ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2026/1731

z dnia 15 lipca 2026 r.

w sprawie zmiany rozporządzeń wykonawczych (UE) 2024/2977, (UE) 2024/2979, (UE) 2024/2980 i (UE) 2024/2982 w odniesieniu do mających zastosowanie norm i specyfikacji

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE ([1]), w szczególności jego art. 5a ust. 23,

a także mając na uwadze, co następuje:

(1) Aby zapewnić maksymalną harmonizację działań państw członkowskich w zakresie opracowywania europejskich portfeli tożsamości cyfrowej, specyfikacje techniczne portfeli opierają się na pracach przeprowadzonych na podstawie zalecenia Komisji (UE) 2021/946 ([2]), a w szczególności na architekturze i ramach odniesienia. Ponieważ architektura i ramy odniesienia uległy istotnym zmianom od czasu przyjęcia rozporządzeń wykonawczych Komisji (UE) 2024/2977 ([3]), (UE) 2024/2979 ([4]), (UE) 2024/2980 ([5]) i (UE) 2024/2982 ([6]), te rozporządzenia wykonawcze należy obecnie zmienić w celu dostosowania ich do nowych norm, specyfikacji i procedur.

Zgodnie z celami rozporządzenia (UE) nr 910/2014 wybrano szereg norm, aby spełnić te specjalne wymogi. Przedmiotowe normy powinny odzwierciedlać utrwalone praktyki i być powszechnie uznawane w odpowiednich sektorach. Na przykład, ponieważ format W3C VCDM jest stosowany jako format odniesienia dla poświadczeń, w szczególności w sektorze edukacji, europejskie portfele tożsamości cyfrowej powinny również obsługiwać ten format, gdy dostępne są nowe profile w formacie W3C VCDM. W razie potrzeby normy te należy dostosować lub uzupełnić tak, aby zapewnić bezpieczeństwo i wiarygodność europejskich portfeli tożsamości cyfrowej przy jednoczesnym ułatwianiu interoperacyjności transgranicznej i efektywnego funkcjonowania rynku wewnętrznego.

(2) W przypadku każdego korzystania z portfela, które wymaga przedstawienia zdjęcia użytkownika portfela, portfel musi obsługiwać funkcjonalność selektywnego ujawniania, a ujawnianie musi znajdować się pod pełną kontrolą użytkownika. Aby chronić możliwość podejmowania decyzji o ujawnieniu oraz zdjęcie przed niezamierzonym lub nieuprawnionym żądaniem ujawnienia, projekt architektury europejskich portfeli tożsamości cyfrowej powinien przewidywać mechanizmy ostrzegania i rejestrowanie wszystkich transakcji dotyczących zdjęcia. W celu zapewnienia, aby użytkownik portfela był świadomy udostępniania danych biometrycznych, ostrzeżenia powinny wskazywać, że żądanie wiąże się z udostępnianiem danych biometrycznych, i w szczególności wymagać od

([1]) Dz.U. L 257 z 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Zalecenie Komisji (UE) 2021/946 z dnia 3 czerwca 2021 r. w sprawie wspólnego unijnego zestawu narzędzi na potrzeby skoordynowanego podejścia do europejskich ram tożsamości cyfrowej (Dz.U. L 210 z 14.6.2021, s. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).
([3]) Rozporządzenie wykonawcze Komisji (UE) 2024/2977 z dnia 28 listopada 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do danych identyfikujących osobę i elektronicznych poświadczeń atrybutów wydawanych europejskim portfelom tożsamości cyfrowej (Dz.U. L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).
([4]) Rozporządzenie wykonawcze Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do integralności i podstawowych funkcji europejskich portfeli tożsamości cyfrowej (Dz.U. L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).
([5]) Rozporządzenie wykonawcze Komisji (UE) 2024/2980 z dnia 28 listopada 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do notyfikowania Komisji w związku z ekosystemem europejskiego portfela tożsamości cyfrowej (Dz.U. L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).
([6]) Rozporządzenie wykonawcze Komisji (UE) 2024/2982 z dnia 28 listopada 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do protokołów i interfejsów, które mają być obsługiwane przez europejskie ramy tożsamości cyfrowej (Dz.U. L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

użytkownika potwierdzenia ujawnienia. W przypadku gdy strona ufająca przetwarza zdjęcie w celu jednoznacznej identyfikacji osoby fizycznej lub potwierdzenia deklarowanej tożsamości tej osoby, zastosowanie mają art. 6 i 9 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 ([7]), a także wszystkie inne wymogi tego rozporządzenia, w tym wymóg, aby przetwarzanie zdjęcia przez strony ufające ograniczało się do tego, co jest niezbędne do zamierzonego wykorzystania. Informacje o zamierzonym wykorzystaniu należy przekazać użytkownikowi portfela wraz z wnioskiem o ujawnienie, przy użyciu jasnego i zrozumiałego języka. Aby należycie uwzględnić wrażliwość danych biometrycznych, użytkownik portfela powinien wyraźnie i specjalnie potwierdzić ujawnienie zdjęcia. Milczenia lub domyślnie zaznaczonych pól wyboru nie należy uznawać za potwierdzenie przez użytkownika portfela. Wyraźne potwierdzenie użytkownika portfela powinno stanowić zabezpieczenie techniczne i samo w sobie nie powinno stanowić podstawy prawnej przetwarzania. Jak określono w art. 9 ust. 4 rozporządzenia (UE) 2016/679 „państwa członkowskie mogą zachować lub wprowadzić dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia".

(3) Aby zapewnić państwom członkowskim wystarczająco dużo czasu na dostosowanie procedur krajowych, zdjęcie użytkownika portfela może stanowić część obowiązkowych danych identyfikujących osobę w przypadku osoby fizycznej dopiero od dnia 11 sierpnia 2028 r. W przypadku gdy obrazy te są pozyskiwane z istniejących dokumentów tożsamości, takich jak dowody osobiste lub paszporty, zastosowanie mają właściwe wymogi określone odpowiednio w rozporządzeniach Rady (UE) 2025/1208 ([8]) lub (WE) nr 2252/2004 ([9]).

(4) W rozporządzeniu (UE) nr 910/2014 wymaga się, aby portfele były w stanie wyświetlać unijny znak zaufania dla portfela tożsamości cyfrowej jako weryfikowalne i rozpoznawalne wskazanie, że portfel zapewniono zgodnie z rozporządzeniem. Stosowanie takiego znaku zaufania przyczyni się do skutecznego funkcjonowania rynku wewnętrznego, zagwarantuje uczciwą konkurencję i będzie chronić interesy konsumentów. Aby umożliwić stosowanie takiego znaku zaufania, należy określić jego cechy wizualne i techniczne.

(5) Jak określono w art. 12b rozporządzenia (UE) nr 910/2014, strażnicy dostępu mają umożliwiać dostawcom europejskich portfeli tożsamości cyfrowej i wydawcom zgłoszonych środków identyfikacji elektronicznej efektywną interoperacyjność z tym samym systemem operacyjnym, sprzętem lub funkcjami oprogramowania oraz, do celów interoperacyjności, dostęp do nich. Taką efektywną interoperacyjność i dostęp zapewnia się bezpłatnie i niezależnie od tego, czy te funkcje sprzętu lub oprogramowania stanowią część systemu operacyjnego, są dostępne dla tego strażnika dostępu lub są przez niego wykorzystywane podczas świadczenia przedmiotowych usług. Ponieważ wszystkie rozwiązania w zakresie portfela powinny obsługiwać wspólny zestaw protokołów i interfejsów w celu zapewnienia użyteczności, bezpieczeństwa i interoperacyjności we wszystkich państwach członkowskich, strażnicy dostępu powinni umożliwiać działanie systemu operacyjnego, funkcji sprzętu lub oprogramowania niezbędnych do wdrożenia protokołów i interfejsów określonych w załączniku XII do niniejszego rozporządzenia. W tym kontekście w internetowych przepływach między urządzeniami, zarówno w odniesieniu do kontroli fizycznej kontroli zbliżeniowej, jak i przesyłania danych między tymi dwoma urządzeniami, strażnicy dostępu powinni preferować lokalny kanał komunikacyjny, którego funkcjonowanie umożliwia wersja 2.3 specyfikacji protokołu Client to Authenticator (CTAP) ([10]), w stosunku do korzystania z usług hybrydowego tunelu CTAP.

(6) Aby zapewnić państwom członkowskim, dostawcom certyfikatów rejestracji strony ufającej portfela i dostawcom portfela wystarczająco dużo czasu na umożliwienie jednostkom portfela uwierzytelniania i walidacji certyfikatów rejestracji strony ufającej portfela, wymóg ten powinien mieć zastosowanie dopiero od dnia 11 sierpnia 2028 r.

(7) Rozporządzenie (UE) 2016/679 oraz – w stosownych przypadkach – dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady ([11]) mają zastosowanie do wszystkich czynności przetwarzania danych osobowych na podstawie niniejszego rozporządzenia.

([7]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([8]) Rozporządzenie Rady (UE) 2025/1208 z dnia 12 czerwca 2025 r. w sprawie poprawy zabezpieczeń dowodów osobistych obywateli Unii i dokumentów pobytowych wydawanych obywatelom Unii i członkom ich rodzin korzystającym z prawa do swobodnego przemieszczania się (Dz.U. L, 2025/1208, 20.6.2025, ELI: http://data.europa.eu/eli/reg/2025/1208/oj).

([9]) Rozporządzenie Rady (WE) nr 2252/2004 z dnia 13 grudnia 2004 r. w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez państwa członkowskie (Dz.U. L 385 z 29.12.2004, s. 1, ELI: http://data.europa.eu/eli/reg/2004/2252/oj).

([10]) Norma zaproponowana przez Fido Alliance, protokół „Client to Authenticator" (CTAP), 26 lutego 2026 r.

