Sekwencja kontroli ramki
29		xxxx xxxx	
30	Flaga	0111 1110	Flaga końcowa

DCS_49 Następnie REDCR odczytuje dane, wydając polecenie GET, które odpowiada poleceniu GET zdefiniowanemu w normie EN 13372 pkt 6.2, 6.3, 6.4 i w normie EN 12834; ustawienia tego polecenia odpowiadają ustawieniom przedstawionym w tabeli 14.10.

Tabela 14.10

Przedstawienie – ustawienia ramki żądania GET

Pole	Ustawienia
Identyfikator źródła (IID)	Brak
Identyfikator łącza (LID)	Adres łącza określonego DSRC-VU
Tworzenie łańcuchów	Nie

Pole	Ustawienia
Identyfikator elementu (EID)	Jak określono w VST. Brak rozszerzenia
Poświadczenia dostępu	Nie
AttributeIdList	Brak rozszerzenia, 1 atrybut, AttributeID = 1 (RtmData)
Fragmentacja	Nie
Ustawienia 2. warstwy	Polecenie PDU, wysondowane polecenie ACn

W tabeli 14.11 przedstawiono przykład odczytu danych RTM.

Tabela 14.11

Przedstawienie – przykład ramki żądania GET

Oktet #	Atrybut/Pole	Bity w oktecie	Opis
1	FLAGA	0111 1110	Flaga początkowa
2	Prywatny LID	xxxx xxxx	Adres łącza określonego DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	Pole kontrolne MAC	1010 s000	Polecenie PDU
7	Pole kontrolne LLC	n111 0111	Wysondowane polecenie ACn, bit n
8	Nagłówek fragmentacji	1xxx x001	Brak fragmentacji
9	Get.request SEQUENCE {	0110	Żądanie Get
	Wskaźnik WARIANTU	0	Brak poświadczeń dostępu
	Wskaźnik WARIANTU	0	Brak IID
	Wskaźnik WARIANTU	1	Występuje AttributeIdList
	Wypełnienie CIĄG BITÓW (ROZMIAR (1))	0	Ustalono na 0.
10	EID INTEGER(0..127,…)	xxxx xxxx	EID wystąpienia aplikacji RTM, jak określono w VST. Brak rozszerzenia
11	AttributeIdList SEQUENCE OF { AttributeId }}	0000 0001	Brak rozszerzenia, liczba atrybutów = 1
12		0000 0001	AttributeId=1, RtmData. Brak rozszerzenia

Oktet #	Atrybut/Pole	Bity w oktecie	Opis
13	FCS	xxxx xxxx	Sekwencja kontroli ramki
14		xxxx xxxx	
15	Flaga	0111 1110	Flaga końcowa

DSC_50 Po otrzymaniu żądania GET *DSRC-VU* wysyła odpowiedź GET wraz z żądanymi danymi zgodnymi z odpowiedzią GET określonymi w normie EN 13372 pkt 6.2, 6.3, 6.4 i w normie EN 12834; ustawienia odpowiadają ustawieniom określonym w tabeli 14.12.

Tabela 14.12

Przedstawienie – ustawienia ramki odpowiedzi GET

Pole	Ustawienia
Identyfikator źródła (IID)	Brak
Identyfikator łącza (LID)	Zgodnie z normą EN 12834
Tworzenie łańcuchów	Nie
Identyfikator elementu (EID)	Jak określono w VST.
Poświadczenia dostępu	Nie
Fragmentacja	Nie
Ustawienia 2. warstwy	Odpowiedź PDU, dostępna odpowiedź i przyjęte polecenie, polecenie ACn

W tabeli 14.13 przedstawiono przykład odczytu danych RTM.

Tabela 14.13

Przedstawienie – przykładowa zawartość ramki odpowiedzi

Oktet #	Atrybut/Pole	Bity w oktecie	Opis
1	FLAGA	0111 1110	Flaga początkowa
2	Prywatny LID	xxxx xxxx	Adres łącza określonego DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	

Oktet #	Atrybut/Pole	Bity w oktecie	Opis
6	Pole kontrolne MAC	1101 0000	Odpowiedź PDU
7	Pole kontrolne LLC	n111 0111	Dostępna odpowiedź, bit n polecenia ACn
8	Pole stanu LLC	0000 0000	Dostępna odpowiedź i przyjęte polecenie
9	Nagłówek fragmentacji	1xxx x001	Brak fragmentacji
10	GET.response SEQUENCE {	0111	Odpowiedź na żądanie Get
	Wskaźnik WARIANTU	0	Brak IID
	Wskaźnik WARIANTU	1	Lista atrybutów występuje
	Wskaźnik WARIANTU	0	Status zwrotu nie występuje
	Wypełnienie CIĄG BITÓW (ROZMIAR (1))	0	Nieużywany
11	EID INTEGER(0..127,…)	xxxx xxxx	Odpowiedź z wystąpienia aplikacji RTM. Brak rozszerzenia
12	AttributeList SEQUENCE OF {	0000 0001	Brak rozszerzenia, liczba atrybutów = 1
13	Attributes SEQUENCE { AttributeId	0000 0001	Brak rozszerzenia, AttributeId=1 (RtmData)
14	AttributeValue CONTAINER {	0000 1010	Brak rozszerzenia, wybór kontenera = 1010.
15		kkkk kkkk	RtmData
16		kkkk kkkk	
17		kkkk kkkk	
…		…	
n	}}}}	kkkk kkkk	
n+1	FCS	xxxx xxxx	Sekwencja kontroli ramki
n+2		xxxx xxxx	
n+3	Flaga	0111 1110	Flaga końcowa

DSC_51 Następnie REDCR zamyka połączenie, wydając polecenie EVENT_REPORT, RELEASE zgodnie z normą EN 13372 pkt 6.2, 6.3, 6.4 i z normą 12834 pkt 7.3.8, bez określonych ustawień RTM. W tabeli 14.14 przedstawiono przykład kodowania bitowego polecenia RELEASE.

Tabela 14.14

Zakończenie. EVENT_REPORT Uwolnienie zawartości ramki

Oktet #	Atrybut/Pole	Bity w oktecie	Opis
1	FLAGA	0111 1110	Flaga początkowa
2	Prywatny LID	xxxx xxxx	Adres łącza określonego DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	Pole kontrolne MAC	1000 s000	Ramka zawiera polecenie LPDU
7	Pole kontrolne LLC	0000 0011	Polecenie interfejsu użytkownika
8	Nagłówek fragmentacji	1xxx x001	Brak fragmentacji
9	EVENT_REPORT.request SEQUENCE {	0010	EVENT_REPORT (Uwolnienie)
	Wskaźnik WARIANTU	0	Brak poświadczeń dostępu
	Wskaźnik WARIANTU	0	Parametr zdarzenia nie występuje
	Wskaźnik WARIANTU	0	Brak IID
	Tryb DANYCH LOGICZNYCH	0	Odpowiedź nieoczekiwana
10	EID INTEGER (0..127,…)	0000 0000	Brak rozszerzenia, EID = 0 (System)
11	EventType INTEGER (0..127,…) }	0000 0000	Typ zdarzenia 0 = Uwolnienie
12	FCS	xxxx xxxx	Sekwencja kontroli ramki
13		xxxx xxxx	
14	Flaga	0111 1110	Flaga końcowa

DSC_52 Nie oczekuje się, że *DSRC-VU* odpowie na polecenie RELEASE. Następnie łączność zostaje zamknięta.

5.4.8 *Opis transakcji testowej DSRC*

DSC_53 Pełne testy obejmujące zabezpieczanie danych muszą być przeprowadzane w sposób określony w dodatku 11 „Wspólne mechanizmy zabezpieczenia" przez upoważnione osoby, które mają dostęp do procedur zabezpieczenia, z zastosowaniem standardowych poleceń GET zdefiniowanych powyżej.

DSC_54 Testy przeprowadzane na zlecenie oraz testy w ramach przeglądów okresowych wiążące się z koniecznością odszyfrowania i zrozumienia treści zaszyfrowanych danych przeprowadza się zgodnie z postanowieniami dodatku 11 „Wspólne mechanizmy zabezpieczenia" oraz dodatku 9 „Homologacja typu – wykaz minimalnych wymaganych testów".

