2025/2462

9.12.2025

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2025/2462

z dnia 8 grudnia 2025 r.

zmieniające rozporządzenie wykonawcze (UE) 2024/482 w odniesieniu do definicji, certyfikacji serii produktów ICT, ciągłości uzasadnienia zaufania oraz dokumentów odzwierciedlających stan wiedzy

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) ([1]), w szczególności jego art. 49 ust. 7,

a także mając na uwadze, co następuje:

(1) W rozporządzeniu wykonawczym Komisji (UE) 2024/482 ([2]) określono role, zasady i obowiązki, a także strukturę europejskiego programu certyfikacji cyberbezpieczeństwa opartego na wspólnych kryteriach (EUCC) zgodnie z europejskimi ramami certyfikacji cyberbezpieczeństwa określonymi w rozporządzeniu (UE) 2019/881.

(2) Wspólna metodyka oceny uzupełniająca wspólne kryteria – stanowiące międzynarodową normę oceny bezpieczeństwa technologii informacyjnych – umożliwia ocenę bezpieczeństwa produktów ICT do celów certyfikacji. W tym kontekście niektóre produkty ICT mogą być tworzone na tej samej podstawie funkcjonalnej w celu zapewnienia podobnych funkcji bezpieczeństwa na różnych platformach lub urządzeniach, co określa się jako serię produktów. Koncepcja, sprzęt, oprogramowanie układowe lub oprogramowanie mogą się jednak różnić w przypadku poszczególnych produktów ICT. To jednostka certyfikująca podejmuje w poszczególnych przypadkach decyzję, czy można przeprowadzić certyfikację serii produktów. Warunki certyfikacji serii produktów mogłyby zostać dokładniej określone w uzupełniających wytycznych dotyczących EUCC.

(3) W celu utrzymania niezawodności certyfikowanych produktów konieczne jest zdefiniowanie, co stanowi istotną oraz nieistotną zmianę celu oceny lub jego środowiska, w tym środowiska operacyjnego lub rozwojowego. W związku z tym konieczne jest sprecyzowanie tych pojęć przy uwzględnieniu istniejących i powszechnie stosowanych specyfikacji technicznych przyjętych przez grupę wyższych urzędników ds. bezpieczeństwa systemów informatycznych (SOG-IS) oraz uczestników porozumienia w sprawie uznawania certyfikatów w dziedzinie bezpieczeństwa informatycznego wydanych na podstawie wspólnych kryteriów (CCRA).

(4) Zmiany nieistotne często charakteryzuje ich ograniczony wpływ na oświadczenie o uzasadnieniu zaufania do produktu zawarte w wydanym certyfikacie EUCC. Z tego względu zmianami nieistotnymi należy zarządzać w ramach procedur utrzymania i nie wymagają one ponownej oceny funkcji bezpieczeństwa produktu. Przykłady zmian nieistotnych, które powinny być uwzględnione w ramach procedur utrzymania, obejmują między innymi zmiany redakcyjne, zmiany w zakresie środowiska celu oceny, które nie prowadzą do zmiany certyfikowanego celu oceny, oraz zmiany certyfikowanego celu oceny, które nie mają wpływu na dowody uzasadnienia zaufania. Zmiany w środowisku rozwojowym można również uznać za nieistotne, pod warunkiem że nie mają one dalszego wpływu na istniejące środki dotyczące uzasadnienia zaufania. W niektórych przypadkach mogą one jednak wymagać przeprowadzenia częściowej oceny odpowiednich środków.

([1]) Dz.U. L 151 z 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

([2]) Rozporządzenie wykonawcze Komisji (UE) 2024/482 z dnia 31 stycznia 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 w odniesieniu do przyjęcia europejskiego programu certyfikacji cyberbezpieczeństwa opartego na wspólnych kryteriach (EUCC) (Dz.U. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(5) Zmianę istotną stanowi każda zmiana certyfikowanego celu oceny lub jego środowiska, która może mieć negatywny wpływ na uzasadnienie zaufania zawarte w certyfikacie EUCC, w związku z czym wymagane jest przeprowadzenie ponownej oceny. Przykłady zmian istotnych obejmują między innymi: zmiany w zestawie wymogów dotyczących deklarowanego zaufania, z wyjątkiem wymogów dotyczących zaufania z rodziny CC ALC_FLR (usuwanie usterek); zmiany w środkach kontroli poufności lub integralności środowiska rozwojowego, w przypadku gdy takie zmiany mogłyby mieć wpływ na bezpieczny rozwój lub realizację celu oceny; oraz zmiany celu oceny służące usunięciu nadającej się do wykorzystania podatności. Ponadto również zbiór zmian nieistotnych, które łącznie mają znaczący wpływ na bezpieczeństwo, może zostać uznany za zmianę istotną. Należy również uznać, że choć poprawka błędu może mieć wpływ jedynie na konkretny aspekt celu oceny, jednak jej nieprzewidywalność i potencjalny wpływ na zaufanie mogą sprawić, że stanowi ona zmianę istotną, jeżeli narusza ona uzasadnienia zaufania do bezpieczeństwa zawarte w certyfikacji.

(6) Zmiany w środowisku zagrożeń niezmienionego certyfikowanego produktu ICT mogą wymagać dokonania ponownej oceny. Należy jasno określić możliwe wyniki takiego procesu ponownej oceny, w szczególności jego wpływ na certyfikat EUCC. Jeżeli ponowna ocena została pomyślnie zakończona, jednostka certyfikująca powinna potwierdzić certyfikat lub wydać nowy certyfikat z przedłużonym terminem ważności. Jeżeli proces ponownej oceny nie został pomyślnie zakończony, jednostka certyfikująca powinna cofnąć certyfikat i ewentualnie wydać nowy certyfikat o innym zakresie. Przepisy te powinny mieć odpowiednio zastosowanie do ponownej oceny profili zabezpieczeń.