([11]) 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 (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(8) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([12]) skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 17 kwietnia 2026 r. ([13])

(9) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią komitetu ustanowionego na mocy art. 48 rozporządzenia (UE) 910/2014,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Zmiany w rozporządzeniu wykonawczym (UE) 2024/2977

W rozporządzeniu wykonawczym (UE) 2024/2977 wprowadza się następujące zmiany:

1) dodaje się art. 3a w brzmieniu:

„*Artykuł 3a*

Ochrona zdjęcia

1. W uzupełnieniu wymogów informacyjnych określonych w rozporządzeniu (UE) 2016/679 dostawcy portfela zapewniają, aby dostarczane przez nich rozwiązania w zakresie portfela wydawały ostrzeżenia dla użytkowników portfela, w przypadku gdy strony ufające żądają ujawnienia zdjęcia, wskazując, że dane żądanie wiąże się z udostępnianiem danych biometrycznych i wymaga potwierdzenia selektywnego ujawnienia zdjęcia.

2. Na potrzeby wdrożenia selektywnego ujawniania zdjęcia stronie ufającej portfela dostawcy portfela zapewniają, aby rozwiązania w zakresie portfela wymagały od użytkownika portfela wyraźnego i specjalnego potwierdzenia przedstawienia zdjęcia.

3. Zdjęcie nie może być jest zachowywane przez strony ufające portfela, chyba że jego przetwarzanie jest niezbędne do celów identyfikacji i uwierzytelniania zgodnie z unijnym prawem o ochronie danych lub jeżeli jest to przewidziane w prawie Unii lub prawie krajowym, zgodnie z unijnym prawem o ochronie danych. Zdjęcia nie można przekazywać państwom trzecim lub organizacjom międzynarodowym, chyba że zezwala na to unijne prawo o ochronie danych.";

2) art. 4 ust. 1 otrzymuje brzmienie:

„1. Elektroniczne poświadczenia atrybutów wydawane do jednostek portfela muszą być zgodne z co najmniej jedną z norm określonych w załączniku II do rozporządzenia wykonawczego (UE) 2024/2979.";

3) art. 5 ust. 4 lit. b) otrzymuje brzmienie:

„b) w przypadku gdy poświadczenie jednostki portfela, do której wydano dane identyfikujące osobę, zostało unieważnione;";

4) załącznik zastępuje się tekstem znajdującym się w załączniku I do niniejszego rozporządzenia.

([12]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([13]) EDPS Formal comments on the draft Implementing Regulation as regards applicable standards and specifications and correcting Implementing Regulation (EU) 2024/2980 [formalne uwagi EIOD dotyczące projektu rozporządzenia wykonawczego Komisji odnośnie do mających zastosowanie norm i specyfikacji oraz sprostowania rozporządzenia wykonawczego (UE) 2024/2980]. | Europejski Inspektor Ochrony Danych.

Artykuł 2

Zmiany w rozporządzeniu wykonawczym (UE) 2024/2979

W rozporządzeniu wykonawczym (UE) 2024/2979 wprowadza się następujące zmiany:

1) w art. 3 uchyla się ust. 2;

2) art. 5 ust. 1 lit. a) otrzymuje brzmienie:

„a) wykonywały operacje kryptograficzne portfela wykorzystujące aktywa krytyczne, które nie są wymagane do uwierzytelniania użytkownika portfela, przechowywane w bezpiecznym urządzeniu kryptograficznym portfela wyłącznie w przypadkach, gdy aplikacje te skutecznie uwierzytelniły użytkowników portfela;";

3) dodaje się art. 5a w brzmieniu:

„*Artykuł 5a*

Mechanizmy kryptograficzne

Do celów art. 4 ust. 2 dostawcy portfela stosują wyłącznie mechanizmy kryptograficzne, o których mowa w załączniku Ia.";

4) w art. 6 wprowadza się następujące zmiany:

a) ust. 1 otrzymuje brzmienie:

„1. Dostawcy portfela wydają poświadczenia jednostki portfela dla każdej jednostki portfela. Dostawcy portfela podpisują lub opatrują pieczęcią poświadczenia jednostki portfela w sposób umożliwiający walidację podpisów lub pieczęci za pomocą certyfikatu wymienionego w wykazie zgodnie z sekcją 2 pkt 1 lit. h) załącznika II do rozporządzenia wykonawczego (UE) 2024/2980.";

b) ust. 2 otrzymuje brzmienie:

„2. Dostawcy portfela zapewniają zgodność poświadczeń jednostki portfela, o których mowa w ust. 1, ze specyfikacjami technicznymi określonymi w załączniku Ib.";

c) ust. 3 lit. b) otrzymuje brzmienie:

„b) zapewniają użytkownikom portfela bezpieczne mechanizmy identyfikacji i uwierzytelniania, które są niezależne od jednostek portfela;";

5) art. 9 ust. 2 lit. b) otrzymuje brzmienie:

„b) imię i nazwisko lub nazwę, dane kontaktowe oraz niepowtarzalny identyfikator odpowiedniej strony ufającej portfela i państwo członkowskie, w którym strona ta ma siedzibę;";

6) w art. 10 ust. 1 otrzymuje brzmienie:

„1. Dostawcy portfela zapewniają, aby elektroniczne poświadczenia atrybutów wydawane zgodnie ze specyfikacjami technicznymi mającymi zastosowanie do wspólnych wbudowanych reguł ujawniania określonymi w załączniku III mogły być przetwarzane przez jednostki portfela, które dostarczają.";

7) w art. 12 wprowadza się następujące zmiany:

a) ust. 2 lit. c) otrzymuje brzmienie:

„c) składanie podpisów lub pieczęci zgodnie co najmniej z obowiązkowym formatem podpisu lub pieczęci, o którym mowa w załączniku IV;";

b) ust. 3 otrzymuje brzmienie:

„3. Aplikacje służące do składania podpisu mogą być zintegrowane z instancjami portfela albo mieć względem nich charakter zewnętrzny.";

c) dodaje się ustęp w brzmieniu:

„4. Aplikacje służące do składania podpisu wykorzystywane przez jednostki portfela obsługują co najmniej interfejs programowania aplikacji, o którym mowa w załączniku IV.";

8) w art. 14 uchyla się ust. 1;

9) dodaje się art. 14a w brzmieniu:

„*Artykuł 14a*

Unijny znak zaufania dla portfela tożsamości cyfrowej

1. Dostawcy portfela zapewniają, aby jednostki portfela wyświetlały unijny znak zaufania dla portfela tożsamości cyfrowej. Unijny znak zaufania dla portfela tożsamości cyfrowej ma formę określoną w załącznikach VI i VII.

2. Dostawcy portfela zapewniają, aby jednostki portfela umożliwiały użytkownikom portfela dostęp do informacji pozwalających im zweryfikować status certyfikacji danego rozwiązania w zakresie portfela. W tym celu dostawcy portfela zapewniają, aby po rejestracji rozwiązania w zakresie portfela odpowiednie jednostki portfela zawierały adresy URL podane przez Komisję Europejską na potrzeby takiej weryfikacji. Dostawcy portfela zapewniają swoim jednostkom portfela dostęp do danych dotyczących unijnego znaku zaufania dla portfela tożsamości cyfrowej, które są zgodne ze specyfikacjami technicznymi określonymi w załączniku VIII.

3. Kolorami referencyjnymi unijnego znaku zaufania dla portfela tożsamości cyfrowej są kolory Pantone nr 661 i Pantone nr 116; lub kolory niebieski (100 % cyjanu + 67 % magenty + 0 % żółtego + 40 % czarnego) i żółty (0 % cyjanu + 20 % magenty + 100 % żółtego + 0 % czarnego) w przypadku stosowania druku czterokolorowego; w przypadku stosowania kolorów RGB kolorami referencyjnymi są niebieski (0 czerwony + 51 zielony + 153 niebieski) i żółty (255 czerwony + 204 zielony + 0 niebieski).

4. Jedynie w przypadku gdy użycie koloru nie jest możliwe, można stosować czarno-biały unijny znak zaufania dla portfela tożsamości cyfrowej, jak określono w załączniku VII.

5. W przypadku gdy unijny znak zaufania dla portfela tożsamości cyfrowej umieszczany jest na ciemnym tle, można zastosować go w negatywie z użyciem tego samego koloru tła. W przypadku gdy unijny znak zaufania dla portfela tożsamości cyfrowej stosowany jest w kolorze na kolorowym tle, co sprawia, że nie jest on dobrze widoczny, można otoczyć unijny znak zaufania dla portfela tożsamości cyfrowej zewnętrzną linią odgraniczającą, aby zwiększyć kontrast z kolorami tła.

6. Minimalny rozmiar unijnego znaku zaufania dla portfela tożsamości cyfrowej wynosi 64 × 85 pikseli w rozdzielczości 150 dpi.

7. Dostawcy portfela zapewniają, aby unijny znak zaufania dla portfela tożsamości cyfrowej był używany w sposób umożliwiający wyraźne wskazanie jednostki portfela, do której się odnosi. Unijny znak zaufania dla portfela tożsamości cyfrowej może być powiązany z elementami graficznymi lub tekstowymi wyraźnie wskazującymi jednostkę portfela, dla której jest używany, pod warunkiem że nie zmieniają one jego rozpoznawalności jako unijnego znaku zaufania dla portfela tożsamości cyfrowej ani nie zmieniają powiązania z wykazem certyfikowanych europejskich portfeli tożsamości cyfrowej, o którym mowa w art. 5d rozporządzenia (UE) nr 910/2014.

8. W przypadku unieważnienia poświadczenia jednostki portfela dostawcy portfela zapewniają, aby unijny znak zaufania dla portfela tożsamości cyfrowej nie był już wyświetlany przez odpowiednią jednostkę portfela.”;

10) dodaje się załączniki Ia i Ib zgodnie z załącznikami II i III do niniejszego rozporządzenia;

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

12) załącznik III zastępuje się załącznikiem V do niniejszego rozporządzenia;

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

14) uchyla się załącznik V;

15) tekst znajdujący się w załączniku VII do niniejszego rozporządzenia wprowadza się jako załącznik VI;

16) tekst znajdujący się w załączniku VIII do niniejszego rozporządzenia wprowadza się jako załącznik VII;

17) tekst znajdujący się w załączniku IX do niniejszego rozporządzenia wprowadza się jako załącznik VIII.