Test podstawowej łączności DSRC można jednak przeprowadzić za pomocą polecenia ECHO. Tego rodzaju testy mogą być przeprowadzane na zlecenie, w ramach przeglądów okresowych lub w inny sposób na żądanie właściwego organu kontrolnego lub zgodnie z wymogami określonymi w rozporządzeniu (UE) nr 165/2014 (zob. pkt 6 poniżej).

DSC_55 W celu przeprowadzenia tego podstawowego testu łączności REDCR wydaje polecenie ECHO w trakcie sesji, tj. po pomyślnym zakończeniu etapu inicjacji. Sekwencja czynności jest zatem zbliżona do sekwencji czynności związanych z zapytaniem:

— Etap 1 *REDCR* wysyła „tabelę usług sygnału" (BST), która zawiera identyfikatory aplikacji (AID) w wykazie obsługiwanych usług. W aplikacji RTM będzie to po prostu usługa z wartością AID = 2.

DSRC-VU oceni otrzymaną BST i jeżeli uzna, że BST żąda danych Freight&Fleet (AID = 2), *DSRC-VU* udzieli odpowiedzi. Jeżeli *REDCR* nie oferuje AID=2, DSRC-VU przerywa transakcję z *REDCR*.

— Krok 2 *DSRC-VU* wysyła żądanie przydzielenia okna prywatnego.

— Krok 3 REDCR przesyła przydział okna prywatnego.

— Krok 4 *DSRC-VU* używa przydzielonego okna prywatnego do wysłania swojej tabeli usług pojazdu (VST). Tego rodzaju VST zawiera wykaz wszystkich różnych wystąpień aplikacji obsługiwanych przez ten *DSRC-VU* w ramach AID=2. Poszczególne wystąpienia są identyfikowane za pomocą jednorazowych identyfikatorów elementu, z których każdy jest powiązany z wartością parametru określającą wystąpienie obsługiwanej aplikacji.

— Krok 5 Następnie *REDCR* analizuje oferowaną tabelę usług pojazdu i albo przerywa łączność (RELEASE), ponieważ nie jest zainteresowany niczym, co dana VST ma do zaoferowania (tj. otrzymuje VST od *DSRC-VU*, która nie jest RTM VU), albo – jeżeli otrzymuje odpowiednią tabelę usług pojazdu – uruchamia wystąpienie aplikacji.

— Krok 6 *REDCR* wydaje polecenie (ECHO) określonemu *DSRC-VU* i przypisuje okno prywatne.

— Krok 7 *DSRC-VU* korzysta z nowo przydzielonego okna prywatnego do wysłania ramki odpowiedzi ECHO.

W poniższych tabelach przedstawiono praktyczny przykład sesji wymiany ECHO.

DSC_56 Inicjację przeprowadza się zgodnie z pkt 5.4.7 (DSC_44–DSC_48) oraz tabelami 14.4–14.9.

DSC_57 Następnie REDCR wydaje polecenie ACTION, ECHO zgodnie z normą ISO 14906, zawierającą 100 oktetów danych i bez określonych ustawień RTM. W tabeli 14.15 przedstawiono zawartość ramki wysłanej przez REDCR.

Tabela 14.15

Przykładowa ramka żądania ACTION, ECHO

Oktet #	Atrybut/Pole	Bity w oktecie	Opis
1	FLAGA	0111 1110	Flaga początkowa
2	Prywatny LID	xxxx xxxx	Adres łącza określonego DSRC-VU
3		xxxx xxxx	

Oktet #	Atrybut/Pole	Bity w oktecie	Opis
4		xxxx xxxx	
5		xxxx xxxx	
6	Pole kontrolne MAC	1010 s000	Polecenie PDU
7	Pole kontrolne LLC	n111 0111	Wysondowane polecenie ACn, bit n
8	Nagłówek fragmentacji	1xxx x001	Brak fragmentacji
9	ACTION.request SEQUENCE {	0000	Żądanie działania (ECHO)
	Wskaźnik WARIANTU	0	Brak poświadczeń dostępu
	Wskaźnik WARIANTU	1	Parametr akcji występuje
	Wskaźnik WARIANTU	0	Brak IID
	Tryb BOOLEAN	1	Odpowiedź oczekiwana
10	EID INTEGER (0..127,…)	0000 0000	Brak rozszerzenia, EID = 0 (System)
11	ActionType INTEGER (0..127,…)	0000 1111	Brak rozszerzenia, typ działania: żądanie ECHO
12	ActionParameter CONTAINER {	0000 0010	Brak rozszerzenia, wybór kontenera = 2
13		0110 0100	Brak rozszerzenia. Długość ciągu = 100 oktetów
14		xxxx xxxx	Dane, które mają być powtórzone
…		…	
113	}}	xxxx xxxx	
11-46-14	FCS	xxxx xxxx	Sekwencja kontroli ramki
11-57-15		xxxx xxxx	
11-68-16	Flaga	0111 1110	Flaga końcowa

DSC_58 Po otrzymaniu żądania ECHO *DSRC-VU* wysyła odpowiedź ECHO o długości 100 oktetów danych, odzwierciedlając otrzymane polecenie, zgodnie z normą ISO 14906, bez określonych ustawień RTM. W tabeli 14.16 przedstawiono przykład szyfrowania na poziomie bitów.

Tabela 14.16

Przykładowa ramka żądania ACTION, ECHO

Oktet #	Atrybut/Pole	Bity w oktecie	Opis
1	FLAGA	0111 1110	Flaga początkowa
2	Prywatny LID	xxxx xxxx	Adres łącza określonego VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	Pole kontrolne MAC	1101 0000	Odpowiedź PDU
7	Pole kontrolne LLC	n111 0111	Polecenie ACn, bit n
8	Pole stanu LLC	0000 0000	Odpowiedź dostępna
9	Nagłówek fragmentacji	1xxx x001	Brak fragmentacji
10	ACTION.response SEQUENCE {	0001	Odpowiedź na DZIAŁANIE (ECHO)
	Wskaźnik WARIANTU	0	Brak IID
	Wskaźnik WARIANTU	1	Parametr odpowiedzi występuje
	Wskaźnik WARIANTU	0	Status zwrotu nie występuje
	Wypełnienie CIĄG BITÓW (ROZMIAR (1))	0	Nieużywany
11	EID INTEGER (0..127,…)	0000 0000	Brak rozszerzenia, EID = 0 (System)
12	KONTENER ResponseParameter {	0000 0010	Brak rozszerzenia, wybór kontenera = 2
13		0110 0100	Brak rozszerzenia. Długość ciągu = 100 oktetów
14		xxxx xxxx	Powtórzone dane
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Sekwencja kontroli ramki
115		xxxx xxxx	
116	Flaga	0111 1110	Flaga końcowa

5.5 **Wsparcie wdrażania dyrektywy 2015/71/WE**

5.5.1 *Informacje ogólne*

DSC_59 W celu wsparcia wdrażania dyrektywy 2015/719/WE w sprawie maksymalnych obciążeń i wymiarów pojazdów ciężarowych protokół transakcji służący do pobierania danych OWS za pośrednictwem połączenia interfejsu DSRC działającego na częstotliwości 5,8 GHz będzie taki sam jak protokół używany do przekazywania danych dotyczących zdalnego monitorowania tachografu (zob. 5.4.1) – jedyna różnica polega na tym, że identyfikator obiektu odnoszący się do normy TARV będzie odnosił się do części 20 normy ISO 15638 (TARV) dotyczącej systemów ważenia w pojeździe.

5.5.2 *Polecenia*

DSC_60 Polecenia stosowane w odniesieniu do transakcji OWS będą takie same jak polecenia stosowane w odniesieniu do transakcji RTM.

5.5.3 *Sekwencja polecenia zapytania*

DSC_61 Sekwencja polecenia zapytania w przypadku danych OWS będzie taka sama jak w przypadku danych dotyczących zdalnego monitorowania tachografu.