(7) W załączniku I do rozporządzenia wykonawczego (UE) 2024/482 wymieniono dokumenty odzwierciedlające stan wiedzy mające zastosowanie do celów oceny produktów ICT i profili zabezpieczeń. Dokumenty takie należy aktualizować w celu odzwierciedlenia najnowszych zmian, takich jak zmiany związane z rozwojem technologicznym, krajobrazem cyberzagrożeń, praktykami branżowymi lub normami międzynarodowymi. Taka aktualizacja jest odpowiednia w przypadku dokumentów odzwierciedlających stan wiedzy dotyczących minimalnych wymogów bezpieczeństwa obiektu, zastosowania potencjału ataku do kart elektronicznych, zastosowania potencjału ataku do urządzeń sprzętowych ze skrzynkami bezpieczeństwa, zastosowania wspólnych kryteriów do układów scalonych i oceny produktu złożonego w przypadku kart elektronicznych i podobnych urządzeń. Nie uwzględniono dokumentów odzwierciedlających stan wiedzy dotyczących oceny i certyfikacji produktu złożonego z wykorzystaniem najnowszej wersji norm dotyczących wspólnych kryteriów, ponownego wykorzystania wyników oceny uzyskanych w ramach audytów obiektu oraz wyjaśnień dotyczących interpretacji profili zabezpieczeń związanych z kwalifikowanymi urządzeniami do składania podpisu elektronicznego, tachografami i modułami bezpieczeństwa sprzętu. Aby zapewnić jednolitą ocenę produktów ICT w ramach EUCC, należy zmienić załącznik I, tak aby uwzględniał te zaktualizowane i nowe dokumenty odzwierciedlające stan wiedzy po ich zatwierdzeniu przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa (ECCG).

(8) Ponadto w programie należy uwzględnić dokument odzwierciedlający stan wiedzy „ADV_SPM.1 interpretation for CC:2022 transition" (Interpretacja ADV_SPM.1 na potrzeby przejścia na CC:2022), aby zapewnić, by procesy certyfikacji oparte na określonych profilach zabezpieczeń mogły nadal wykorzystywać modelowanie formalne (ADV_SPM.1) do czasu aktualizacji odpowiednich profili zabezpieczeń, na przykład poprzez dodanie zgodnej z CC:2022 konfiguracji profilu zabezpieczeń wykorzystującej wiele uzasadnień zaufania, która obsługuje ADV_SPM.1. Aby zapewnić rynkowi wystarczająco dużo czasu na przejście na zaktualizowane normy dotyczące wspólnych kryteriów, należy przewidzieć szczegółowe przepisy przejściowe w odniesieniu do profili zabezpieczeń Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014, Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020 oraz Java Card System – Open Configuration (v3.1), BSI-CC-PP-0099-V2-2020. Aby uniknąć zakłóceń na rynku należy ustalić, że dokument odzwierciedlający stan wiedzy dotyczący interpretacji ADV_SPM.1 na potrzeby przejścia na CC:2022 ma zastosowanie do procesów certyfikacji zainicjowanych przed przyjęciem niniejszego rozporządzenia. Stosowanie tego dokumentu powinno być jednak ściśle ograniczone do tego, co jest niezbędne, przy uwzględnieniu czasu potrzebnego do zakończenia aktualizacji odpowiednich profili zabezpieczeń. Dokładniej rzecz ujmując, w odniesieniu do procesów certyfikacji, które wykorzystują profile zabezpieczeń Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014 lub Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020, ten dokument odzwierciedlający stan wiedzy powinien mieć zastosowanie do tych procesów, które zostały zainicjowane przed dniem 1 października 2026 r. W odniesieniu do procesów certyfikacji, które wykorzystują profil zabezpieczeń Java Card System – Open Configuration (v3.1), BSI-CC-PP-0099-V2-2020, przedmiotowy dokument odzwierciedlający stan wiedzy powinien mieć zastosowanie wyłącznie do tych procesów, które zostały zainicjowane przed datą wejścia w życie niniejszego rozporządzenia, z uwagi na fakt, że dostępna jest już nowa wersja profilu zabezpieczeń Java Card System – Open Configuration.

(9) Zmiana w dokumentach odzwierciedlających stan wiedzy dokonana w trakcie procesu certyfikacji mogłaby zakłócić ocenę produktu i opóźnić wydanie certyfikatu. W przypadku nowych lub zaktualizowanych dokumentów odzwierciedlających stan wiedzy konieczne jest zatem ustanowienie odpowiednich przepisów przejściowych, aby umożliwić sprzedawcom, ITSEF, jednostkom certyfikującym i innym zainteresowanym stronom dokonanie niezbędnych dostosowań. Mające zastosowanie zaktualizowane i nowe dokumenty odzwierciedlające stan wiedzy powinny dotyczyć nowych wniosków o certyfikację, w tym wniosków o ponowną ocenę, natomiast w przypadku trwających już procesów certyfikacji powinno być możliwe dalsze korzystanie z wcześniejszych wersji dokumentów odzwierciedlających stan wiedzy.

(10) W załącznikach II i III do rozporządzenia wykonawczego (UE) 2024/482 wymieniono, odpowiednio, profile zabezpieczeń certyfikowane na poziomie AVA_VAN 4 lub 5 oraz zalecane profile zabezpieczeń. Niektóre odniesienia są niepełne lub nieaktualne ze względu na aktualizację profili zabezpieczeń. Odniesienia te należy uzupełnić, jak również należy dodać nowe odniesienia, aby zapewnić bardziej kompleksowe uwzględnienie układów scalonych, kart elektronicznych i powiązanych urządzeń oraz zaufanego przetwarzania danych.