Artykuł 3

Zmiany w rozporządzeniu wykonawczym (UE) 2024/2980

W rozporządzeniu wykonawczym (UE) 2024/2980 wprowadza się następujące zmiany:

1) art. 5 pkt 2 otrzymuje brzmienie:

„2. W stosownych przypadkach Komisja ustanawia, prowadzi i publikuje wykaz zawierający notyfikowane przez państwa członkowskie informacje na temat dostawców portfela, dostawców danych identyfikujących osobę, dostawców certyfikatów dostępu strony ufającej portfela i dostawców certyfikatów rejestracji strony ufającej portfela, o których mowa w załączniku II sekcje 2, 3, 4 i 5.";

2) w załączniku II do rozporządzenia wykonawczego (UE) 2024/2980 wprowadza się zmiany zgodnie z załącznikiem X do niniejszego rozporządzenia.

Artykuł 4

Zmiany w rozporządzeniu wykonawczym (UE) 2024/2982

W rozporządzeniu wykonawczym (UE) 2024/2982 wprowadza się następujące zmiany:

1) art. 1 pkt 2 otrzymuje brzmienie:

„2) prezentacji atrybutów danych identyfikujących osobę i elektronicznych poświadczeń atrybutów stronom ufającym portfela;";

2) w art. 3 wprowadza się następujące zmiany:

a) pkt 1 otrzymuje brzmienie:

„1) uwierzytelniały i walidowały certyfikaty dostępu strony ufającej portfela w przypadku interakcji ze stronami ufającymi portfela, nie powierzając wykonania tych procesów przeglądarce systemu operacyjnego lub innej aplikacji pośredniczącej;";

b) uchyla się pkt 2;

c) pkt 3 otrzymuje brzmienie:

„3) uwierzytelniały i walidowały żądania przekazane za pomocą certyfikatów dostępu strony ufającej portfela;";

d) pkt 4 otrzymuje brzmienie:

„4) uwierzytelniały i walidowały certyfikat rejestracji strony ufającej portfela;";

e) pkt 5 otrzymuje brzmienie:

„5) wyświetlały użytkownikom portfela informacje zawarte w certyfikatach dostępu strony ufającej portfela;";

f) uchyla się pkt 8;

g) pkt 9 otrzymuje brzmienie:

„9) nie przedstawiały stronom ufającym portfela żadnych żądanych atrybutów do czasu zakończenia następujących etapów:

a) weryfikacji, czy wbudowane reguły ujawniania zostały przetworzone w jednostce portfela zgodnie z art. 10 rozporządzenia wykonawczego (UE) 2024/2979;

b) weryfikacji, czy użytkownicy portfela zatwierdzili prezentację częściowo lub w całości.";

3) art. 4 ust. 1 otrzymuje brzmienie:

„1. Dostawcy portfela dopilnowują, aby rozwiązania w zakresie portfela obsługiwały protokoły i interfejsy określone w załączniku I na potrzeby wydawania danych identyfikujących osobę i elektronicznych poświadczeń atrybutów jednostkom portfela.";

4) w art. 5 wprowadza się następujące zmiany:

   a) ust. 1 i 2 otrzymują brzmienie:

      „1. Dostawcy portfela zapewniają, aby rozwiązania w zakresie portfela obsługiwały protokoły i interfejsy do celów prezentacji atrybutów stronom ufającym portfela, zdalnie i, w stosownych przypadkach, zbliżeniowo, zgodnie ze specyfikacjami technicznymi określonymi w załączniku II.

      2. Dostawcy portfela dopilnowują, aby – na wniosek użytkowników – jednostki portfela odpowiadały na skutecznie uwierzytelnione i zwalidowane żądania stron ufających portfela, o których mowa w art. 3, zgodnie ze specyfikacjami technicznymi określonymi w załączniku II.";

   b) uchyla się ust. 5;

5) art. 8 otrzymuje brzmienie:

   „*Artykuł 8*

   Wejście w życie

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

   Art. 3 ust. 4 stosuje się od dnia 11 sierpnia 2028 r.

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

6) uchyla się załącznik;

7) tekst zamieszczony w załączniku XI do niniejszego rozporządzenia dodaje się jako załącznik I;

8) tekst zamieszczony w załączniku XII do niniejszego rozporządzenia dodaje się jako załącznik II.

Artykuł 5

Wejście w życie

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 15 lipca 2026 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

ZAŁĄCZNIK I

„ZAŁĄCZNIK

Specyfikacje techniczne dotyczące danych identyfikujących osobę, o których mowa w art. 3 ust. 3

1. Sekcja 1: Zbiór danych identyfikujących osobę fizyczną

Tabela 1

Obowiązkowe dane identyfikujące osobę w przypadku osoby fizycznej na potrzeby selektywnego ujawniania

Identyfikator danych	Definicja
`family_name`	Aktualne nazwisko(-a) użytkownika, którego dotyczą dane identyfikujące osobę.
`given_name`	Aktualne imię (imiona), w tym, w stosownych przypadkach, drugie imię (imiona) użytkownika, którego dotyczą dane identyfikujące osobę.
`birth_date`	Dzień, miesiąc i rok urodzenia użytkownika, którego dotyczą dane identyfikujące osobę.
`birth_place`	Państwo zgodnie z kodem państwa alpha-2 według normy ISO 3166-1 lub stan, prowincja, powiat, obszar lokalny, gmina, miasto, miejscowość lub wieś urodzenia użytkownika, do którego odnoszą się dane identyfikujące osobę.
`nationality`	Co najmniej jeden kod państwa alpha-2 według normy ISO 3166-1, odzwierciedlający obywatelstwo użytkownika, którego dotyczą dane identyfikujące osobę.
`portrait`	Z wyjątkiem sytuacji gdy użytkownik jednoznacznie zrezygnuje, w stosownych przypadkach, wizerunek twarzy użytkownika, którego dotyczą dane identyfikujące osobę, zgodny z wymogami dotyczącymi jakości pełnego wizerunku twarzy w pozycji frontalnej określonymi w normie ISO/IEC 39794-5 lub na potrzeby kompatybilności wstecznej w normie ISO/IEC 19794-5, pkt 8.2, 8.3 i 8.4, przedstawiony w formie zakodowanych danych wizerunku bez nagłówków lub bloków określonych w pkt 5 normy ISO/IEC 19794-5, z wyjątkiem samych danych obrazu (JPEG), ma zastosowanie od dnia 11 sierpnia 2028 r.

— Państwa członkowskie mogą postanowić, że użytkownik ma możliwość odmówić umieszczenia zdjęcia w danych identyfikujących osobę.

— Państwa członkowskie zapewniają, aby selektywne ujawnianie miało zastosowanie do każdego identyfikatora danych, w tym do zdjęcia.

— W przypadku gdy data urodzenia osoby fizycznej nie jest znana, państwa członkowskie wybierają odpowiednie wartości zgodne ze specyfikacjami określonymi w sekcjach 4.1 lub 4.2 niniejszego załącznika (w zależności od przypadku).

— W przypadku gdy obywatelstwo osoby fizycznej jest nieznane, państwa członkowskie stosują wartość »QU«.

— W przypadku gdy osoba fizyczna nie posiada obywatelstwa, państwa członkowskie stosują wartość »QS«.

— W przypadku odmowy umieszczenia zdjęcia wyrażonej przez użytkownika, państwa członkowskie ustawiają wartość jako pustą.

Tabela 2

Opcjonalne dane identyfikujące osobę w przypadku osoby fizycznej na potrzeby selektywnego ujawniania

Identyfikator danych	Definicja
resident_address	Pełny adres zamieszkania użytkownika, którego dotyczą dane identyfikujące osobę, pod którym użytkownik ten obecnie przebywa lub można się z nim skontaktować (ulica, numer domu, miasto itp.).
resident_country	Kraj, w którym obecnie zamieszkuje użytkownik, którego dotyczą dane identyfikujące osobę, wyrażony jako kod państwa alpha-2 według normy ISO 3166-1.
resident_state	Stan, prowincja, powiat lub obszar lokalny aktualnego zamieszkania użytkownika, którego dotyczą dane identyfikujące osobę.
resident_city	Gmina, miasto lub wieś aktualnego zamieszkania użytkownika, którego dotyczą dane identyfikujące osobę.
resident_postal_code	Kod pocztowy miejsca aktualnego zamieszkania użytkownika, którego dotyczą dane identyfikujące osobę.
resident_street	Nazwa ulicy, przy której aktualnie mieszka użytkownik, którego dotyczą dane identyfikujące osobę, w tym numer domu i wszelkie informacje uzupełniające.
personal_administrative_-number	Wartość przypisana użytkownikowi, którego dotyczą dane identyfikujące osobę, która jest niepowtarzalna wśród wszystkich osobistych numerów administracyjnych wydanych przez dostawcę danych identyfikujących osobę. W przypadku gdy państwa członkowskie zdecydują się na włączenie tego atrybutu, mają obowiązek opisać w swoich systemach identyfikacji elektronicznej, w ramach których wydawane są dane identyfikujące osobę, politykę, którą stosują do wartości tego atrybutu, w tym, w stosownych przypadkach, szczególne warunki przetwarzania tej wartości.
family_name_birth	Nazwisko (nazwiska) użytkownika, którego dotyczą dane identyfikujące osobę, w momencie urodzenia.
given_name_birth	Imię (imiona), w tym drugie imię (imiona) użytkownika, którego dotyczą dane identyfikujące osobę, w momencie urodzenia.
sex	Dopuszcza się jedną z następujących wartości: 0 = nieznana; 1 = mężczyzna; 2 = kobieta; 3 = inna; 4 = osoba interseksualna; 5 = różnorodna; 6 = otwarta; 9 = nie dotyczy. W odniesieniu do wartości 0, 1, 2 i 9 stosuje się normę ISO/IEC 5218.
email_address	Adres poczty elektronicznej użytkownika, którego dotyczą dane identyfikujące osobę [zgodny z formatem RFC 5322 ([1])].

Identyfikator danych	Definicja
`mobile_phone_number`	Numer telefonu komórkowego użytkownika, którego dotyczą dane identyfikujące osobę, rozpoczynający się do symbolu »+« jako kodu prefiksu międzynarodowego i kodu państwa, po którym występują tylko cyfry.