5.5.4 *Struktury danych*

DSC_62 Ładunek (dane OWS) składa się z połączenia:

1. danych EncryptedOwsPayload stanowiących zaszyfrowane dane OwsPayload określone w specyfikacji ASN.1 w sekcji 5.5.5. Metoda szyfrowania jest taka sama jak metoda przyjęta w odniesieniu do RtmData, które określono w dodatku 11;

2. DSRCSecurityData obliczone za pomocą tych samych algorytmów przyjętych w odniesieniu do RtmData, które określono w dodatku 11.

5.5.5 *Moduł ASN.1 w odniesieniu do transakcji DSRC dotyczącej OWS*

DSC_63. Zawarta w module ASN.1 definicja danych DSRC w ramach aplikacji RTM jest następująca:

```
   TarvRtm {iso(1) standard(0) 15638 part9(9) version1(1)}
   DEFINITIONS AUTOMATIC TAGS
   ::= BEGIN
   IMPORTS
   -- Imports data attributes and elements from EFC which are used for RTM
   LPN
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Imports function parameters from the EFC Application Interface Definition
   SetMMIRq
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Imports the L7 DSRCData module data from the EFC Application Interface Definition
   Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
   Attributes,
   BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
   EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
   ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
   FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};


   -- Definitions of the RTM functions:
   RTM-InitialiseComm-Request ::= BST
   RTM-InitialiseComm-Response::= VST
   RTM-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials ABSENT,iid
   ABSENT,  attrIdList})
   RTM-DataRetrieval-Response::= Get-Response {RtmContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
   RTM-TerminateComm::= Event-Report-Request {RtmContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
   eventType (0)})

   RTM-TestComm-Request::= Action-Request {RtmContainer} (WITH COMPONENTS {..., eid (0), actionType
   (15), accessCredentials ABSENT, iid ABSENT})

   RTM-TestComm-Response::= Action-Response {RtmContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
   (0), iid ABSENT})

   -- Definitions of the RTM attributes:
   RtmData ::= SEQUENCE {
        encryptedTachographPayload OCTET STRING (SIZE(67)) (CONSTRAINED BY { -- calculated encrypting
   TachographPayload as per Appendix 11 --}),
        DSRCSecurityData OCTET STRING
        }
   TachographPayload ::= SEQUENCE {
               tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
               tp15638SpeedingEvent            BOOLEAN,  -- 1= Irregularities in speed (see Annex 1C)
               tp15638DrivingWithoutValidCard  BOOLEAN,     -- 1= Invalid card usage (see Annex 1C)
               tp15638DriverCard               BOOLEAN,-- 0= Indicates a valid driver card  (see Annex 1C)
               tp15638CardInsertion            BOOLEAN, -- 1= Card insertion while driving (see Annex 1C)
               tp15638MotionDataError          BOOLEAN, -- 1= Motion data error (see Annex 1C)
               tp15638VehicleMotionConflict    BOOLEAN, -- 1= Motion conflict (see Annex 1C)
               tp156382ndDriverCard            BOOLEAN, -- 1= Second driver card inserted (see Annex 1C)
               tp15638CurrentActivityDriving   BOOLEAN, -- 1= other activity selected;
                                                          -- 0= driving selected
               tp15638LastSessionClosed        BOOLEAN, -- 1= improperly, 0= properly, closed
               tp15638PowerSupplyInterruption  INTEGER (0..127), -- Supply interrupts in the last 10 days
               tp15638SensorFault              INTEGER (0..255),-- eventFaultType as per data dictionary
   -- All subsequent time related types as defined in Annex 1C.
               tp15638TimeAdjustment           INTEGER(0..4294967295), -- Time of the last time adjustment
               tp15638LatestBreachAttempt      INTEGER(0..4294967295), -- Time of last breach attempt
               tp15638LastCalibrationData      INTEGER(0..4294967295), -- Time of last calibration data
               tp15638PrevCalibrationData      INTEGER(0..4294967295), -- Time of previous calibration data
               tp15638DateTachoConnected       INTEGER(0..4294967295), -- Date tachograph connected
               tp15638CurrentSpeed             INTEGER (0..255), -- Last current recorded speed
               tp15638Timestamp                INTEGER(0..4294967295) -- Timestamp of current record[2]
               }
Rtm-ContextMark ::= SEQUENCE {
  standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version

  RtmCommProfile          INTEGER {
                                C1 (1),
                                C2 (2)
                                } (0..255) DEFAULT 1
  }
RtmTransferAck ::= INTEGER {
                  Ok (1),
                  NoK (2)
                  } SIZE (1..255)
```

5.5.6 *Elementy OwsData, wykonywane czynności i definicje*

Elementy OwsData zdefiniowano, aby zapewnić wsparcie wdrażania dyrektywy 2015/719/WE w sprawie maksymalnych obciążeń i wymiarów pojazdów ciężarowych. Ich znaczenie jest następujące:

— recordedWeight oznacza całkowite zmierzone obciążenie pojazdu ciężarowego z dokładnością do 10 kg, jak określono w normie EN ISO 14906. Na przykład wartość 2 500 odpowiada obciążeniu wynoszącemu 25 ton;

— axlesConfiguration oznacza konfigurację pojazdu ciężarowego jako liczbę osi. Konfigurację określa się za pomocą maski bitów składającej się z 20 bitów (wersja rozszerzona z normy EN ISO 14906).

Maska bitów składająca się z 2 bitów odpowiada konfiguracji osi o następującym formacie:

— wartość 00B oznacza, że wartość jest „niedostępna", ponieważ pojazd nie posiada sprzętu do gromadzenia obciążenia na osi;

— wartość 01B oznacza, że oś nie występuje;

— wartość 10B oznacza, że oś występuje oraz że obciążenie zostało obliczone i zgromadzone oraz jest podane w polu axlesRecordedWeight;

— wartość 11B jest zarezerwowana do wykorzystania w przyszłości.

Ostatnie cztery bity są zarezerwowane do wykorzystania w przyszłości.

Liczba osi										
Liczba osi na ciągniku			Liczba osi na przyczepie							
00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	RFU (4 bity)

— axlesRecordedWeight oznacza określone obciążenie zarejestrowane dla każdej osi z dokładnością do 10 kg. W odniesieniu do każdej osi stosuje się dwa oktety. Na przykład wartość 150 oznacza obciążenie wynoszące 1 500 kg.

Inne rodzaje danych określono w pkt 5.4.5.

5.5.7 *Mechanizmy przesyłania danych*

DSC_64 Mechanizm przesyłania danych OWS pomiędzy interrogatorem a urządzeniem DSRC w pojeździe jest taki sam jak w przypadku danych RTM (zob. pkt 5.4.6).

DSC_65 Przesyłanie danych pomiędzy platformą zbierającą dane na temat maksymalnego obciążenia a urządzeniem DSRC w pojeździe opiera się na fizycznym połączeniu oraz interfejsach i protokole określonym w sekcji 5.6.

5.6 **Przesyłanie danych pomiędzy DSRC-VU a VU**

5.6.1 *Połączenie fizyczne i interfejsy*

DSC_66 Połączenie między *VU* a *DSRC-VU* może odbywać się za pomocą fizycznego okablowania lub łączności bezprzewodowej o krótkim zasięgu opartej na technologii Bluetooth v4.0 BLE.

DSC_67 Niezależnie od wybranego fizycznego połączenia i interfejsu następujące wymogi muszą być spełnione:

DSC_68 a) aby można było zawierać umowy z różnymi dostawcami na dostawę VU i DSRC-VU oraz w praktyce różnych serii DSRC-VU, połączenie między VU a DSRC-VU musi być otwartym połączeniem standardowym. VU musi być połączony z DSRC-VU za pomocą:

(i) zamontowanego na stałe kabla o długości co najmniej 2 metrów z wykorzystaniem łącznika Straight DIN 41612 H11 – 11-biegunowego zatwierdzonego wtyku z DSRC-VU w celu dopasowania do podobnego gniazda zatwierdzonego przez DIN/ISO z urządzenia VU albo

(ii) technologii Bluetooth Low Energy (BLE) albo

(iii) standardowego połączenia określonego w ISO 11898 lub SAE J1939,

DSC_69 b) definicja interfejsów i połączenia między VU i DSRC-VU musi obsługiwać polecenia protokołu aplikacji zdefiniowane w pkt 5.6.2 oraz

DSC_70 c) VU i DSRC-VU muszą obsługiwać operację przesyłania danych za pośrednictwem połączenia w odniesieniu do wydajności i zasilania.