(11) Należy wprowadzić zmiany w art. 19 rozporządzenia wykonawczego (UE) 2024/482 w celu sprecyzowania, że załącznik IV ma zastosowanie, z niezbędnymi zmianami, do przeglądu certyfikatów EUCC dotyczących profili zabezpieczeń.

(12) Biorąc pod uwagę, że cel bezpieczeństwa stanowi jeden z kluczowych elementów umożliwiających zrozumienie zakresu procesu certyfikacji, konieczne jest również, by ENISA publikowała na swojej stronie internetowej cel bezpieczeństwa odpowiadający każdemu certyfikatowi EUCC.

(13) Ponadto jednostki certyfikujące powinny przekazywać ENISA wersję celu bezpieczeństwa i sprawozdania z certyfikacji w języku angielskim, aby umożliwić agencji udostępnienie tych informacji w języku angielskim na odpowiedniej stronie internetowej, zgodnie z art. 42 ust. 2 rozporządzenia wykonawczego (UE) 2024/482. Z tego względu wnioskodawcy ubiegający się o certyfikację powinni przekazywać jednostkom certyfikującym wersję celu bezpieczeństwa w języku angielskim, jeżeli jednostka certyfikująca tego zażąda.

(14) Nie jest konieczne, by odniesienie do nazwy jednostki certyfikującej występowało w niepowtarzalnym identyfikatorze certyfikatu, gdyż do zidentyfikowania takiej jednostki wystarcza jej numer identyfikacyjny. Miesiąc wydania również nie musi występować, gdyż liczenie certyfikatów odbywa się w ujęciu rocznym. W celu uproszczenia należy zatem skreślić ten wymóg. Ponieważ rok wydania certyfikatu odpowiada wydaniu pierwszego certyfikatu, w celu zapewnienia identyfikowalności ta sama data powinna pojawić się w niepowtarzalnym identyfikatorze na certyfikatach wydanych po dokonaniu przeglądu.

(15) Należy zatem odpowiednio zmienić rozporządzenie wykonawcze (UE) 2024/482.

(16) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią komitetu ustanowionego na mocy art. 66 rozporządzenia (UE) 2019/881,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

W rozporządzeniu wykonawczym (UE) 2024/482 wprowadza się następujące zmiany:

1) w art. 2 dodaje się punkty 16, 17 i 18 w brzmieniu:

„16) »seria produktów« oznacza zestaw produktów ICT wnioskodawcy, które to produkty są zbudowane na tej samej podstawie funkcjonalnej w celu zaspokojenia tych samych potrzeb w zakresie bezpieczeństwa, ale których koncepcja, sprzęt, oprogramowanie układowe lub oprogramowanie mogą różnić się w przypadku poszczególnych produktów ICT;

17) »zmiana nieistotna« oznacza każdą zmianę certyfikowanego celu oceny lub jego środowiska, która nie ma negatywnego wpływu na uzasadnienie zaufania zawarte w certyfikacie EUCC;

18) »zmiana istotna« oznacza każdą zmianę certyfikowanego celu oceny lub jego środowiska, która może mieć negatywny wpływ na uzasadnienie zaufania zawarte w certyfikacie EUCC.";

2) w art. 5 dodaje się ust. 3 w brzmieniu:

„3. Jednostka certyfikująca może zezwolić na certyfikację serii produktów.";

3) art. 9 ust. 2 lit. a) otrzymuje brzmienie:

„a) przekazać jednostce certyfikującej i ITSEF wszelkie niezbędne kompletne i prawidłowe informacje, a na żądanie przekazać dodatkowe niezbędne informacje, w tym wersję celu bezpieczeństwa w języku angielskim;";

4) art. 11 ust. 3 lit. b) otrzymuje brzmienie:

„b) niepowtarzalny identyfikator certyfikatu, składający się z:

1) nazwy programu;

2) numeru identyfikacyjnego, zgodnie z art. 3 rozporządzenia wykonawczego (UE) 2024/3143, jednostki certyfikującej, która wydała certyfikat;

3) roku wydania pierwotnego certyfikatu;

4) numeru identyfikacyjnego przydzielonego przez jednostkę certyfikującą, która wydała certyfikat.";

5) art. 19 ust. 1 otrzymuje brzmienie:

„1. Na wniosek posiadacza certyfikatu lub z innych uzasadnionych powodów jednostka certyfikująca może podjąć decyzję o przeglądzie certyfikatu EUCC dla profilu zabezpieczeń. Przegląd przeprowadza się zgodnie z załącznikiem IV. Jednostka certyfikująca określa zakres przeglądu. Jeżeli jest to konieczne do przeprowadzenia przeglądu, jednostka certyfikująca zwraca się do ITSEF o przeprowadzenie ponownej oceny certyfikowanego profilu zabezpieczeń.";

6) w art. 42 wprowadza się następujące zmiany:

a) w ust. 1 dodaje się lit. i) w brzmieniu:

„i) cel bezpieczeństwa odpowiadający każdemu certyfikatowi EUCC.";

b) ust. 2 otrzymuje brzmienie:

„2. Informacje, o których mowa w ust. 1, udostępnia się co najmniej w języku angielskim. W tym celu jednostki certyfikujące przekazują ENISA oryginalne wersje językowe sprawozdań z certyfikacji oraz celów bezpieczeństwa, a także przekazują bez zbędnej zwłoki wersję takich dokumentów w języku angielskim.";

7) art. 48 ust. 4 otrzymuje brzmienie:

„4. O ile w załączniku I lub II nie określono inaczej, dokumenty odzwierciedlające stan wiedzy stosuje się do procesów certyfikacji, w tym ponownej oceny, które zostały zainicjowane począwszy od dnia rozpoczęcia stosowania aktu zmieniającego, na mocy którego zostały one włączone do załącznika I lub II.";

8) załącznik I zastępuje się tekstem znajdującym się w załączniku I do niniejszego rozporządzenia;

9) załącznik II zastępuje się tekstem znajdującym się w załączniku II do niniejszego rozporządzenia;

10) załącznik III zastępuje się tekstem znajdującym się w załączniku III do niniejszego rozporządzenia;

11) w załączniku IV wprowadza się zmiany zgodnie z załącznikiem IV do niniejszego rozporządzenia;

12) w załączniku V wprowadza się zmiany zgodnie z załącznikiem V do niniejszego rozporządzenia;

13) załącznik IX zastępuje się tekstem znajdującym się w załączniku VI do niniejszego rozporządzenia.