([1]) P. Resnick, Ed., »Internet Message Format«, RFC 5322, październik 2008 r.

2. Sekcja 2: Zbiór danych identyfikujących osobę prawną

Tabela 3

Obowiązkowe dane identyfikujące osobę w przypadku osoby prawnej

Identyfikator danych
aktualna nazwa prawna
niepowtarzalny identyfikator zbudowany przez wysyłające państwo członkowskie zgodnie ze specyfikacjami technicznymi do celów transgranicznej identyfikacji, który jest możliwie jak najtrwalszy w czasie.

— W przypadku gdy identyfikator danych nie jest znany danej osobie lub nie może zostać wydany w inny sposób jako część zbioru danych identyfikujących osobę, państwa członkowskie powinny zastosować wartość atrybutu odpowiednią do danej sytuacji.

Tabela 4

Opcjonalne dane identyfikujące osobę w przypadku osoby prawnej

Identyfikator danych
aktualny adres
numer identyfikacyjny VAT
numer identyfikacji podatkowej
niepowtarzalny identyfikator europejski, o którym mowa w dyrektywie Parlamentu Europejskiego i Rady (UE) 2017/1132 ([1])
identyfikator podmiotu prawnego (LEI), o którym mowa w rozporządzeniu wykonawczym Komisji (UE) 2022/1860 ([2])
numer rejestracyjny i identyfikacyjny przedsiębiorcy (EORI), o którym mowa w rozporządzeniu wykonawczym Komisji (UE) nr 1352/2013 ([3])
numer akcyzowy określony w art. 2 pkt 12 rozporządzenia Rady (UE) nr 389/2012 ([4])

([1]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/1132 z dnia 14 czerwca 2017 r. w sprawie niektórych aspektów prawa spółek (Dz.U. L 169 z 30.6.2017, s. 46, ELI: http://data.europa.eu/eli/dir/2017/1132/oj).

([2]) Rozporządzenie wykonawcze Komisji (UE) 2022/1860 z dnia 10 czerwca 2022 r. ustanawiające, na potrzeby stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 648/2012, wykonawcze standardy techniczne w odniesieniu do standardów, formatów, częstotliwości i metod oraz zasad dokonywania zgłoszeń (Dz.U. L 262 z 7.10.2022, s. 68, ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj).

([3]) Rozporządzenie wykonawcze Komisji (UE) nr 1352/2013 z dnia 4 grudnia 2013 r. ustanawiające formularze przewidziane w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 608/2013 w sprawie egzekwowania praw własności intelektualnej przez organy celne (Dz.U. L 341 z 18.12.2013, s. 10, ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj).

([4]) Rozporządzenie Rady (UE) nr 389/2012 z dnia 2 maja 2012 r. w sprawie współpracy administracyjnej w dziedzinie podatków akcyzowych oraz uchylenia rozporządzenia (WE) nr 2073/2004 (Dz.U. L 121 z 8.5.2012, s. 1, ELI: http://data.europa.eu/eli/reg/2012/389/oj).

3. Sekcja 3: Zbiór metadanych dotyczących danych identyfikujących osobę

Tabela 5

Metadane dotyczące danych identyfikujących osobę

Identyfikator danych	Definicja	Występowanie
`issuing_authority`	Nazwa organu administracyjnego, który wydał dane identyfikujące osobę, lub kod kraju alpha-2 danego państwa członkowskiego zgodnie z normą ISO 3166, jeżeli nie istnieje odrębny organ uprawniony do wydawania danych identyfikujących osobę.	obowiązkowe
`issuing_country`	Kod państwa alpha-2, jak określono w normie ISO 3166-1, państwa lub terytorium dostawcy danych identyfikujących osobę.	obowiązkowe
`expiry_date`	Data (i w miarę możliwości godzina) upływu administracyjnego okresu ważności danych identyfikujących osobę.	opcjonalne
`document_number`	Numer danych identyfikujących osobę nadany przez dostawcę danych identyfikujących osobę.	opcjonalne
`issuing_jurisdiction`	Kod podziału terytorialnego państwa jurysdykcji, w którym wydano dane identyfikujące osobę, zgodnie z normą ISO 3166-2:2020, pkt 8. Pierwsza część kodu jest taka sama jak wartość dla państwa wydającego.	opcjonalne
`issuance_date`	Data, i w miarę możliwości godzina, rozpoczęcia biegu administracyjnego okresu ważności danych identyfikujących osobę.	opcjonalne

4. Sekcja 4: Kodowanie atrybutów danych identyfikujących osobę fizyczną

— Dane identyfikujące osobę fizyczną wydaje się zgodnie z normami określonymi w załączniku II do rozporządzenia wykonawczego (UE) 2024/2979, pkt 5 (format SD-JWT VC) i 6 (format ISO/IEC-mdoc), w zakresie mającym zastosowanie do elektronicznych poświadczeń atrybutów. Pkt 5.2.2, 5.2.4, 5.2.5, EAA-6.1-03, 6.2.2, 6.2.3, 6.2.4 i 6.2.5 nie mają zastosowania.

— Kodowanie danych identyfikujących osobę fizyczną musi być zgodne ze specyfikacjami technicznymi zawartymi w sekcjach 4.1 i 4.2 niniejszego załącznika.

4.1. Kodowanie danych identyfikujących osobę fizyczną w formacie ISO/IEC-mdoc

— Typem poświadczenia danych identyfikujących osobę w formacie ISO/IEC mdoc jest »eu.europa.ec.eudi.pid.1«. Identyfikator przestrzeni nazw atrybutów danych identyfikujących osobę określonych w niniejszym załączniku to »eu.europa.ec.eudi.pid.1«.

— W przypadku gdy dane identyfikujące osobę obejmują dane, w odniesieniu do których w niniejszym załączniku nie określono identyfikatorów danych, dane te określa się w obrębie krajowej przestrzeni nazw danych identyfikujących osobę, w której stosuje się format ogólny eu.europa.ec.eudi.pid.[kod państwa ISO 3166-1 alpha-2 lub kod regionu ISO 3166-2], po którym następuje opcjonalna kropka i numer wersji.

— W przypadku stosowania krajowej przestrzeni nazw jej schemat, w tym wszystkie identyfikatory danych, ich definicje, występowanie i formaty kodowania, publikuje się zgodnie z art. 8 rozporządzenia wykonawczego Komisji (UE) 2025/1569 ([1]).

— Dane identyfikujące osobę oraz ich metadane określone w sekcjach 1 i 3 niniejszego załącznika włącza się do elementów danych identyfikujących osobę w rozumieniu specyfikacji formatu ISO/IEC mdoc.

— Element deviceKey w ramach elementu deviceKeyInfo typu MobileSecurityObject zawiera klucz publiczny.

— Ten klucz publiczny odpowiada kluczowi prywatnemu przechowywanemu w bezpiecznym urządzeniu kryptograficznym portfela (WSCD) użytkownika portfela.

— Nagłówek chroniony podpisu cyfrowego CB-AdES podpisującego dane identyfikujące osobę w formacie ISO/IEC-mdoc zawiera parametry nagłówka x5u i x5t – oba określone w RFC 9360 ([2]).

— Algorytmem skrótu stosowanym w parametrze nagłówka x5t jest SHA-256.

— Wymogi dotyczące kodowania danych identyfikujących osobę w formacie ISO/IEC-mdoc określono w tabeli 6:

Tabela 6

Wymagania dotyczące kodowania danych identyfikujących osobę w formacie ISO/IEC-mdoc

Identyfikator danych	Identyfikator atrybutu	Format kodowania
family_name	family_name	tstr
given_name	given_name	tstr
birth_date	birth_date	full-date
birth_place	place_of_birth	place_of_birth
nationality	nationality	nationalities
resident_address	resident_address	tstr
resident_country	resident_country	tstr
resident_state	resident_state	tstr
resident_city	resident_city	tstr
resident_postal_code	resident_postal_code	tstr
resident_street	resident_street	tstr
personal_administrative_number	personal_administrative_number	tstr
portrait	portrait	bstr
family_name_birth	family_name_birth	tstr
given_name_birth	given_name_birth	tstr
sex	sex	uint

([1]) Rozporządzenie wykonawcze Komisji (UE) 2025/1569 z dnia 29 lipca 2025 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do kwalifikowanych elektronicznych poświadczeń atrybutów oraz elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu (Dz.U. L, 2025/1569, 30.7.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([2]) J. Schaad, »CBOR Object Signing and Encryption (COSE): Header Parameters for Carrying and Referencing X.509 Certificates«(https://datatracker.ietf.org/doc/rfc9360/).