5.6.2 *Protokół aplikacji*

DSC_71 Protokół aplikacji między urządzeniem do łączności na odległość w VU a DSRC-VU jest odpowiedzialny za okresowe przesyłanie danych dotyczących łączności na odległość z VU do DSRC.

DSC_72 Określono następujące polecenia główne:

1. Inicjacja łącza komunikacyjnego – żądanie
2. Inicjacja łącza komunikacyjnego – odpowiedź
3. Wysyłanie danych z identyfikatorem aplikacji RTM i ładunkiem określonym przez dane RTM
4. Potwierdzenie danych
5. Zamknięcie łącza komunikacyjnego – żądanie
6. Zamknięcie łącza komunikacyjnego – odpowiedź

DSC_73 W module ASN1.0 wcześniejsze polecenia można zdefiniować w następujący sposób:

```
Remote Communication DT Protocol DEFINITIONS ::= BEGIN

     RCDT-Communication Link Initialization - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

     RCDT-Communication Link Initialization - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer         BOOLEAN
     }

          RCDT- Send Data ::=
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER, RCDTData
          SignedTachographPayload
     }

          RCDT Data Acknowledgment ::
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER,
          answer         BOOLEAN
     }

          RCDT-Communication Link Termination - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

          RCDT-Communication Link Termination - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer         BOOLEAN
     }

End
```

DSC_74 Opis poleceń i parametrów jest następujący:

— `RCDT-Communication Link Initialization – Request` stosuje się w celu zainicjowania łącza komunikacyjnego. Polecenie jest wysyłane przez VU do DSRC-VU. VU ustanawia LinkIdentifier i przekazuje DSRC-VU w celu śledzenia określonego łącza komunikacyjnego.

(Uwaga: służy to obsłudze przyszłych łączy i innych aplikacji/modułów takich jak system ważenia w pojeździe);

— `RCDT-Communication Link Initialization – Response` jest stosowane przez DSRC-VU w celu dostarczenia odpowiedzi na żądanie zainicjowania łącza komunikacyjnego. Polecenie jest wysyłane przez DSRC-VU do VU. Polecenie przekazuje wynik inicjacji w formie odpowiedzi = 1 (Sukces) lub = 0 (Niepowodzenie).

DSC_75 Zainicjowanie łącza komunikacyjnego następuje dopiero po zainstalowaniu, kalibracji i uruchomieniu silnika/VU.

— `RCDT-Send Data` jest stosowane przez VU do przesyłania podpisanych RCDTData (tj. *danych dotyczących łączności na odległość*) do DSRC-VU. Dane będą wysyłane co 60 sekund. Parametr DataTransactionId identyfikuje określoną transmisję danych. LinkIdentifier wykorzystuje się także do upewnienia się, że łącze jest prawidłowe;

— `RCDT-Data Acknowledgment` jest wysyłane przez DSRC-VU w celu dostarczenia VU informacji zwrotnej dotyczącej odbioru danych z polecenia `RCDT-Send Data` określonego przez parametr DataTransactionId. Parametr odpowiedzi to 1 (Sukces) lub =0 (Niepowodzenie). Jeżeli VU otrzyma więcej niż trzy odpowiedzi równe 0 lub jeżeli VU nie otrzyma komunikatu RCDT Data Acknowledgment w odniesieniu do konkretnego wysłanego wcześniej polecenia z określonym DataTransactionId, VU wygeneruje i zarejestruje zdarzenie;

— `RCDT-Communication Link Termination request` komunikat jest wysyłane przez VU do DSRC-VU w celu zakończenia łącza w odniesieniu do konkretnego LinkIdentifier.

DSC_76 Po ponownym uruchomieniu DSRC-VU lub VU wszystkie istniejące łącza komunikacyjne należy usunąć, ponieważ w związku z nagłym zamknięciem VU mogą wystąpić „zawieszone" łącza.

— `RCDT-Communication Link Termination – Response` jest wysyłane przez DSRC-VU do VU w celu potwierdzenia żądania zakończenia łącza przez VU w odniesieniu do konkretnego LinkIdentifier.

5.7 **Obsługa błędów**

5.7.1 *Rejestrowanie i przekazywanie danych w DSRC-VU*

DSC_77 Już zabezpieczone *Dane* są przekazywane *DSRC-VU* za pomocą funkcji *VUSM*. *VUSM* sprawdza, czy dane zarejestrowane w *DSRC-VU* zostały poprawnie zarejestrowane. Rejestrowanie i zgłaszanie wszelkich błędów, jakie wystąpiły podczas przesyłania danych z *VU* do pamięci *DSRC-VU*, odbywa się przy użyciu zdarzenia typu EventFaultType z wartością enum ustawioną na '62'H Błąd łączności z urządzeniem do łączności na odległość wraz ze znacznikiem czasu.

DSC_78 *VU* zachowuje plik opatrzony unikatową nazwą, która jest łatwa do zidentyfikowania dla inspektorów w celu zarejestrowania „usterek łączności wewnętrznej VU".

DSC_79 Jeżeli VUPM próbuje uzyskać dane VU z modułu zabezpieczeń (w celu przejścia do urządzenia VU-DSRC), ale kończy się to niepowodzeniem, wówczas rejestruje takie niepowodzenie jako zdarzenie typu EventFaultType z wartością enum *'62'H Błąd łączności z urządzeniem do łączności na odległość* wraz ze znacznikiem czasu. Błąd związany z łącznością zostaje wykryty w przypadku nieotrzymania komunikatu `RCDT Data Acknowledgment` dotyczącego powiązanego (tj. z tym samym DataTransactionId w komunikatach `Send Data i Acknowledgment`) komunikatu `komunicatu RCDT Send Data` więcej niż trzy razy z rzędu.

5.7.2 *Błędy łączności bezprzewodowej*

DSC_80 Obsługa błędów związanych z łącznością jest zgodna z powiązanymi normami dotyczącymi DSRC, mianowicie EN 300 674-1, EN 12253, EN 12795, EN 12834 i odpowiednimi parametrami normy EN 13372.

5.7.2.1 *Błędy szyfrowania i błędy podpisu*

DSC_81 Błędy szyfrowania i podpisu obsługuje się zgodnie z dodatkiem 11 „Wspólne mechanizmy zabezpieczenia", przy czym błędy te nie występują w żadnych komunikatach o błędzie związanych z przesyłaniem danych DSRC.

5.7.2.2 *Rejestrowanie błędów*

Urządzenie DSRC umożliwia dynamiczną łączność bezprzewodową w środowisku z niepewnymi warunkami atmosferycznymi i zakłóceniami, zwłaszcza w przypadku kombinacji „przenośny REDCR" i „pojazd w ruchu" występujących w tej aplikacji. Konieczne jest zatem ustalenie różnicy między „niepowodzeniem odczytu" a „błędem". Podczas transakcji zachodzącej przez interfejs bezprzewodowy niepowodzenie odczytu jest zjawiskiem powszechnym, a jego skutkiem jest zwykle ponowienie próby, tj. reemisja BST i ponowna próba sekwencji, które w większości przypadków doprowadzą do skutecznego nawiązania łączności i przesłania danych, chyba że docelowy pojazd wyjedzie poza zasięg urządzenia w czasie wymaganym do przeprowadzenia ponownej transmisji. (Przypadek „skutecznego odczytu" może obejmować kilka prób i ponowień).