Artykuł 2

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

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

Sporządzono w Brukseli dnia 8 grudnia 2025 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

ZAŁĄCZNIK I

„ZAŁĄCZNIK I

Dokumenty odzwierciedlające stan wiedzy potwierdzające domeny techniczne i inne dokumenty odzwierciedlające stan wiedzy

1. Dokumenty odzwierciedlające stan wiedzy potwierdzające domeny techniczne na poziomie AVA_VAN 4 lub 5:
   a) następujące dokumenty dotyczące zharmonizowanej oceny domeny technicznej »karty elektroniczne i podobne urządzenia«:
      1) »Minimum ITSEF requirements for security evaluations of smart cards and similar devices« [»Minimalne wymogi ITSEF dotyczące oceny bezpieczeństwa kart elektronicznych i podobnych urządzeń«], wersja 1.1;
      2) »Minimum Site Security Requirements« [»Minimalne wymogi bezpieczeństwa obiektu«], wersja 2;
      3) »Reusing evaluation results of site audits (STAR)« [»Ponowne wykorzystanie wyników oceny uzyskanych w ramach audytów obiektu«], wersja 1;
      4) »Application of Common Criteria to integrated circuits« [»Zastosowanie wspólnych kryteriów do układów scalonych«], wersja 2;
      5) »Security Architecture requirements (ADV_ARC) for smart cards and similar devices« [»Wymogi architektury bezpieczeństwa (ADV_ARC) dotyczące kart elektronicznych i podobnych urządzeń«], wersja 1.1;
      6) »Certification of »open« smart card products« [»Certyfikacja »otwartych« produktów kart elektronicznych«], wersja 1.1;
      7) »Composite product evaluation for smart cards and similar devices for CC3.1« [»Ocena produktu złożonego w przypadku kart elektronicznych i podobnych urządzeń dla CC3.1«], wersja 2;
      8) »Composite product evaluation and certification for CC:2022« [»Ocena i certyfikacja produktu złożonego dla CC:2022«], wersja 1;
      9) »Application of Attack Potential to Smartcards and Similar Devices« [»Zastosowanie potencjału ataku do kart elektronicznych i podobnych urządzeń«], wersja 2;
      10) »Security Evaluation and Certification of Qualified Electronic Signature/Seal Creation Devices« [»Ocena i certyfikacja bezpieczeństwa kwalifikowanych urządzeń do składania podpisu elektronicznego/pieczęci"«], wersja 1;
      11) »ADV_SPM.1 interpretation for CC:2022 transition« [»Interpretacja ADV_SPM.1 na potrzeby przejścia na CC:2022«], wersja 1.1, mający zastosowanie do procesów certyfikacji wykorzystujących następujące profile zabezpieczeń:
         a) profile zabezpieczeń Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014, lub Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020, zainicjowanych przed dniem 1 października 2026 r.;
         b) profil zabezpieczeń Java Card System – Open Configuration (v3.1), BSI-CC-PP-0099-V2-2020, zainicjowanych przed dniem 29 grudnia 2025 r.;
   b) następujące dokumenty dotyczące zharmonizowanej oceny domeny technicznej »urządzenia sprzętowe ze skrzynkami bezpieczeństwa«:
      1) »Minimum ITSEF requirements for security evaluations of smart cards and similar devices« [»Minimalne wymogi ITSEF dotyczące oceny bezpieczeństwa urządzeń sprzętowych ze skrzynkami bezpieczeństwa«], wersja 1.1;
      2) »Minimum Site Security Requirements« [»Minimalne wymogi bezpieczeństwa obiektu«], wersja 2;
      3) »Reusing evaluation results of site audits (STAR)« [»Ponowne wykorzystanie wyników oceny uzyskanych w ramach audytów obiektu«], wersja 1;
      4) »Application of Attack Potential to hardware devices with security boxes« [»Zastosowanie potencjału ataku do urządzeń sprzętowych ze skrzynkami bezpieczeństwa«], wersja 2;
      5) »Hardware assessment in EN 419221-5 (HSM PP)« [»Ocena sprzętu w normie EN 419221-5 (HSM PP)«], wersja 1;
      6) »JIL Tachograph MS PP Clarification« [»Sprecyzowanie profilu zabezpieczeń dla tachografów JIL«], wersja 1.
2. Dokumenty odzwierciedlające stan wiedzy związane ze zharmonizowaną akredytacją jednostek oceniających zgodność:
   a) »Accreditation of ITSEFs for the EUCC« [»Akredytacja ITSEF dla EUCC«], wersja 1.1 w odniesieniu do akredytacji wydanych przed dniem 8 lipca 2025 r.;
   b) »Accreditation of ITSEFs for the EUCC« [»Akredytacja ITSEF dla EUCC«], wersja 1.6c w odniesieniu do nowo wydanych akredytacji lub akredytacji poddanych przeglądowi po dniu 8 lipca 2025 r.;
   c) »Accreditation of CBs for the EUCC« [»Akredytacja jednostek certyfikujących dla EUCC«], wersja 1.6b."