Identyfikator danych	Identyfikator atrybutu	Format kodowania
email_address	email_address	tstr
mobile_phone_number	mobile_phone_number	tstr
expiry_date	expiry_date	tdate lub full-date
issuing_authority	issuing_authority	tstr
issuing_country	issuing_country	tstr
document_number	document_number	tstr
issuing_jurisdiction	issuing_jurisdiction	tstr
issuance_date	issuance_date	tdate lub full-date

— Przy notacji formatu kodowania atrybutów określonego w tabeli 6 stosuje się typy reprezentacji określone w RFC 8610 ([3]), z następującymi dodatkowymi wymogami:

a) tstr koduje się w UTF-8;

b) tstr obsługuje pełny zakres Unicode;

c) tstr ma maksymalną długość 150 znaków;

d) datę koduje się zgodnie z RFC 8943 ([4]);

e) pełną datę interpretuje się jako #6.1004(tstr), przy czym tag 1004 określono w RFC 8943;

f) atrybut tdate zawiera ciąg znaków daty i godziny określony w RFC 3339 ([5]);

g) atrybut full-date zawiera ciąg znaków full-date określony w RFC 3339, zgodnie z RFC 8943;

h) o ile nie wskazano inaczej, reprezentacja daty w atrybutach:

— nie wykorzystuje ułamków sekund;

— nie wykorzystuje lokalnego przesunięcia względem UTC, a przesunięcie czasowe określone w RFC 3339 ustawia się jako »Z«;

i) liczbę całkowitą o głównych typach 0 i 1 koduje się w możliwie najmniejszej reprezentacji, zgodnie z RFC 8949 ([6]), pkt 4.2;

j) place_of_birth zawiera co najmniej jedną z następujących par klucz–wartość: »country«, »region«, lub »locality«;

k) wyrażenie długości w bstr, tstr, tablicy lub mapie musi być możliwie najkrótsze, jak określono w RFC 8949, pkt 4.2;

([3]) C. Vigano and H. Birkholz, »Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures«, RFC 8610, czerwiec 2019 r.
([4]) M. Jones, A. Nadalin and J. Richter, »Concise Binary Object Representation (CBOR) Tags for Date«, RFC 8943, listopad 2020 r.
([5]) G. Klyne and C. Newman, »Date and Time on the Internet: Timestamps«, RFC 3339, lipiec 2002 r.
([6]) C. Bormann i P. Hoffman, »Concise Binary Object Representation (CBOR)«, RFC 8949, grudzień 2020 r.

l) atrybut obywatelstwa koduje się jako tablicę kodów państw alpha-2 zgodnie z normą ISO 3166-1. Jeżeli stosuje się notację CDDL, jak określono w RFC 8610, kodowanie tego atrybutu jest następujące:

— nationalities = [+ CountryCode];

— CountryCode = tstr; kod kraju alpha-2 określony w normie ISO 3166-1;

— w przypadku gdy użytkownik portfela, którego dotyczą dane identyfikujące osobę, ma wiele obywatelstw, a dostawca danych identyfikujących osobę poświadcza te obywatelstwa, dostawca danych identyfikujących osobę może uwzględnić wszystkie obywatelstwa w danych identyfikujących osobę;

— atrybut »place_of_birth« koduje się jako typ place_of_birth. Jeżeli stosuje się notację CDDL, jak określono w RFC 8610, kodowanie tego atrybutu jest następujące:

place_of_birth =

{

? 'country': tstr; pojedynczy kod państwa alpha-2 określony w normie ISO 3166-1

? 'region': tstr; nazwa stanu, prowincji, powiatu lub obszaru lokalnego

? 'locality': tstr; nazwa gminy, miasta, miejscowości lub wsi

}

4.2 Wymagania dotyczące kodowania danych identyfikujących osobę w formacie SD-JWT VC

— Dane identyfikujące osobę oraz ich metadane określone w niniejszej sekcji włącza się do danych identyfikujących osobę jako elementy danych w rozumieniu specyfikacji formatu SD-JWT VC.

— Wszystkie elementy danych zawarte w danych identyfikujących osobę, o których mowa w poprzednim tiret, podlegają selektywnemu ujawnianiu indywidualnie, z wyjątkiem tych elementów danych, które w formacie SD-JWT VC określono jako niepodlegające selektywnemu ujawnianiu.

— W tabeli 7 określono kodowanie nazw elementów danych, które są nazwami publicznymi.

— W tabeli 8 określono kodowanie nazw elementów danych, które są specyficzne dla danych identyfikujących osobę.

— Ciąg znaków JSON stosowany w danych identyfikujących osobę zakodowanych w SD-JWT VC koduje się w UTF-8 i obsługuje on pełny zakres Unicode, chyba że wyraźnie określono inaczej w tabeli 8 poniżej lub odniesieniach w niej zawartych.

— Elementy danych JWT nbf i exp, jak określono w RFC 7519 ([7]), wykorzystuje się do wyrażenia technicznego okresu ważności danych identyfikujących osobę zgodnych z formatem SD-JWT VC.

([7]) J. Jones i in., »JSON Web Token (JWT)«, RFC 7519, maj 2015 r.

— Dane identyfikujące osobę obejmują element danych cnf określony w RFC 7800 ([8]), który jest kluczem publicznym wygenerowanym z klucza prywatnego przechowywanego w WSCD jednostki portfela użytkowników.

— Nagłówek chroniony podpisu cyfrowego podpisującego dane identyfikujące osobę w formacie SD-JWT VC zawiera parametry nagłówka x5u i x5t#S256 określone w RFC 7515 ([9]).

Tabela 7

Wymagania dotyczące kodowania danych identyfikujących osobę w formacie SD-JWT VC przy użyciu nazw publicznych

Identyfikator danych	Identyfikator atrybutu	Format kodowania
`family_name`	`family_name`	ciąg znaków
`given_name`	`given_name`	ciąg znaków
`birth_date`	`birthdate`	ciąg znaków, ISO 8601-1, format RRRR-MM-DD
`birth_place`	`place_of_birth`	struktura JSON
`nationality`	`nationalities`	tablica ciągów znaków
`resident_address`	`address.formatted`	ciąg znaków
`resident_country`	`address.country`	ciąg znaków
`resident_state`	`address.region`	ciąg znaków
`resident_city`	`address.locality`	ciąg znaków
`resident_postal_code`	`address.postal_code`	ciąg znaków
`resident_street`	`address.street_address`	ciąg znaków
`family_name_birth`	`birth_family_name`	ciąg znaków
`given_name_birth`	`birth_given_name`	ciąg znaków
`email_address`	`email`	ciąg znaków
`mobile_phone_number`	`phone_number`	ciąg znaków
`portrait`	`picture`	ciąg znaków; adres URL danych zawierający wizerunek zakodowany w base64 w formacie JPEG

([8]) M. Jones i in., »Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)«, RFC 7800, kwiecień 2016 r.
([9]) M. Jones i in., »JSON Web Signature (JWS)«, RFC 7515, maj 2015 r.

Tabela 8

Wymagania dotyczące kodowania danych identyfikujących osobę w formacie SD-JWT VC przy użyciu nazw prywatnych

Identyfikator danych	Identyfikator atrybutu	Format kodowania
`expiry_date`	`date_of_expiry`	ciąg znaków, ISO 8601-1, format RRRR-MM-DD
`issuance_date`	`date_of_issuance`	ciąg znaków, ISO 8601-1, format RRRR-MM-DD
`personal_administrative_number`	`personal_administrative_number`	ciąg znaków
`sex`	`sex`	numer
`issuing_authority`	`issuing_authority`	ciąg znaków
`issuing_country`	`issuing_country`	ciąg znaków
`document_number`	`document_number`	ciąg znaków
`issuing_jurisdiction`	`issuing_jurisdiction`	ciąg znaków

— Podstawowym typem danych identyfikujących osobę jest »urn:eudi:pid:1« zawarty w elemencie danych vtc. Wszystkie dane identyfikujące osobę wykorzystują typy w przestrzeni nazw »urn:eudi:pid:«.

— W przypadku gdy dane identyfikujące osobę obejmują atrybuty, które nie są określone w niniejszym załączniku, atrybuty te definiuje się w ramach typu krajowego.

— W przypadku stosowania typu krajowego jego schemat, w tym wszystkie identyfikatory danych, ich definicje, występowanie i formaty kodowania definiuje się w schemacie, który jest publikowany zgodnie z art. 8 rozporządzenia wykonawczego (UE) 2025/1569.

5. Sekcja 5: Szczegółowe informacje dotyczące infrastruktury zaufania

Wykaz dostawców danych identyfikujących osobę udostępniony przez Komisję zgodnie z rozporządzeniem wykonawczym (UE) 2024/2980 umożliwia uwierzytelnianie danych identyfikujących osobę.”

ZAŁĄCZNIK II

„ZAŁĄCZNIK Ia

Mechanizmy kryptograficzne, o których mowa w art. 5a

Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa, podgrupa ds. kryptografii: »Uzgodnione mechanizmy kryptograficzne« opublikowane przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (»ENISA«) ([1]).”

([1]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_pl.

ZAŁĄCZNIK III

„ZAŁĄCZNIK Ib

Specyfikacje techniczne dotyczące poświadczeń jednostki portfela, o których mowa w art. 6 ust. 2a

1. Poświadczenie jednostki portfela musi obejmować co najmniej jedno poświadczenie instancji portfela oraz co najmniej jedno poświadczenie klucza.

2. Poświadczenie instancji portfela i poświadczenia klucza muszą spełniać następujące wymogi:

   a) Wymagania dotyczące formatu

      — FR-WIA-1: Poświadczeniem instancji portfela jest JSON Web Token (JWT), jak określono w RFC 7519 ([1]), podpisany lub opatrzony pieczęcią przez dostawcę portfela za pomocą kompaktowego podpisu podstawowego JAdES B.

         — FR-WIA-1.1: Poświadczenie instancji portfela jest poświadczeniem portfela określonym w dodatku E do OpenID for Verifiable Credential Issuance v1.0 ([2]) (»OID4VCI«) i rozszerzonym, jak określono w C-WIA-1 i C-WIA-2 poniżej.

      — FR-KA-1: Poświadczeniem klucza jest JWT określone w RFC 7519, podpisane lub opatrzone pieczęcią przez dostawcę portfela za pomocą kompaktowego podpisu podstawowego JAdES B.

         — FR_KA_1.1: Poświadczeniem klucza jest poświadczenie klucza określone w dodatku D do OID4VCI, rozszerzone zgodnie z C_KA-1 i C_KA-2 poniżej

   b) Wymagania w zakresie transportu

      — TR-WIA-1: Jednostka portfela korzysta z poświadczenia instancji portfela podczas wydawania danych identyfikujących osobę, kwalifikowanych lub niekwalifikowanych elektronicznych poświadczeń atrybutów lub elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu.

      — TR-WIA-2: Dostawca portfela weryfikuje integralność instancji portfela oraz podpisuje lub opatruje pieczęcią poświadczenie instancji portfela.

         — TR-WIA-2.1: W przypadku gdy dostawca portfela wydaje poświadczenie instancji portfela, różnica między czasem, w którym dostawca portfela zweryfikował integralność instancji portfela, a czasem, który wskaże w parametrze nagłówka »exp« wydanego poświadczenia instancji portfela, musi wynosić mniej niż 24 godziny.

         — TR-WIA-2.2: Dostawca portfela zapewnia, aby jednostka portfela zawierała poświadczenia instancji portfela niezbędne do wydawania danych identyfikujących osobę oraz elektronicznych poświadczeń atrybutów.