Niepowodzenie odczytu może być spowodowane niewłaściwym sparowaniem anteny (błąd „celowania"); faktem, że jedna z anten jest zasłonięta – może to być celowe, ale może być też spowodowane fizyczną obecnością innego pojazdu; zakłóceniami radiowymi, szczególnie w systemie łączności bezprzewodowej działającym na częstotliwości około 5,8 GHz lub w innych systemach publicznej łączności bezprzewodowej lub może być spowodowane zakłóceniem radarowym lub trudnymi warunkami atmosferycznymi (np. w trakcie burzy); lub po prostu faktem, że pojazd wyjechał poza obszar objęty zasięgiem łączności DSRC. Poszczególnych przypadków niepowodzenia odczytu, ze względu na ich charakter, nie można zarejestrować po prostu dlatego, że nie doszło do nawiązania łączności.

Jeżeli przedstawiciel właściwego organu kontrolnego wybiera pojazd i podejmuje próbę skierowania zapytania do jego *DSRC-VU*, jednak nie dochodzi do skutecznego przesłania danych, usterka taka mogła nastąpić w wyniku celowego manipulowania, w związku z czym przedstawiciel właściwego organu kontrolnego potrzebuje środka, aby móc wprowadzić usterkę do rejestru i ostrzec współpracowników znajdujących się na dalszym etapie łańcucha o możliwym naruszeniu. Współpracownicy mogą wówczas zatrzymać pojazd i przeprowadzić kontrolę fizyczną. W związku z tym, że nie nawiązano łączności, DSRC-VU nie może jednak dostarczyć danych dotyczących usterki. Przekazywanie tego rodzaju sprawozdań powinno być zatem funkcją projektu urządzenia REDCR.

„Niepowodzenie odczytu" różni się pod względem technicznym od „błędu". W tym kontekście „błąd" oznacza pozyskanie błędnej wartości.

Dane przesłane do *DSRC-VU* są dostarczane w postaci już zabezpieczonej, dlatego muszą zostać zweryfikowane przez dostawcę danych (zob. pkt 5.4).

Dane przesłane następnie przez interfejs radiowy są sprawdzane w ramach cyklicznej kontroli nadmiarowej na poziomie łączności. Jeżeli dane zostaną zatwierdzone w ramach CRC, oznacza to, że są poprawne. Jeżeli dane nie zostaną zatwierdzone w ramach CRC, oznacza to retransmisję danych. Prawdopodobieństwo, że niepoprawne dane pomyślnie przejdą CRC, jest statystycznie na tyle znikome, że można je pominąć.

Jeżeli dane nie zostaną zatwierdzone w ramach CRC i nie ma czasu na retransmisję i otrzymanie poprawnych danych, wówczas rezultatem nie będzie błąd, lecz wystąpienie określonego typu niepowodzenia odczytu.

Jedyne znaczące dane na temat „usterki", które można zarejestrować, dotyczą liczby udanych inicjacji transakcji, które z kolei nie skutkują skutecznym przesłaniem danych do REDCR.

DSC_82 REDCR rejestruje zatem z sygnaturą czasową liczbę przypadków, gdy faza „inicjowania" zapytania DSRC przebiegła pomyślnie, ale transakcja zakończyła się, zanim REDCR pomyślnie pobrał *Dane*. Dane te są udostępniane przedstawicielowi właściwego organu kontrolnego i przechowywane w pamięci urządzenia REDCR. Środkiem pozwalającym na osiągnięcie tego celu jest kwestia projektu produktu lub specyfikacja właściwego organu kontrolnego.

Jedyne znaczące dane na temat „błędów", które można zarejestrować, dotyczą liczby przypadków, gdy REDCR nie udało się deszyfrować otrzymanych *Danych*. Należy jednak zauważyć, że będzie to dotyczyło wyłącznie wydajności oprogramowania REDCR. Dane można technicznie deszyfrować, ale będą pozbawione sensu pod względem semantycznym.

DSC_83 *REDCR* rejestruje zatem z sygnaturą czasową liczbę podjętych prób deszyfrowania danych otrzymanych przez interfejs DSRC, które zakończyły się niepowodzeniem.

6 TESTY PRZEPROWADZANE PRZY ODDANIU DO EKSPLOATACJI ORAZ TESTY W RAMACH PRZEGLĄDÓW OKRESOWYCH FUNKCJI ŁĄCZNOŚCI NA ODLEGŁOŚĆ

6.1 **Uwagi ogólne**

DSC_84 Przewiduje się dwa rodzaje testów w odniesieniu do funkcji łączności na odległość:

1) test ECHO w celu zatwierdzania kanału łączności *bezprzewodowej DSRC-REDCR >>-:-<DSRC-VU;*
2) test bezpieczeństwa typu *end-to-end* przeprowadzany w celu zapewnienia, aby karta warsztatowa była w stanie uzyskać dostęp do zaszyfrowanych i podpisanych danych utworzonych przez VU i przesyłanych za pośrednictwem kanału komunikacji bezprzewodowej.

6.2 **ECHO**

Niniejsza klauzula zawiera postanowienia, które mają służyć wyłącznie sprawdzeniu, czy połączenie *DSRC-REDCR >>-:-<DSRC-VU* jest aktywne.

Celem polecenia ECHO jest umożliwienie warsztatom lub placówkom przeprowadzających testy na potrzeby homologacji typu zbadania, czy połączenie DSRC działa bez konieczności dostępu do poświadczeń zabezpieczenia; Urządzenie testera musi być jedynie w stanie zainicjować łączność DSRC (wysłanie BST z AID=2), a następnie wysłać polecenie ECHO i – zakładając, że DSRC pracuje – otrzymać odpowiedź ECHO. Więcej szczegółowych informacji można znaleźć w pkt 5.4.8. Zakładając, że otrzyma tę odpowiedź prawidłowo, łącze DSRC (*DSRC-REDCR >>-:-<DSRC-VU*) można zatwierdzić jako funkcjonujące poprawnie.

6.3 **Testy mające na celu zatwierdzanie treści zabezpieczonych danych**

DSC_85 Tego rodzaju test wykonuje się w celu zatwierdzenia bezpiecznych przepływów danych typu end-to-end. Do przeprowadzenia takiego testu niezbędny jest czytnik testowy DSRC. Czytnik testowy DSRC wykonuje te same funkcje i jest wdrażany z tą samą specyfikacją co czytnik wykorzystywany przez przedstawiciela organów ścigania z taką różnicą, że to karta warsztatowa jest wykorzystywana do uwierzytelniania użytkownika czytnika testowego DSRC, a nie karta kontrolna. Test można przeprowadzić po początkowej aktywacji tachografu inteligentnego lub pod koniec procedury kalibracji. Po aktywacji przyrząd rejestrujący generuje zabezpieczone dane dotyczące wczesnego wykrywania i przekazuje je do DSRC-VU.

DSC_86 Pracownicy warsztatu muszą umieścić czytnik testowy DSRC w odległości od 2 do 10 m od przodu pojazdu.

DSC_87 Następnie pracownicy warsztatu włożą kartę warsztatową do czytnika testowego DSRC w celu przekazania przyrządowi rejestrującemu zapytania o przekazanie danych dotyczących wczesnego wykrywania. Po pomyślnym zapytaniu pracownicy warsztatu uzyskają dostęp do otrzymanych danych w celu upewnienia się, że zostały one pomyślnie zatwierdzone pod względem integralności i deszyfrowane.

Dodatek 15

MIGRACJA: ZARZĄDZANIE WSPÓŁISTNIENIEM GENERACJI URZĄDZEŃ

SPIS TREŚCI

1. DEFINICJE

Do celów niniejszego dodatku stosuje się następujące definicje:

system tachografu inteligentnego: zgodnie z definicją zawartą w niniejszym załączniku (rozdział 1: definicja bbb));

system tachografu pierwszej generacji: zgodnie z definicją zawartą w niniejszym rozporządzeniu (art. 2: definicja 1));

system tachografu drugiej generacji: zgodnie z definicją zawartą w niniejszym rozporządzeniu (art. 2: definicja 7));

data wprowadzenia: zgodnie z definicją zawartą w niniejszym załączniku (rozdział 1: definicja ccc));

inteligentne urządzenie dedykowane (IDE): urządzenie służące do przeprowadzania operacji pobierania danych, zgodnie z definicją zawartą w dodatku 7 do niniejszego załącznika.