ZAŁĄCZNIK II

„ZAŁĄCZNIK II

Profile zabezpieczeń certyfikowane na poziomie AVA_VAN 4 lub 5

1. W przypadku kwalifikowanych urządzeń do składania podpisu i pieczęci na odległość:

   a) EN 419241-2:2019 – Wiarygodne systemy serwerów obsługujących podpisy – Część 2: Profil zabezpieczeń dla QSCD dla serwerów obsługujących podpisy (v0.16), ANSSI-CC-PP-2018/02-M01;

   b) EN 419221-5: 2018 – Profile zabezpieczeń dla modułów kryptograficznych TSP – Część 5: Moduł kryptograficzny dla usług zaufania (v0.15), ANSSI-CC-PP-2016/05-M01.

2. Profile zabezpieczeń, które przyjęto jako dokumenty odzwierciedlające stan wiedzy:

   [BRAK].”

ZAŁĄCZNIK III

„ZAŁĄCZNIK III

Zalecane profile zabezpieczeń

Profile zabezpieczeń stosowane w certyfikacji produktów ICT, w tym produktów w następujących domenach technicznych:

1. Karty elektroniczne i podobne urządzenia:

   a) paszport:

      1) profil zabezpieczeń dokumentu podróży odczytywanego maszynowo z podstawową kontrolą dostępu »aplikacji ICAO« (v1.10), BSI-CC-PP-0055-2009;

      2) profil zabezpieczeń dokumentu podróży odczytywanego maszynowo z wykorzystaniem standardowej procedury inspekcji z protokołem PACE (PACE_PP) (v1), BSI-CC-PP-0068-V2-2011-MA-01;

      3) profil zabezpieczeń dokumentu podróży odczytywanego maszynowo z rozszerzoną kontrolą dostępu »aplikacji ICAO« z protokołem PACE (v1.3), BSI-CC-PP-0056-V2-2012-MA-02;

   b) bezpieczne urządzenia służące do składania podpisu elektronicznego (SSCD):

      1) EN 419211-2:2013 – Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu – Część 2: Urządzenie z generowaniem kluczy (v1.03), BSI-CC-PP-0059-2009-MA-02;

      2) EN 419211-3:2013 – Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu – Część 3: Urządzenie z importem kluczy (v1.0.2), BSI-CC-PP-0075-2012-MA-01;

      3) EN 419211-4:2013 – Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu – Część 4: Rozszerzenie dla urządzenia z generowaniem kluczy i zaufanym kanałem z aplikacją generującą certyfikaty (v1.0.1), BSI-CC-PP-0071-2012-MA-01;

      4) EN 419211-5:2013 – Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu – Część 5: Rozszerzenie dla urządzenia z generowaniem kluczy i zaufanym kanałem z aplikacją do składania podpisu (v1.0.1), BSI-CC-PP-0072-2012-MA-01;

      5) EN 419211-6:2014 – Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu – Część 6: Rozszerzenie dla urządzenia z importem kluczy i zaufanym kanałem z aplikacją do składania podpisu (v1.0.4), BSI-CC-PP-0076-2013-MA-01;

   c) tachograf: Tachograf cyfrowy – karta do tachografu (TC PP) (v1.0), BSI-CC-PP-0091-2017;

   d) układ scalony, platforma Java Card i wbudowana uniwersalna karta z układem scalonym (eUICC):

      1) uniwersalny profil zabezpieczeń dla platformy kart SIM Java, konfiguracje bazowa i SCWS (v2.0.2), ANSSI-CC-PP-2010/04 (konfiguracja bazowa), ANSSI-CC-PP-2010/05 (konfiguracje bazowa i SCWS);

      2) profil zabezpieczeń dla platformy bezpieczeństwa układów scalonych z pakietami uzupełniającymi (v1.0), BSI-CC-PP-0084-2014;

      3) wbudowana uniwersalna karta z układem scalonym (eUICC) do urządzeń komunikacji maszyna–maszyna (v1.1), BSI-CC-PP-0089-2015;

      4) dostawca usług kryptograficznych – CSP (v0.9.8), BSI-CC-PP-0104-2019;

      5) dostawca usług kryptograficznych – usługa znacznika czasu i audyt (PPC-CSP-TS-Au) wersja 0.9.5, BSI-CC-PP-0107-2019;

      6) dostawca konfiguracji usług kryptograficznych – usługa znacznika czasu, audyt i klastering (PPC-CSP-TS-Au) wersja 0.9.4, BSI-CC-PP-0108-2019;

      7) Java Card System – zamknięta konfiguracja (v3.1), BSI-CC-PP-0101-V2-2020;

      8) profil zabezpieczeń dla elementów bezpiecznych – GPC_SPE_174 (v1.0), CCN-CC-PP-5-2021;

      9) profil zabezpieczeń dla bezpiecznego podsystemu w systemie jednoukładowym (3S in SoC) (v1.8), BSI-CC-PP-0117-V2-2023;

      10) Java Card System – otwarta konfiguracja, (v3.2), BSI-CC-PP-0099-V3-2024;

      11) wbudowana uniwersalna karta z układem scalonym (eUICC) dla profilu zabezpieczeń dla urządzeń konsumenckich (v2.1), BSI-CC-PP-0100-V2-2025;

   e) moduł zaufanej platformy: Profil zabezpieczeń dla specyfikacji modułu zaufanej platformy dla komputerów PC rodziny 2.0, poziom 0, wersja 1.59 (v1.3), ANSSI-CC-PP-2021/02.