      — TR-WIA-3: W trakcie wydawania jednostka portfela przekazuje poświadczenie instancji portfela do serwera autoryzacji zarówno w ramach żądania autoryzacji typu pushed, jak i żądania tokenu, jak określono w OID4VCI.

         — TR-WIA-3.1: Jednostka portfela przesyła poświadczenie instancji portfela wraz z dowodem posiadania (»PoP«), jak określono w dodatku E do OID4VCI.

         — TR-WIA-3.2: Jednostka portfela przekazuje to samo poświadczenie instancji portfela tylko jednemu serwerowi autoryzacji.

([1]) RFC 7519: JSON Web Token (JWT), maj 2015 r.
([2]) OpenID for Verifiable Credential Issuance v1.0, https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html.

— TR-WIA-3.2.1: W przypadku gdy dostawca portfela korzysta z opcji »per-issuer reuse« określonej w R_WIA_1 poniżej, jednostka portfela może przekazywać poświadczenie instancji portfela temu samemu serwerowi autoryzacji wielokrotnie.

— TR-WIA-3.2.2: W przypadku gdy dostawca portfela nie korzysta z opcji »per-issuer reuse«, jednostka portfela wykorzystuje poświadczenie instancji portfela w co najwyżej jednym procesie wydawania.

— TR-WIA-4: W przypadku gdy serwer autoryzacji otrzymuje poświadczenie instancji portfela, weryfikuje podpis tego poświadczenia instancji portfela przy użyciu klucza publicznego zawartego w certyfikacie podpisującym uwzględnionym w parametrze »x5c« nagłówka JOSE poświadczenia instancji portfela.

— TR-WIA-4.1: Serwer autoryzacji weryfikuje również, czy certyfikat podpisu można zweryfikować za pomocą kotwicy zaufania znajdującej się w wykazie dostawców portfela, o którym mowa w art. 5 rozporządzenia wykonawczego (UE) 2024/2980, potencjalnie z wykorzystaniem certyfikatów pośrednich zawartych w parametrze »x5c«.

— TR-WIA-4.2: Serwer autoryzacji weryfikuje, czy poświadczenie instancji portfela nie wygasło.

— TR-WIA-4.3: Serwer autoryzacji weryfikuje podpis PoP przy użyciu klucza publicznego zawartego w elemencie danych »cnf«.

— TR_KA-1: Jednostka portfela wykorzystuje poświadczenie klucza podczas wydawania danych identyfikujących osobę oraz podczas wydawania powiązanych z urządzeniem kwalifikowanych lub niekwalifikowanych elektronicznych poświadczeń atrybutów lub elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu.

— TR_KA-1.1: Jednostka portfela nie wykorzystuje poświadczenia klucza podczas wydawania niepowiązanych z urządzeniem kwalifikowanych lub niekwalifikowanych elektronicznych poświadczeń atrybutów ani elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu.

— TR_KA-2: Dostawca portfela zapewnia jednostce portfela różne poświadczenia klucza dla WSCD jednostki portfela i dla każdego z jej magazynów kluczy.

— TR_KA-2.1: Dostawca portfela podpisuje lub opatruje pieczęcią poświadczenie klucza po uprzednim zweryfikowaniu, że klucze objęte poświadczeniem są przechowywane w WSCD jednostki portfela lub w magazynie kluczy opisanym w tym poświadczeniu klucza.

— TR_KA-2.2: Poświadczenie klucza musi zawierać co najmniej jeden poświadczony klucz publiczny. Liczba kluczy w poświadczeniu klucza przekazywanym wystawcy poświadczenia nie powinna przekraczać maksymalnej wielkości partii określonej przez tego wystawcę poświadczenia w jego metadanych wydawcy poświadczenia; zob. ETSI TS 119 472-3 ([3]), parametr »credential_configurations_supported. credential_metadata.credential_reuse_policy.options.batch_size«.

— TR_KA-2.3: Dostawca portfela umieszcza klucz publiczny (odpowiadający kluczowi prywatnemu przechowywanemu w WSCD lub w magazynie kluczy jednostki portfela) w co najwyżej jednym poświadczeniu klucza.

— TR_KA-2.4: Jednostka portfela wykorzystuje poświadczenie klucza w co najwyżej jednym procesie wydawania lub ponownego wydawania poświadczenia.

— TR_KA-2.5: Dostawca portfela zapewnia, aby jednostka portfela posiadała poświadczenia klucza niezbędne do wydawania danych identyfikujących osobę oraz powiązanych z urządzeniem elektronicznych poświadczeń atrybutów.

([3]) ETSI, »Podpisy elektroniczne i infrastruktura (ESI); Podpisy cyfrowe JAdES; Część 3: poziomy i profile bazowe JAdES«, ETSI TS 119 472-3, V1.1.1, marzec 2026 r.

— TR_KA-3: W razie potrzeby podczas wydawania jednostka portfela zamieszcza poświadczenie klucza w polu »proofs« żądania poświadczenia skierowanego do wystawcy poświadczenia, zgodnie z OID4VCI, w postaci dowodu typu »jwt« lub typu »attestation«.

— TR_KA_3.1: W przypadku gdy jednostka portfela zawiera poświadczenie klucza w elemencie »jwt«, podpisuje lub opatruje pieczęcią to poświadczenie klucza przy użyciu klucza prywatnego odpowiadającego kluczowi publicznemu znajdującemu się pod indeksem 0 w tablicy »attested_keys« w obiekcie »key_attestation«.

— TR_KA-4: W przypadku gdy wystawca poświadczenia wydaje dane uwierzytelniające powiązane z urządzeniem, wskazuje on w parametrze »proof_types_supported« w swoich metadanych uwierzytelniających wystawcy, jak określono w pkt 12.2.4 OID4VCI, że obsługuje zarówno typ dowodu »jwt«, jak i »attestation« dla poświadczeń klucza, które obejmują obiekt »key_attestations_required«.

— TR_KA-4.1: W przypadku gdy wystawca poświadczenia wydaje dane uwierzytelniające niepowiązane z urządzeniem, pomija parametry »proof_types_supported« oraz »cryptographic_binding_methods_supported« w metadanych uwierzytelniających wystawcy.

— TR_KA-5: W przypadku gdy wystawca poświadczenia otrzymuje poświadczenie klucza w typie dowodu »jwt« lub »attestation«, weryfikuje podpis poświadczenia klucza przy użyciu klucza publicznego zawartego w certyfikacie podpisu zawartym w parametrze »x5c« w nagłówku JOSE poświadczenia klucza oraz sprawdza, czy ten certyfikat podpisu zawiera kotwicę zaufania w wykazie dostawców portfela, o którym mowa w art. 5 rozporządzenia wykonawczego (UE) 2024/2980, potencjalnie z wykorzystaniem certyfikatów pośrednich zawartych w parametrze »x5c«.

— TR_KA-6: W przypadku gdy wystawca poświadczenia otrzymuje poświadczenie klucza w typie dowodu »jwt«, weryfikuje podpis elementu »jwt« przy użyciu klucza znajdującego się pod indeksem 0 w tablicy »attested_keys« w obiekcie »key_attestation« zawartym w elemencie »jwt«.

— TR_KA-6.1: Wystawca poświadczenia weryfikuje, czy pole »nonce« elementu »jwt« zawiera prawidłową wartość c_nonce z jego punktu końcowego nonce_endpoint, jak określono w OID4VCI.

— TR_KA-7: W przypadku gdy wystawca poświadczenia otrzymuje poświadczenie klucza w typie dowodu »attestation«, weryfikuje, czy obiekt »key_attestation« zawiera prawidłową wartość c_nonce z jego punktu końcowego nonce_endpoint.

— TR_KA-8: Dostawca danych identyfikujących osobę zapewnia, aby dane identyfikujące osobę były powiązane z kluczem publicznym pochodzącym z poświadczenia klucza odnoszącego się do WSCD.

c) Wymagania w odniesieniu do treści

— C_WIA-1: Poświadczenie instancji portfela zawiera co najmniej:

— element danych »wallet_name« określony w dodatku E do OID4VCI, którego wartością jest identyfikator rozwiązania w zakresie portfela, który można znaleźć w wykazie dostawców portfela, o którym mowa w art. 5 rozporządzenia wykonawczego (UE) 2024/2980;

— element danych »wallet_version« ([4]), będący ciągiem znaków, którego wartością jest wersja rozwiązania w zakresie portfela;

— element danych »wallet_solution_certification_information«, będący obiektem JSON zawierającym informacje o jednostce oceniającej zgodność, która certyfikowała rozwiązanie w zakresie portfela, numer certyfikacji (w stosownych przypadkach) oraz inne istotne szczegóły dotyczące certyfikacji;

([4]) Ten element danych jest zdefiniowany w tym wspólnym repozytorium danych umożliwiających identyfikację, ponieważ nie jest częścią specyfikacji OID4VCI.

— element danych »client_status«, zawierający dwa podpola:

— »status«: odniesienie do wykazu statusów określone w dodatku E do OID4VCI, które odzwierciedla status unieważnienia instancji portfela. Szczegółowe informacje znajdują się w lit. e) poniżej;

— »exp«: wartość NumericDate, określona w RFC 7519, wskazująca czas, do którego dostawca portfela będzie utrzymywał status unieważnienia pod indeksem wykazu statusów wskazanym w polu »status«;

— element danych »exp« określony w dodatku E do OID4VCI.

— *UWAGA:* Element danych »client_status.status« w poświadczeniu instancji portfela odzwierciedla status unieważnienia instancji portfela, a nie status unieważnienia samego poświadczenia. Jak opisano w R_WIA-1 poniżej, dostawca portfela może zdecydować o ograniczeniu zakresu każdego poświadczenia instancji portfela do konkretnego serwera autoryzacji na podstawie faktu, że wszystkie poświadczenia przekazywane do tego serwera zawierają tę samą wartość indeksu w polu »client_status.status«.

— *UWAGA:* Wartość »idx« w elemencie danych »status« może być wykorzystywana jako niepowtarzalny identyfikator (w parach) instancji portfela oraz jednostki portfela.