2. PRZEPISY OGÓLNE

2.1. Informacje ogólne na temat przejścia

Preambuła do niniejszego załącznika zawiera informacje ogólne na temat przejścia od stosowania systemów tachografów pierwszej generacji do stosowania systemów tachografów drugiej generacji.

W uzupełnieniu postanowień niniejszej preambuły:

— czujniki ruchu pierwszej generacji nie będą interoperacyjne z przyrządami rejestrującymi drugiej generacji;

— instalacja czujników ruchu drugiej generacji rozpocznie się w tym samym czasie co instalacja przyrządów rejestrujących drugiej generacji;

— urządzenia do pobierania i kalibracji danych będą musiały ewoluować, aby mogły obsługiwać urządzenia rejestrujące i karty do tachografu obu generacji.

2.2. **Interoperacyjność między VU a kartami**

Przyjmuje się, że karty do tachografu pierwszej generacji są interoperacyjne z przyrządami rejestrującymi pierwszej generacji (zgodnie z załącznikiem 1B do niniejszego rozporządzenia), natomiast karty do tachografu drugiej generacji są interoperacyjne z przyrządami rejestrującymi drugiej generacji (zgodnie z załącznikiem 1C do niniejszego rozporządzenia). Ponadto zastosowanie mają przedstawione poniżej wymogi.

MIG_001 Z wyjątkiem treści wymogów MIG_004 i MIG_005 karty do tachografu pierwszej generacji mogą być nadal używane w przyrządach rejestrujących drugiej generacji do upływu daty ich ważności. Właściciele takich kart mogą jednak wystąpić z wnioskiem o ich wymianę na karty do tachografu drugiej generacji, jak tylko te drugie karty staną się dostępne.

MIG_002 Przyrządy rejestrujące drugiej generacji muszą być w stanie obsługiwać każdą włożoną ważną kartę kierowcy, kartę kontrolną oraz kartę firmową pierwszej generacji.

MIG_003 Warsztaty mogą raz na zawsze pozbawić przyrządy rejestrującej tej funkcji, tak aby karty do tachografu pierwszej generacji nie mogły być już dłużej akceptowane. Może to nastąpić dopiero po wszczęciu przez Komisję Europejską stosownej procedury, w ramach której zwróci się ona do warsztatów o podjęcie takich działań, np. w ramach każdego przeglądu okresowego tachografu.

MIG_004 Przyrządy rejestrujące drugiej generacji muszą być w stanie obsługiwać wyłącznie karty warsztatowe drugiej generacji.

MIG_005 Do celów określania trybu pracy przyrządy rejestrujące drugiej generacji rozpoznają wyłącznie typy włożonych ważnych kart, bez względu na ich generację.

MIG_006 Każda ważna karta do tachografu drugiej generacji musi umożliwiać jej zastosowanie w przyrządach rejestrujących pierwszej generacji w dokładnie taki sam sposób jak karty do tachografu pierwszej generacji tego samego typu.

2.3. **Interoperacyjność między VU a czujnikami ruchu**

Przyjmuje się, że czujniki ruchu pierwszej generacji są interoperacyjne z przyrządami rejestrującymi pierwszej generacji, natomiast czujniki ruchu drugiej generacji są interoperacyjne z przyrządami rejestrującymi drugiej generacji. Ponadto zastosowanie mają przedstawione poniżej wymogi.

MIG_007 Przyrządów rejestrujących drugiej generacji nie będzie można parować ani używać z czujnikami ruchu pierwszej generacji.

MIG_008 Czujniki ruchu drugiej generacji można parować i używać wyłącznie z przyrządami rejestrującymi drugiej generacji lub z obiema generacjami przyrządów rejestrujących.

2.4. **Interoperacyjność między przyrządami rejestrującymi, kartami do tachografu i urządzeniami służącymi do pobierania danych**

MIG_009 Urządzenia służące do pobierania danych mogą być używane tylko z jedną generacją przyrządów rejestrujących i kart do tachografu bądź z obiema generacjami.

2.4.1 *Bezpośrednie pobieranie danych z karty przez inteligentne urządzenia dedykowane*

MIG_010 Inteligentne urządzenia dedykowane pobierają dane z kart do tachografu danej generacji włożonych do ich czytników kart z zastosowaniem mechanizmów zabezpieczenia i protokołu pobierania danych tej generacji, a pobierane dane mają format zdefiniowany dla danej generacji.

MIG_011 Aby organy kontrolne spoza UE mogły kontrolować kierowców, należy umożliwić pobieranie danych z kart kierowców (i kart warsztatowych) drugiej generacji w dokładnie taki sam sposób, w jaki pobierane są dane z kart kierowców (i kart warsztatowych) pierwszej generacji. Tego rodzaju pobieranie obejmuje:

— niepodpisane pliki elementarne `IC` i `ICC`,

— niepodpisane pliki elementarne (pierwszej generacji) `Card_Certificate` i `CA_Certificate`,

— pliki elementarne zawierające inne dane aplikacyjne (w pliku katalogowym TACHO) żądane przez protokół pobierania danych z kart pierwszej generacji. Informacje takie są zabezpieczone podpisem cyfrowym zgodnie z mechanizmami zabezpieczenia pierwszej generacji.

Tego rodzaju pobieranie nie może obejmować plików elementarnych zawierających dane aplikacyjne istniejących wyłącznie w kartach kierowców (i kartach warsztatowych) drugiej generacji (pliki elementarne zawierające dane aplikacyjne w pliku katalogowym TACHO_G2).

2.4.2 *Pobieranie danych z karty za pomocą przyrządu rejestrującego*

MIG_012 Dane z karty drugiej generacji włożonej do przyrządu rejestrującego pierwszej generacji są pobierane za pomocą protokołu pobierania danych pierwszej generacji. Karta taka odpowiada na polecenia przyrządu rejestrującego w dokładnie taki sam sposób jak karta pierwszej generacji, a pobierane dane mają taki sam format jak dane pobierane z karty pierwszej generacji.

MIG_013 Dane z karty pierwszej generacji włożonej do przyrządu rejestrującego drugiej generacji są pobierane za pomocą protokołu pobierania danych określonego w dodatku 7 do niniejszego załącznika. Przyrząd rejestrujący wysyła polecenia do karty w dokładnie taki sam sposób jak przyrząd rejestrujący pierwszej generacji, a pobierane dane mają format określony w odniesieniu do kart pierwszej generacji.

2.4.3 *Pobieranie danych z przyrządów rejestrujących*

MIG_014 Dane z przyrządów rejestrujących drugiej generacji są pobierane z zastosowaniem mechanizmów zabezpieczenia drugiej generacji i protokołu pobierania danych określonego w dodatku 7 do niniejszego załącznika.

MIG_015 Aby organy kontrolne spoza UE mogły kontrolować kierowców oraz aby warsztaty spoza UE mogły pobierać dane z przyrządów rejestrujących, opcjonalnie można również umożliwić pobieranie danych z przyrządów rejestrujących drugiej generacji z zastosowaniem mechanizmów zabezpieczenia pierwszej generacji oraz protokołu pobierania danych pierwszej generacji. Pobierane dane mają taki sam format jak dane pobierane z przyrządu rejestrującego pierwszej generacji. Funkcję tę można wybrać za pomocą poleceń w menu.

2.5. **Interoperacyjność między VU a urządzeniami do kalibracji**

MIG_016 Urządzenia do kalibracji muszą być w stanie przeprowadzać kalibrację tachografów każdej generacji, z zastosowaniem protokołu kalibracyjnego danej generacji. Urządzenia do kalibracji mogą być używane tylko z jedną generacją tachografów bądź z obiema generacjami.

3. GŁÓWNE DZIAŁANIA W OKRESIE POPRZEDZAJĄCYM DATĘ WPROWADZENIA

MIG_017 Klucze testowe i certyfikaty muszą zostać udostępnione producentom najpóźniej **30 miesięcy** przed datą wprowadzenia.

MIG_018 Badania interoperacyjności muszą być gotowe do rozpoczęcia na wniosek producentów najpóźniej **15 miesięcy** przed datą wprowadzenia.

MIG_019 Oficjalne klucze i certyfikaty muszą zostać udostępnione producentom najpóźniej **12 miesięcy** przed datą wprowadzenia.