2. Urządzenia sprzętowe ze skrzynkami zabezpieczającymi:

   a) punkty interakcji (płatności) i terminale płatnicze (POI):

      1) punkt interakcji »POI-CHIP-ONLY« (v4.0), ANSSI-CC-PP-2015/01;

      2) punkt interakcji »POI-CHIP-ONLY and Open Protocol Package« (v4.0), ANSSI-CC-PP-2015/02;

      3) punkt interakcji »POI-COMPREHENSIVE« (v4.0), ANSSI-CC-PP-2015/03;

      4) punkt interakcji »POI-COMPREHENSIVE and Open Protocol Package« (v4.0), ANSSI-CC-PP-2015/04;

      5) punkt interakcji »POI-PED-ONLY« (v4.0), ANSSI-CC-PP-2015/05;

      6) punkt interakcji »POI-PED-ONLY and Open Protocol Package« (v4.0), ANSSI-CC-PP-2015/06;

   b) sprzętowy moduł bezpieczeństwa:

      1) moduł kryptograficzny dla dostawcy kryptograficznych usług operacji podpisu z kopią zapasową – PP CMCSOB 14167-2 (v0.35), ANSSI-CC-PP-2015/08;

      2) moduł kryptograficzny dla dostawcy kryptograficznych usług generowania klucza – PP CMCKG 14167-3 (v0.20), ANSSI-CC-PP-2015/09;

      3) moduł kryptograficzny dla dostawcy kryptograficznych usług operacji podpisu bez kopii zapasowej – PP CMCSO 14167-4 (v0.32), ANSSI-CC-PP-2015/10;

   c) tachograf:

      1) tachograf cyfrowy – czujnik ruchu (profil zabezpieczeń czujnika ruchu) (v1.0), BSI-CC-PP-0093-2017;

      2) tachograf cyfrowy – przyrząd rejestrujący (profil zabezpieczeń przyrządu rejestrującego) (v1.15), BSI-CC-PP-0094-V2-2021;

      3) tachograf cyfrowy – urządzenie zewnętrzne GNSS (profil zabezpieczeń urządzenia zewnętrznego GNSS (EGF)) (v1.10), BSI-CC-PP-0092-V2-2021.

3. Inne: Profil zabezpieczeń zaufanego środowiska wykonawczego – GPD_SPE_021 (v1.3), ANSSI-CC-PP-2014/01-M02.”

ZAŁĄCZNIK IV

W załączniku IV do rozporządzenia wykonawczego (UE) 2024/482 wprowadza się następujące zmiany:

1) pkt IV.2 ppkt 4 otrzymuje brzmienie:

„4. Jednostka certyfikująca dokonuje przeglądu zaktualizowanego sprawozdania technicznego z oceny i sporządza sprawozdanie z ponownej oceny. Status pierwotnego certyfikatu zostaje następnie zmieniony zgodnie z art. 13 lub art. 19. Jeżeli proces ponownej oceny zakończy się pomyślnie, w przypadku certyfikacji produktu zastosowanie ma art. 13 ust. 2 lit. a) lub c), natomiast w przypadku certyfikacji profilu zabezpieczeń zastosowanie ma art. 19 ust. 2 lit. a) lub c). Jeżeli proces ponownej oceny nie zakończy się pomyślnie, w przypadku certyfikacji produktu zastosowanie ma art. 13 ust. 2 lit. b) lub d), natomiast w przypadku certyfikacji profilu zabezpieczeń zastosowanie ma art. 19 ust. 2 lit. b) lub d).”;

2) w pkt IV.3 wprowadza się następujące zmiany:

a) tytuł pkt IV.3 otrzymuje brzmienie:

„IV.3 **Zmiany w certyfikowanym produkcie ICT – utrzymanie i ponowna ocena**”;

b) ppkt 4 i 5 otrzymują brzmienie:

„4. Po przeprowadzeniu badania jednostka certyfikująca określa skalę zmiany jako nieistotną lub istotną w zależności od jej skutków dla uzasadnienia zaufania zawartego w certyfikacie EUCC.

5. W przypadku gdy jednostka certyfikująca potwierdziła, że zmiany są nieistotne, nie wydaje się nowego certyfikatu dla zmienionego produktu ICT zgodnie z art. 13 ust. 2 lit. a) lub art. 19 ust. 2 lit. a) oraz sporządza się sprawozdanie z utrzymania dotyczące pierwotnego sprawozdania z certyfikacji.”;

c) dodaje się ppkt 5a w brzmieniu:

„5a. W przypadku jakichkolwiek zmian środków dotyczących uzasadnienia zaufania w środowisku rozwojowym, w tym dodania wymogów dotyczących uzasadnienia zaufania z rodziny CC ALC_FLR (usuwanie usterek), jednostka certyfikująca może zwrócić się do ITSEF o przeprowadzenie częściowej oceny przedmiotowych środków dotyczących uzasadnienia zaufania. ITSEF publikuje sprawozdanie techniczne z częściowej oceny, na podstawie którego jednostka certyfikująca potwierdza, że zmiany są nieistotne lub istotne. W przypadku gdy jednostka certyfikująca potwierdziła, że zmiany są nieistotne, zastosowanie ma pkt IV.3 ppkt 5. W przypadku gdy jednostka certyfikująca potwierdziła, że zmiany są istotne, zastosowanie ma pkt IV.3 ppkt 7.”.

ZAŁĄCZNIK V

Pkt V.1 w załączniku V do rozporządzenia wykonawczego (UE) 2024/482 otrzymuje brzmienie:

„V.1 **Sprawozdanie z certyfikacji**

1. Na podstawie sprawozdań technicznych z oceny przedstawionych przez ITSEF jednostka certyfikująca sporządza sprawozdanie z certyfikacji, które zostaje opublikowane wraz z odpowiednim certyfikatem EUCC i celem bezpieczeństwa.

2. Sprawozdanie z certyfikacji jest źródłem szczegółowych i praktycznych informacji na temat produktu ICT oraz na temat bezpiecznego wdrożenia produktu ICT. Musi ono zatem zawierać wszystkie publicznie dostępne i możliwe do udostępnienia informacje istotne dla użytkowników i zainteresowanych stron. W sprawozdaniu z certyfikacji można przywoływać publicznie dostępne i możliwe do udostępnienia informacje.