— C_WIA-2: Poświadczenie instancji portfela powinno również zawierać element danych »wallet_link« określony w dodatku E do OID4VCI, przy czym wartością tego elementu jest URI, pod którym można uzyskać dalsze informacje na temat rozwiązania w zakresie portfela.

— C_WIA-3: Serwer autoryzacji nie interpretuje parametru »exp« na najwyższym poziomie poświadczenia instancji portfela jako końca okresu utrzymywania statusu unieważnienia instancji portfela.

— *UWAGA:* Parametr »exp« na najwyższym poziomie poświadczenia instancji portfela oznacza moment wygaśnięcia samego poświadczenia.

— C_KA-1: Poświadczenie klucza obejmuje:

— elementy danych »key_storage« i »user_authentication« określone w dodatku D do OID4VCI;

— atrybuty »key_storage« i »user_authentication« przyjmują wartość »iso_18045_high«, jeżeli poświadczenie klucza odnosi się do WSCD;

— element danych »certification« określony w dodatku D do OID4VCI, zawierający adres URL, pod którym można uzyskać informacje na temat certyfikacji osiągniętej przez WSCD lub magazyn kluczy, orientacyjnie schemat, taki jak Common Criteria lub GlobalPlatform, ocenione wymagania, takie jak mający zastosowanie profil zabezpieczeń, oraz poziom oceny;

— na podstawie tych informacji musi być możliwe ustalenie, czy przechowywanie kluczy odbywa się w WSCD;

— element danych »key_storage_status«, zawierający dwa podpola:

— »status«: odniesienie do wykazu statusów określone w dodatku D.1 do OID4VCI. Wartość ta odzwierciedla albo status unieważnienia WSCD lub typu magazynu kluczy wykorzystywanego do przechowywania poświadczonych kluczy, albo – w ramach opcji »per-key-attestation index« – status unieważnienia indywidualnego WSCD lub magazynu kluczy jednostki portfela. Zob. R_KA_1 poniżej, aby zapoznać się z dostępnymi opcjami przypisania indeksów;

— »exp«: wartość NumericDate, określona w RFC 7519, wskazująca czas, do którego dostawca portfela będzie utrzymywał status unieważnienia pod indeksem wykazu statusów wskazanym w polu »status«;

— element danych »exp« określony w dodatku D do OID4VCI.

— *UWAGA* dotycząca wartości »idx« w elemencie danych »key_storage_status.status« w poświadczeniu klucza: w przypadku gdy dostawca portfela korzysta z opcji »type-shared index« (zob. R_KA_1 poniżej), wszystkie poświadczenia klucza dla tego samego typu WSCD lub magazynu kluczy współdzielą ten sam indeks wykazu statusów. W związku z tym wartość »idx« nie jest niepowtarzalna dla jednostki portfela. Natomiast w przypadku gdy dostawca portfela korzysta z opcji »per-key-attestation index«, wartość »idx« jest niepowtarzalna dla każdej jednostki portfela (lub niepowtarzalna dla każdej pary jednostki portfela i wystawcy poświadczenia). W żadnym przypadku wystawca poświadczenia nie wykorzystuje jednak wartości »idx« w poświadczeniu klucza jako identyfikatora jednostki portfela, lecz zamiast tego wykorzystuje wartość »idx« w poświadczeniu instancji portfela.

— C_KA-2: W przypadku gdy poświadczenie klucza jest przekazywane w typie dowodu »attestation«, zawiera ono również prawidłową wartość c_nonce, jak określono w dodatku F.3 do OID4VCI.

— C_KA-3: Wystawca poświadczenia nie interpretuje parametru »exp« na najwyższym poziomie poświadczenia klucza jako końca okresu utrzymywania statusu unieważnienia WSCD lub magazynu kluczy.

— *UWAGA:* Parametr »exp« na najwyższym poziomie poświadczenia klucza oznacza moment wygaśnięcia samego poświadczenia klucza.

d) Wymagania dotyczące cyklu życia

— W niniejszym załączniku określono następujące parametry metadanych wystawcy poświadczenia:

— »preferred_client_status_period«: OPTIONAL. Liczba całkowita określająca preferowany pozostały okres utrzymywania statusu poświadczenia instancji portfela, który jednostka portfela ma przedstawić podczas wydawania, wyrażony w sekundach. Pozostały okres utrzymywania statusu definiuje się jako różnicę między wartością »client_status.exp« w poświadczeniu a momentem otrzymania poświadczenia.

— »preferred_key_storage_status_period«: OPTIONAL. Liczba całkowita określająca preferowany pozostały okres utrzymywania statusu poświadczenia klucza, który jednostka portfela ma przedstawić podczas wydawania, wyrażony w sekundach. Pozostały okres utrzymywania statusu definiuje się jako różnicę między wartością »key_storage_status.exp« w poświadczeniu a momentem otrzymania poświadczenia.

— LC_WIA-1: Serwer autoryzacji może przekazywać swoje preferencje dotyczące pozostałego okresu utrzymywania statusu w poświadczeniach instancji portfela poprzez uwzględnienie parametru metadanych »preferred_client_status_period« w swoim punkcie końcowym metadanych wystawcy poświadczenia, jak określono w pkt 12.2.2 OID4VCI.

— LC_WIA-1.1: Pole to należy umieścić na najwyższym poziomie metadanych wystawcy poświadczenia.

— LC_WIA_2: Serwer autoryzacji nie interpretuje parametru »exp« na najwyższym poziomie poświadczenia instancji portfela jako końca okresu utrzymywania statusu unieważnienia instancji portfela.

— LC_WIA_3: W przypadku gdy dostawca portfela podpisuje lub opatruje pieczęcią poświadczenie instancji portfela, utrzymuje on status unieważnienia odpowiedniej instancji portfela do momentu upływu wartości »wallet_instance_status.exp« wskazanej w tym poświadczeniu.

— LC_KA-1: W przypadku gdy wymagane jest poświadczenie klucza, wystawca poświadczenia może przekazywać swoje preferencje dotyczące pozostałego okresu utrzymywania statusu w poświadczeniach klucza poprzez uwzględnienie parametru metadanych »preferred_key_storage_status_period« w swoim punkcie końcowym metadanych wystawcy poświadczenia, jak określono w pkt 12.2.2 OID4VCI.

— LC_KA-1.1: Pole to należy umieścić w obiekcie »key_attestations_required«, jak określono w pkt 12.2.4 OID4VCI.

— LC_KA-2: Dostawca portfela określa techniczny okres ważności wydawanych przez siebie poświadczeń klucza.

— LC_KA-3: W przypadku gdy dostawca portfela podpisuje lub opatruje pieczęcią poświadczenie klucza, utrzymuje on status unieważnienia odpowiedniego WSCD lub magazynu kluczy do momentu upływu wartości »key_storage_status.exp« wskazanej w tym poświadczeniu.

— LC_GEN-1: Dostawca portfela zapewnia, aby jednostka portfela mogła zawsze przedstawiać poświadczenia jednostki portfela oraz poświadczenia klucza, których wartości »client_status.exp« i »key_storage_status.exp« (odpowiednio) przypadają co najmniej 31 dni po momencie ich przedstawienia serwerowi autoryzacji lub wystawcy poświadczenia.

— *UWAGA:* Gwarantuje to, że dostawcy danych identyfikujących osobę mogą polegać na mechanizmie łańcuchowego sprawdzania unieważnienia bez konieczności wydawania krótkoterminowych danych identyfikujących osobę.

— LC_GEN-2: Dostawca portfela zapewnia, aby jednostka portfela pobierała metadane wystawcy poświadczenia w trakcie wydawania.

  — LC_GEN_2.1: Jeżeli pole »preferred_key_storage_status_period« jest zawarte w tych metadanych, jednostka portfela przekazuje poświadczenie klucza, dla którego wartość (»key_storage_status.exp« – czas bieżący) – »preferred_key_storage_status_period« jest możliwie najmniejsza, lecz nie jest ujemna. Jeżeli jednostka portfela nie ma dostępu do takiego poświadczenia klucza, musi uzyskać nowe poświadczenie klucza od dostawcy portfela, które spełnia warunek »key_storage_status.exp« – czas bieżący ≥ »preferred_key_storage_status_period«.

  — LC_GEN_2.2: Jeżeli w tych metadanych znajduje się pole »preferred_client_status_period«, jednostka portfela przekazuje poświadczenie instancji portfela, dla którego wartość (»client_status.exp« – czas bieżący) – »preferred_client_status_period« jest możliwie najmniejsza, lecz nie jest ujemna. Jeżeli jednostka portfela nie ma dostępu do takiego poświadczenia instancji portfela, zwraca się do dostawcy portfela o wydanie nowego poświadczenia instancji portfela spełniającego warunek »client_status.exp« – czas bieżący ≥ »preferred_client_status_period«.

— LC_GEN-3: Techniczny okres ważności danych identyfikujących osobę kończy się przed upływem zarówno wartości »client_status.exp« poświadczenia instancji portfela, jak i »key_storage_status.exp« poświadczenia klucza przekazanych dostawcy danych identyfikujących osobę w procesie wydawania.

— LC_GEN-4: Dostawca danych identyfikujących osobę, którego dane identyfikujące osobę mają techniczny okres ważności dłuższy niż 24 godziny, sprawdza status unieważnienia zarówno poświadczenia instancji portfela, jak i poświadczenia klucza otrzymanych w trakcie wydawania co najmniej raz na 24 godziny przez cały techniczny okres ważności danych identyfikujących osobę. W przypadku unieważnienia któregokolwiek z nich dostawca unieważnia dane identyfikujące osobę.

e) Wymogi dotyczące unieważniania

— R_GEN-1: Dostawca portfela stosuje wykazy statusów tokenów (określone w wykazie statusów tokenów opracowanym przez IETF) jako mechanizm unieważniania zarówno poświadczeń klucza, jak i poświadczeń instancji portfela, jak określono odpowiednio w dodatkach D i E do OID4VCI.