MIG_020 Państwa członkowskie muszą być w stanie rozpocząć wydawanie kart warsztatowych drugiej generacji najpóźniej **3 miesiące** przed datą wprowadzenia.

MIG_021 Państwa członkowskie muszą być w stanie rozpocząć wydawanie wszystkich typów kart do tachografu drugiej generacji najpóźniej **1 miesiąc** przed datą wprowadzenia.

4. PRZEPISY DOTYCZĄCE OKRESU PO DACIE WPROWADZENIA

MIG_022 Po upływie daty wprowadzenia państwa członkowskie wydają wyłącznie karty do tachografu drugiej generacji.

MIG_023 Producenci przyrządów rejestrujących / czujników ruchu mogą produkować przyrząd rejestrujące / czujniki ruchu pierwszej generacji, dopóki są one wykorzystywane w danym obszarze, tak aby była możliwa wymiana nieprawidłowo działających elementów składowych.

MIG_024 Producenci przyrządów rejestrujących / czujników ruchu mogą ubiegać się o utrzymanie homologacji typu przyrządów rejestrujących / czujników ruchu pierwszej generacji, które mają już homologację typu, oraz uzyskać zgodę na takie utrzymanie.

Dodatek 16.

ADAPTER DO POJAZDÓW KATEGORII M1 I N1

SPIS TREŚCI

1. SKRÓTY I DOKUMENTY REFERENCYJNE

1.1. **Skróty**

TBD Do ustalenia

VU Przyrząd rejestrujący

1.2. **Normy referencyjne**

ISO 16844-3 Pojazdy drogowe – Tachografy – Część 3: Podłączenie czujnika ruchu

2. OGÓLNA CHARAKTERYSTYKA I FUNKCJE ADAPTERA

2.1. **Ogólny opis adaptera**

ADA_001 Adapter dostarcza podłączonemu do niego VU (przyrządowi rejestrującemu) w sposób pewny i ciągły dane o ruchu pojazdu, odwzorowujące jego prędkość i przebytą drogę.

Adapter przeznaczony jest wyłącznie do pojazdów, które muszą być wyposażone w urządzenie rejestrujące zgodnie z niniejszym rozporządzeniem.

Instaluje się go i używa wyłącznie w pojazdach określonych w definicji yy) „adapter" w załączniku IC, w których z mechanicznego punktu widzenia niemożliwy jest montaż stosowanych czujników ruchu innego rodzaju, pod innym względem zgodnych z wymaganiami przedstawionymi w niniejszym załączniku i w dodatkach 1–16 do niniejszego załącznika.

Adapter nie może być mechanicznie sprzężony z ruchomą częścią pojazdu, lecz podłącza się go do impulsów prędkości/przebytej drogi, które są generowane przez zintegrowane czujniki lub alternatywne interfejsy.

ADA_002 Czujnik ruchu posiadający homologację typu (zgodnie z przepisami niniejszego załącznika IC sekcja 8 – Homologacja typu dla urządzenia rejestrującego i kart do tachografów) umieszczony jest w obudowie adaptera, gdzie znajduje się również przetwornik przekazujący odbierane impulsy do wbudowanego czujnika ruchu. Sam wbudowany czujnik ruchu jest podłączony do VU w taki sposób, aby sprzężenie między VU a adapterem było zgodne z wymaganiami ISO16844-3.

2.2. **Funkcje**

ADA_003 Adapter realizuje następujące funkcje:

— odbiór i adaptacja wejściowych impulsów pomiaru prędkości;

— przekazywanie odbieranych impulsów do wbudowanego czujnika ruchu;

— wszystkie funkcje wbudowanego czujnika ruchu przekazują w sposób pewny dane o ruchu pojazdu do VU.

2.3. **Zabezpieczenie**

ADA_004 Adapter nie musi posiadać certyfikacji bezpieczeństwa zgodnie z ogólnym celem zabezpieczenia czujnika ruchu określonym w dodatku 10 do niniejszego załącznika. Zastosowanie mają natomiast wymagania dotyczące zabezpieczenia określone w sekcji 4.4 niniejszego dodatku.

3. WYMAGANIA DOTYCZĄCE URZĄDZEŃ REJESTRUJĄCYCH W PRZYPADKU ZAMONTOWANIA ADAPTERA

Wymagania zawarte w kolejnych rozdziałach wskazują sposób, w jaki należy rozumieć wymagania niniejszego załącznika w przypadku zastosowania adaptera. W nawiasach podano odpowiednie numery poszczególnych wymagań załącznika IC.

ADA_005 Urządzenie rejestrujące każdego pojazdu wyposażonego w adapter musi być zgodne ze wszystkimi przepisami niniejszego załącznika, chyba że w niniejszym dodatku przewidziano inaczej.

ADA_006 W przypadku zainstalowania adaptera, na urządzenie rejestrujące składają się przewody, adapter (wraz z czujnikiem ruchu) oraz VU [01].

ADA_007 Przepisy regulujące wykrywanie zdarzeń lub usterek urządzenia rejestrującego otrzymują brzmienie:

— zdarzenie „przerwa w zasilaniu" jest wyzwalane przez VU, o ile nie jest on w trybie kalibracyjnym, w przypadku każdej przerwy w zasilaniu wbudowanego czujnika ruchu przekraczającej 200 milisekund [79];

— zdarzenie „błąd danych dotyczących ruchu" jest wyzwalane przez UV w przypadku przerwy w normalnym strumieniu danych między wbudowanym czujnikiem ruchu a VU lub w przypadku błędu spójności lub autentyczności danych, który występuje podczas wymiany danych między wbudowanym czujnikiem ruchu a VU [83];

— zdarzenie „próba naruszenia zabezpieczenia" jest wyzwalane przez VU w przypadku każdego zdarzenia mającego wpływ na zabezpieczenie wbudowanego czujnika ruchu, o ile nie jest on w trybie kalibracyjnym [85];

— usterka „urządzenie rejestrujące" jest wyzwalana przez VU, o ile nie jest on w trybie kalibracyjnym, w przypadku każdej usterki wbudowanego czujnika ruchu [88].

ADA_008 Usterki adaptera wykrywalne przez urządzenie rejestrujące to usterki związane z wbudowanym czujnikiem ruchu [88].

ADA_009 Funkcja kalibracji VU pozwala na automatyczne sparowanie wbudowanego czujnika ruchu z VU [202, 204].

4. WYMAGANIA KONSTRUKCYJNE I FUNKCJONALNE W STOSUNKU DO ADAPTERA

4.1. **Odbiór i przetwarzanie wejściowych impulsów prędkości**

ADA_011 Interfejs wejściowy adaptera odbiera impulsy o częstotliwości odwzorowującej prędkość i przebytą drogę. Własności elektryczne impulsów wejściowych: *do ustalenia przez producenta*. Prawidłowe sprzężenie wejścia adaptera z pojazdem umożliwiają w stosownych przypadkach regulacje, których może dokonać wyłącznie producent adaptera lub zatwierdzony warsztat montujący adapter.

ADA_012 Interfejs wejściowy adaptera musi w stosownych przypadkach mnożyć lub dzielić częstotliwość impulsów wejściowych prędkości przez stałą wartość, aby dostosować sygnał do zakresu współczynnika k zdefiniowanego w niniejszym załączniku (4 000 do 25 000 impulsów/km). Wartość stałej może zaprogramować wyłącznie producent adaptera lub zatwierdzony warsztat instalujący adapter.

4.2. **Przekazywanie odbieranych impulsów do wbudowanego czujnika ruchu**

ADA_013 Impulsy wejściowe, poddane ewentualnej adaptacji w sposób opisany powyżej, przekazywane są do wbudowanego czujnika ruchu w taki sposób, że każdy wejściowy impuls wykrywany jest przez czujnik ruchu.

4.3. **Wbudowany czujnik ruchu**

ADA_014 Wbudowany czujnik ruchu stymulowany jest przez przekazywane impulsy, co pozwala mu na wytwarzanie danych o ruchu, dokładnie odwzorowujących ruch pojazdu w taki sposób, jakby był on mechanicznie sprzężony z ruchomą częścią pojazdu.