3. Sprawozdanie z certyfikacji zawiera co najmniej następujące informacje:
   a) streszczenie;
   b) identyfikację produktu ICT;
   c) informacje na potrzeby kontaktu w związku z oceną produktu ICT;
   d) politykę bezpieczeństwa;
   e) założenia i sprecyzowanie zakresu;
   f) informacje dotyczące architektury;
   g) w stosownych przypadkach – dodatkowe informacje na temat cyberbezpieczeństwa;
   h) streszczenie oceny produktu ICT oraz ocenianą konfigurację;
   i) wyniki oceny i informacje dotyczące certyfikatu;
   j) w stosownych przypadkach – uwagi i zalecenia;
   k) w stosownych przypadkach – załączniki;
   l) odniesienie do celu bezpieczeństwa produktu ICT przedłożonego do certyfikacji;
   m) znak lub etykietę związane z programem, o ile są dostępne;
   n) w stosownych przypadkach – glosariusz;
   o) bibliografię.

4. Streszczenie, o którym mowa w ppkt 3 lit. a), jest krótkim streszczeniem całego sprawozdania z certyfikacji. Zawiera ono jasny i zwięzły przegląd wyników oceny oraz następujące informacje:
   a) nazwę ocenionego produktu ICT;
   b) nazwę ITSEF, która przeprowadziła ocenę;
   c) datę zakończenia oceny;
   d) datę wydania certyfikatu;
   e) w stosownych przypadkach – datę wydania pierwotnego certyfikatu;
   f) okres ważności;
   g) niepowtarzalny identyfikator certyfikatu zgodnie z art. 11;
   h) krótki opis wyników sprawozdania z certyfikacji, w tym:
      (i) wersję oraz, w stosownych przypadkach, wydanie wspólnych kryteriów zastosowanych do oceny;
      (ii) pakiet dotyczący uzasadnienia zaufania zawarty we wspólnych kryteriach lub wykaz komponentów uzasadnienia zaufania do bezpieczeństwa, poziom AVA_VAN stosowany podczas oceny oraz odpowiadający mu poziom uzasadnienia zaufania określony w art. 52 rozporządzenia (UE) 2019/881, do którego to poziomu odnosi się certyfikat EUCC;
      (iii) w stosownych przypadkach – profil(-e) zabezpieczeń, w odniesieniu do którego(-ych) zadeklarowano zgodność produktu ICT;
      (iv) odniesienie do polityki bezpieczeństwa ocenionego produktu ICT;
      (v) w stosownych przypadkach – zastrzeżenie(-a) o wyłączeniu odpowiedzialności.

5. Identyfikator, o którym mowa w ppkt 3 lit. b), jasno określa oceniony produkt ICT i zawiera następujące informacje:

   a) niepowtarzalny identyfikator ocenionego produktu ICT;

   b) wyliczenie komponentów produktu ICT stanowiących część oceny, wraz z numerem wersji każdego komponentu;

   c) odniesienie do dodatkowych wymogów dotyczących środowiska operacyjnego certyfikowanego produktu ICT.

6. Informacje na potrzeby kontaktu, o których mowa w ppkt 3 lit. c), obejmują co najmniej następujące informacje:

   a) imię i nazwisko lub nazwę twórcy;

   b) imię i nazwisko lub nazwę oraz dane kontaktowe posiadacza certyfikatu EUCC;

   c) nazwę jednostki certyfikującej, która wydała certyfikat;

   d) odpowiedzialny krajowy organ ds. certyfikacji cyberbezpieczeństwa;

   e) nazwę ITSEF, która przeprowadziła ocenę, oraz, w stosownych przypadkach, wykaz podwykonawców.

7. Polityka bezpieczeństwa, o której mowa w ppkt 3 lit. d), zawiera opis polityki bezpieczeństwa produktu ICT jako zbioru usług w zakresie bezpieczeństwa oraz polityk lub zasad, których egzekwowaniu oceniony produkt ICT ma służyć lub z którymi musi być zgodny. Zawiera ona również następujące informacje:

   a) opis procedur posiadacza certyfikatu w zakresie zarządzania podatnością i ujawniania podatności, który powinien zawierać wyłącznie informacje, które mogą zostać udostępnione publicznie;

   b) politykę posiadacza certyfikatu w zakresie ciągłości uzasadnienia zaufania, w tym, w stosownych przypadkach, opis procesów posiadacza certyfikatu w zakresie zarządzania cyklem życia lub produkcji zgodnie z sekcją IV.1 załącznika IV;

   c) w stosownych przypadkach – obecność procedury zarządzania poprawkami oraz wynik jej oceny zgodnie z sekcją IV.4 załącznika IV.

8. Założenia i sprecyzowanie zakresu, o których mowa w ppkt 3 lit. e), obejmują informacje dotyczące okoliczności i celów związanych z przewidzianym stosowaniem produktu, o którym to stosowaniu mowa w art. 7 ust. 1 lit. c), w tym następujące elementy:

   a) założenia dotyczące stosowania i wdrażania produktu ICT w formie minimalnych wymogów, takich jak spełnienie wymogów dotyczących właściwej instalacji i konfiguracji oraz wymogów sprzętowych;

   b) założenia dotyczące środowiska w odniesieniu do zgodnego z wymogami funkcjonowania produktu ICT;

   c) opis wszelkich zagrożeń dla produktu ICT, którym nie przeciwdziałają ocenione funkcje bezpieczeństwa produktu zgodnie z przewidzianym stosowaniem, jeżeli zostaną uznane za istotne dla potencjalnego użytkownika produktu ICT.

   Informacje, o których mowa w akapicie pierwszym, muszą być jak najbardziej jasne i zrozumiałe, aby umożliwić użytkownikom certyfikowanego produktu ICT podejmowanie świadomych decyzji dotyczących ryzyka związanego z jego stosowaniem.

9. Informacje dotyczące architektury, o których mowa w ppkt 3 lit. f), obejmują ogólny opis produktu ICT i jego głównych komponentów w oparciu o wymogi zdefiniowane we wspólnych kryteriach dla rodziny uzasadnienia zaufania Development – TOE Design (rozwój – koncepcja celu oceny) (ADV_TDS).

10. Dodatkowe informacje na temat cyberbezpieczeństwa, o których mowa w ppkt 3 lit. g), obejmują link do strony internetowej posiadacza certyfikatu EUCC, o której mowa w art. 55 rozporządzenia (UE) 2019/881.

11. Streszczenie oceny produktu ICT oraz oceniana konfiguracja, o których mowa w ppkt 3 lit. h), obejmują opis działań w zakresie badania produktu przeprowadzonych zarówno przez twórcę, jak i oceniającego, w tym przedstawienie podejścia do badań, konfiguracji i stopnia szczegółowości. Obejmuje to co najmniej następujące informacje:

    a) wskazanie wykorzystanych komponentów uzasadnienia zaufania pochodzących z norm, o których mowa w art. 3;

    b) wersję dokumentów odzwierciedlających stan wiedzy i dalsze kryteria oceny bezpieczeństwa zastosowane w ocenie;

    c) ustawienia i konfigurację celu oceny wykorzystywanego na potrzeby badania i analizy podatności;

    d) wszelkie zastosowane profile zabezpieczeń, w tym następujące informacje: nazwę, wersję, datę i certyfikat profilu zabezpieczeń.

12. Wyniki oceny i informacje dotyczące certyfikatu, o których mowa w ppkt 3 lit. i), obejmują informacje na temat osiągniętego poziomu uzasadnienia zaufania, o którym mowa w art. 4 niniejszego rozporządzenia oraz w art. 52 rozporządzenia (UE) 2019/881.

13. Uwagi i zalecenia, o których mowa w ppkt 3 lit. j), stosuje się w celu przekazania dodatkowych informacji na temat wyników oceny. Te uwagi i zalecenia mogą przybrać formę informacji na temat niedociągnięć produktu ICT wykrytych podczas oceny lub wzmianek na temat cech, które są szczególnie przydatne.

14. Załączniki, o których mowa w ppkt 3 lit. k), stosuje się w celu przedstawienia wszelkich dodatkowych informacji, które mogą być przydatne dla odbiorców sprawozdania, ale logicznie nie odpowiadają odpowiednim punktom sprawozdania, w tym w przypadku pełnego opisu polityki bezpieczeństwa.

15. Cel bezpieczeństwa, o którym mowa w ppkt 3 lit. l), musi odnosić się do ocenianego celu bezpieczeństwa. Oceniany cel bezpieczeństwa przedstawia się wraz ze sprawozdaniem z certyfikacji do celów publikacji na stronie internetowej, o której mowa w art. 50 ust. 1 rozporządzenia (UE) 2019/881. W przypadku gdy przed publikacją konieczna jest sanityzacja ocenianego celu bezpieczeństwa, dokonuje się jej zgodnie z pkt V.2 załącznika V do niniejszego rozporządzenia.

16. Znaki lub etykiety związane z programem EUCC, o których mowa w ppkt 3 lit. m), umieszcza się w sprawozdaniu z certyfikacji zgodnie z zasadami i procedurami określonymi w art. 11.

17. Glosariusz, o którym mowa w ppkt 3 lit. n), stosuje się w celu zwiększenia czytelności sprawozdania przez przedstawienie definicji akronimów lub terminów, których znaczenie może być niejasne.

18. Bibliografia, o której mowa w ppkt 3 lit. o), zawiera odniesienia do wszystkich dokumentów wykorzystanych przy sporządzaniu sprawozdania z certyfikacji. Dokumenty te obejmują co najmniej:

    a) kryteria oceny bezpieczeństwa, dokumenty odzwierciedlające stan wiedzy i inne wykorzystane odpowiednie specyfikacje;

    b) sprawozdanie techniczne z oceny;

    c) w stosownych przypadkach – sprawozdanie techniczne z oceny na potrzeby oceny złożonej;

    d) referencyjną dokumentację techniczną;

    e) wytyczne dotyczące bezpieczeństwa dla twórców;

    f) wykaz dotyczący konfiguracji dla twórców.

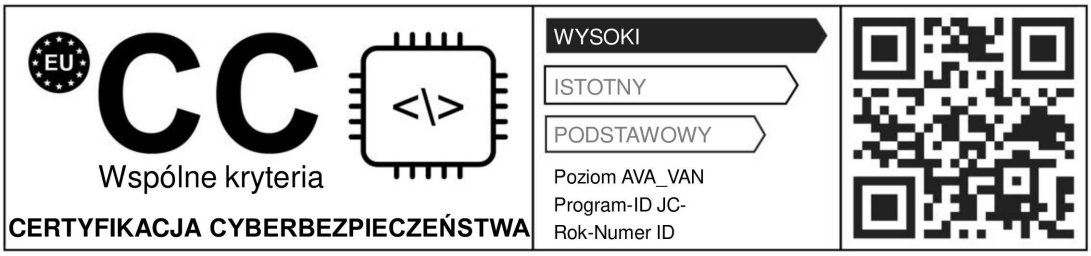
    Aby zagwarantować odtwarzalność oceny, cała przywołana dokumentacja musi być jednoznacznie zidentyfikowana za pomocą właściwej daty wydania i właściwego numeru wersji.”.

ZAŁĄCZNIK VI

„ZAŁĄCZNIK IX

Znak i etykieta

1. Forma znaku i etykiety:



2. W przypadku zmniejszenia lub powiększenia znaku i etykiety należy zachować proporcje przedstawione w pkt 1.

3. W przypadku fizycznej obecności znak i etykieta muszą mieć co najmniej 5 mm wysokości.”