ADA_015 VU wykorzystuje dane identyfikacyjne wbudowanego czujnika ruchu do identyfikacji adaptera [95].

ADA_016 Dane instalacyjne przechowywane we wbudowanym czujniku ruchu uważa się za dane instalacyjne adaptera [122].

4.4. **Wymogi bezpieczeństwa**

ADA_017 Obudowa adaptera musi być wykonana w sposób uniemożliwiający jej otwarcie. Musi być zaplombowana, by łatwo można było wykryć próby fizycznej ingerencji (np. w drodze oględzin, zob. ADA_035). Plomby muszą spełniać te same wymogi co plomby czujników ruchu [398–406].

ADA_018 Należy wykluczyć możliwość usunięcia wbudowanego czujnika ruchu z adaptera bez naruszania plomb założonych na obudowę adaptera lub uszkodzenia plomb między czujnikiem a obudową adaptera (zob. ADA_034).

ADA_019 Konstrukcja adaptera musi być taka, by dane o ruchu mogły być przetwarzane i odbierane tylko z wejścia adaptera.

4.5. **Parametry pracy**

ADA_020 Adapter musi realizować wszystkie funkcje w zakresie temperatur określonym przez producenta.

ADA_021 Adapter musi realizować wszystkie funkcje w zakresie wilgotności od 10 % do 90 % [214].

ADA_022 Adapter musi być zabezpieczony przed zbyt wysokim napięciem, odwróceniem biegunowości zasilania oraz przed zwarciami [216].

ADA_023 Adapter musi:

— reagować na pole magnetyczne, które zakłóca wykrywanie ruchu pojazdu. W takich okolicznościach przyrząd rejestrujący zarejestruje i zapisze w pamięci usterkę czujnika [88]; albo

— posiadać czujnik, który jest chroniony przed polami magnetycznymi lub odporny na nie [217].

ADA_024 Adapter musi spełniać przepisy międzynarodowego regulaminu EKG ONZ nr 10, odnoszące się do kompatybilności elektromagnetycznej, jak również musi być zabezpieczony przed skutkami wyładowań elektrostatycznych oraz stanów nieustalonych [218].

4.6. **Materiały**

ADA_025 Adapter musi spełniać wymagania odnośnie do stopnia ochrony *(do ustalenia przez producenta, zależnie od miejsca instalacji)* [220, 221].

ADA_026 Obudowa adaptera musi być żółta.

4.7. **Oznakowania**

ADA_027 Do adaptera musi być przymocowana tabliczka opisowa z następującymi danymi:

— nazwa i adres producenta adaptera;

— numer części producenta i rok produkcji adaptera;

— znak homologacji typu dla adaptera lub urządzenia rejestrującego zawierającego adapter;

— data instalacji adaptera;

— numer identyfikacyjny pojazdu, w którym zainstalowano dany adapter.

ADA_028 Na tabliczce opisowej umieszcza się również następujące dane, jeżeli nie można ich bezpośrednio odczytać z zewnątrz na wbudowanym czujniku ruchu:

— nazwa producenta wbudowanego czujnika ruchu;

— numer części producenta i rok produkcji wbudowanego czujnika ruchu;

— znak homologacji wbudowanego czujnika ruchu.

5. INSTALACJA URZĄDZENIA REJESTRUJĄCEGO W PRZYPADKU ZASTOSOWANIA ADAPTERA

5.1. **Instalacja**

ADA_029 Adaptery przeznaczone do zamontowania w pojazdach są montowane wyłącznie przez producentów pojazdów, bądź przez zatwierdzone warsztaty, upoważnione do instalacji, aktywacji oraz kalibracji tachografów cyfrowych i inteligentnych.

ADA_030 Taki zatwierdzony warsztat instalujący adaptery musi dostosować interfejs wejściowy oraz wybrać podzielnik wejściowego sygnału (w stosownych przypadkach).

ADA_031 Taki zatwierdzony warsztat instalujący adapter musi zaplombować jego obudowę.

ADA_032 Adapter montuje się jak najbliżej tej części pojazdu, która jest źródłem impulsów wejściowych.

ADA_033 Przewody zasilające adapter muszą być czerwone (plus zasilania) i czarne (masa).

5.2. **Plombowanie**

ADA_034 W odniesieniu do plombowania zastosowanie mają następujące wymagania:

— obudowa adaptera musi być zaplombowana (zob. ADA_017);

— obudowa wbudowanego czujnika ruchu musi być połączona plombą z obudową adaptera, chyba że nie można usunąć czujnika ruchu z obudowy adaptera bez naruszania plomby(plomb) obudowy adaptera (zob. ADA_018);

— obudowa adaptera musi być połączona plombą z pojazdem;

— połączenie między adapterem a urządzeniem będącym źródłem impulsów wejściowych musi być zaplombowane na obu końcach (na tyle, na ile jest to możliwe).

6. KONTROLE, PRZEGLĄDY I NAPRAWY

6.1. **Przeglądy okresowe**

ADA_035 Każdy przegląd okresowy (przegląd okresowy oznacza przegląd zgodny z wymaganiami [409]–[413] zawartymi w załączniku 1C) urządzenia rejestrującego w przypadku zastosowania adaptera obejmuje sprawdzenie:

— czy na adapterze znajdują się odpowiednie znaki homologacji typu;

— czy plomby na adapterze i jego podłączeniach są nienaruszone;

— czy adapter zainstalowano zgodnie z informacjami podanymi na tabliczce instalacyjnej;

— czy adapter zainstalowano zgodnie z instrukcjami producenta adaptera lub pojazdu;

— czy dopuszcza się instalację adaptera w kontrolowanym pojeździe.

ADA_036 Przedmiotowe przeglądy obejmują kalibrację i wymianę wszystkich plomb, niezależnie od ich stanu.

7. HOMOLOGACJA TYPU URZĄDZENIA REJESTRUJĄCEGO W PRZYPADKU ZASTOSOWANIA ADAPTERA

7.1. **Uwagi ogólne**

ADA_037 Urządzenie rejestrujące dostarcza się do homologacji typu w stanie kompletnym z adapterem [425].

ADA_038 Do homologacji typu można przedstawić sam adapter lub adapter jako element składowy urządzenia rejestrującego.

ADA_039 Homologacja typu obejmuje badania funkcjonalności adaptera. Pozytywne wyniki każdego z tych badań potwierdza się odpowiednim świadectwem [426].

7.2. **Świadectwo funkcjonalności**

ADA_040 Świadectwo funkcjonalności adaptera lub urządzenia rejestrującego zawierającego adapter wydaje się producentowi adaptera wyłącznie po pozytywnym przejściu co najmniej przez wszystkie wyszczególnione niżej badania funkcjonalności.

Nr	Badanie	Wyszczególnienie	Odpowiednie wymagania
1.	**Badanie administracyjne**		
1.1	Dokumentacja	Prawidłowość dokumentacji adaptera	
2.	**Kontrola wizualna**		
2.1.	Zgodność adaptera z dokumentacją		
2.2.	Identyfikacja / oznakowania adaptera		ADA_027, ADA_028
2.3	Materiały, z których wykonany jest adapter		[219]–[223] ADA_026
2.4.	Plombowanie		ADA_017, ADA_018, ADA_034
3.	**Badania funkcjonalności**		
3.1	Przekazywanie impulsów prędkości do wbudowanego czujnika ruchu		ADA_013
3.2	Odbiór i przetwarzanie wejściowych impulsów prędkości		ADA_011, ADA_012
3.3	Dokładność pomiaru ruchu		[30]–[35], [217]
4.	**Badania środowiskowe**		
4.1	Wyniki badań producenta	Wyniki badań środowiskowych przeprowadzonych przez producenta	ADA_020, ADA_021, ADA_022, ADA_024
5.	**EMC (kompatybilność elektromagnetyczna)**		
5.1	Emisje radiacyjne i wrażliwość na radiację	Sprawdzenie zgodności z przepisami dyrektywy 2006/28/WE	ADA_024
5.2	Wyniki badań producenta	Wyniki badań środowiskowych przeprowadzonych przez producenta	ADA_024