— *UWAGA:* W celu poprawy skalowalności swoich wykazów statusów dostawca portfela może skorzystać z następujących optymalizacji:

  — podział wykazu statusów na wiele części, w przypadku gdy dostawcy portfela posiadają znaczną liczbę użytkowników i wydanych poświadczeń. Istnieje wiele strategii podziału na części, na przykład opartych na stałej wielkości lub na okresach. Wybór strategii podziału na części pozostawia się uznaniu dostawcy portfela. Przy wyborze należy uwzględnić rozmiar wykazu statusów przeznaczonego do pobrania oraz prywatność użytkownika;

  — posiadanie wielu wykazów statusów;

  — kompresja wykazu statusów w celu zmniejszenia jego rozmiaru.

— R_WIA-1: Dostawca portfela może przypisywać tę samą wartość do elementu danych »idx« w elemencie danych »client_status.status« we wszystkich poświadczeniach instancji portfela, które dana jednostka portfela przedstawia temu samemu serwerowi autoryzacji. Opcję tę określa się jako »per-issuer reuse«. W przypadku korzystania z tej opcji:

  — R_WIA-1.1: Jednostka portfela przechowuje informacje o tym, jakiej wartości indeksu użyła dla każdego serwera autoryzacji, z którym wcześniej wchodziła w interakcję, oraz przy ponownej interakcji z tym samym serwerem żąda poświadczenia instancji portfela zawierającego tę samą wartość indeksu.

  — R_WIA-1.2: W przypadku gdy dostawca portfela otrzymuje wniosek o wydanie poświadczenia instancji portfela zawierającego określoną wartość indeksu, weryfikuje on, czy wnioskująca jednostka portfela wcześniej otrzymała tę wartość indeksu, przed wydaniem nowego poświadczenia instancji portfela z tą wartością.

  — R_WIA-1.3: Jednostka portfela nie wykorzystuje tej samej wartości indeksu w interakcjach z różnymi serwerami autoryzacji.

— *UWAGA:* W przypadku stosowania opcji »per-issuer reuse« dostawca portfela może ustalić, z iloma serwerami autoryzacji dana jednostka portfela wchodziła w interakcję oraz jak często wchodzi w interakcję z każdym z nich.

— R_WIA-2: Dostawca portfela dokumentuje w swojej polityce prywatności, czy stosuje opcję »per-issuer reuse« w odniesieniu do unieważniania instancji portfela.

— R_WIA-3: W przypadku gdy dostawca portfela nie stosuje opcji »per-issuer reuse«, przypisuje on nową, niemożliwą do powiązania wartość indeksu do każdego wydawanego poświadczenia instancji portfela.

— R_WIA-4: W przypadku gdy jednostka portfela musi zostać unieważniona, dostawca portfela unieważnia wartości indeksu w elemencie danych »client_status.status« we wszystkich poświadczeniach instancji portfela powiązanych z tą jednostką portfela.

— R_WIA-5: Dostawca portfela uwzględnia skalę wdrożenia oraz architekturę systemu przy określaniu rozmiaru wykazów statusów poświadczeń instancji portfela, zapewniając, aby były one wystarczająco duże, by zapobiegać korelacji i chronić prywatność użytkowników. W miarę możliwości wykaz statusów powinien odnosić się do co najmniej 10 000 poświadczeń.

— R_KA_1: Dostawca portfela wybiera jedną z następujących opcji przypisywania indeksów dla elementu danych »key_storage_status.status« w poświadczeniu klucza:

  — opcja 1 (»type-shared index«): wszystkie poświadczenia klucza odnoszące się do kluczy przechowywanych w tym samym typie WSCD lub magazynie kluczy zawierają tę samą wartość indeksu w »key_storage_status.status«;

  — opcja 2 (»per-key-attestation index«): poświadczenie klucza odnoszące się do kluczy przechowywanych w indywidualnym WSCD lub w magazynie kluczy zawiera niepowtarzalną wartość indeksu dla każdej pary jednostki portfela i wystawcy poświadczenia w »key_storage_status.status«.

— *UWAGA:* W przypadku gdy dostawca portfela korzysta z opcji 1, pojedyncze działanie unieważniające powoduje unieważnienie wszystkich poświadczeń klucza danego typu we wszystkich jednostkach portfela. Ponadto, ponieważ wszystkie poświadczenia klucza dla tego samego typu WSCD lub magazynu kluczy współdzielą jeden indeks wykazu statusów, liczba wpisów w wykazie statusów poświadczeń klucza odzwierciedla liczbę typów WSCD lub magazynów kluczy obsługiwanych przez dostawcę portfela, a nie liczbę wdrożonych jednostek portfela. Względy ochrony prywatności uzasadniające minimalny rozmiar wykazów statusów dla wykazów statusów instancji portfela nie mają zatem zastosowania do wykazów statusów poświadczeń klucza w ramach opcji 1, pod warunkiem że wystarczająco wiele jednostek portfela korzysta z tego samego typu WSCD lub magazynu kluczy.

— *UWAGA:* W przypadku gdy dostawca portfela korzysta z opcji 2, każdy indeks odzwierciedla stan unieważnienia konkretnego WSCD lub magazynu kluczy poświadczonego w danym poświadczeniu klucza.

— *UWAGA:* W przypadku gdy dostawca portfela korzysta z opcji 2, określone WSCD lub określony magazyn kluczy mogą również zostać unieważnione na wniosek użytkownika.

— R_KA-2: W przypadku gdy dostawca portfela korzysta z opcji 2, może on fakultatywnie stosować opcję »per-issuer reuse« opisaną w R_WIA-1. Jeżeli dostawca portfela korzysta z tej opcji, wymagania R_WIA-1–R_WIA-3 stosuje się odpowiednio.

— R_KA-3: W przypadku gdy dostawca portfela korzysta z opcji 2, uwzględnia on skalę wdrożenia oraz architekturę systemu przy określaniu rozmiaru wykazów statusów poświadczeń klucza, zapewniając, aby były one wystarczająco duże, aby zapobiec korelacji i chronić prywatność użytkowników. W miarę możliwości wykaz statusów powinien odnosić się do co najmniej 10 000 poświadczeń klucza.

— R_KA-4: W przypadku gdy dostawca portfela korzysta z opcji 1 (type-shared index), unieważnia on wpis »key_storage_status.status« wyłącznie w przypadku, gdy dany typ WSCD lub magazynu kluczy wykazuje podatność na zagrożenia bezpieczeństwa.

f) Wymagania dotyczące algorytmów podpisu

— SA-1: Do podpisywania poświadczeń instancji portfela, poświadczeń klucza, powiązanych dowodów posiadania oraz wykazów statusów tokenów stosuje się jeden z następujących algorytmów:

— ES256 (ECDSA z SHA-256 i P-256)

— ES384 (ECDSA z SHA-384 i P-384)

— ES512 (ECDSA z SHA-512 i P-521)

— SA-2: Dostawca portfela wybiera, który z algorytmów wymienionych w SA-1 będzie stosował.

— SA-3: Serwer autoryzacji lub wystawca poświadczenia (zgodnie z OID4VCI) obsługuje wszystkie algorytmy wymienione w SA-1.”

ZAŁĄCZNIK IV

„ZAŁĄCZNIK II

Wykaz norm, o którym mowa w art. 8

Zastosowanie mają specyfikacje techniczne określone w pkt 2–6 ETSI TS 119 472-1 V1.2.1 (2026–02). Odczytuje się je z uwzględnieniem następujących dostosowań:

1) 2.1. Normative references

— [16] ETSI EN 319 412-1 V1.6.1 (2025-06): »Podpisy elektroniczne i infrastruktura (ESI); Profile certyfikatu; Część 1: Opis ogólny oraz ogólne struktury danych«.

— [17] ETSI TS 119 412-6 V1.1.1 (2025-09): »Podpisy elektroniczne i infrastruktura zaufania (ESI); Profile certyfikatu; Część 6: Wymagania dotyczące profili certyfikatów dla dostawców PID, portfela, EAA, QEAA i PSBEAA«.

— [25] Wykaz statusów tokenów (Token Status List – TSL) opracowany przez IETF, draft-ietf-oauth-status-list-20: »Token Status List«, 20 kwietnia 2026 r.

2) 4.2.11.1. General requirements

— EAA-4.2.11.1-06: W przypadku gdy element statusu jest stosowany w odniesieniu do danych identyfikujących osobę, kwalifikowanych elektronicznych poświadczeń atrybutów lub elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu, wskazuje on jedynie, czy poświadczenie zostało unieważnione, czy nie, i nie obsługuje żadnych innych wartości statusu, np. zawieszenia.

— EAA-4.2.11.1-06.1: W przypadku gdy poświadczenie zostało unieważnione, unieważnienie takie ma charakter trwały.

3) 4.2.13. EAA short-lived

— EAA-4.2.13-03: W przypadku gdy poświadczenia krótkoterminowe są wydawane z okresem ważności nieprzekraczającym 24 godzin, unieważnianie nie jest wymagane.

4) 4.6.3. Wymogi dotyczące EU EAA wydane przez organ sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu (PuB-EAA)

— PuB-EAA-4.6.2-03: nieważny.

— Pub-EAA-4.6.2-04: nieważny.

— PuB-EAA-4.6.3-03: Podpis cyfrowy PuB-EAA powinien zawierać kwalifikowany certyfikat potwierdzający podpis cyfrowy PuB-EAA.

— PuB-EAA-4.6.3-04: Kwalifikowany certyfikat potwierdzający podpis cyfrowy PuB-EAA musi spełniać wymogi pkt 8 normy ETSI TS 119412-6 v1.1.1 i zawierać QcType qcStatement określone w normie ETSI EN 319 412-5 v2.5.1, o wartości id-etsi-qct-eidaspsbeaa określonej w następujący sposób:

id-etsi-qct-eidaspsbeaa OBJECT IDENTIFIER::= {id-etsi-eidas2-qct-extensions 3} – certyfikat, o którym mowa w art. 45f ust. 1 lit. b), potwierdzający kwalifikowany podpis elektroniczny lub kwalifikowaną pieczęć elektroniczną podmiotu sektora publicznego, o którym mowa w art. 3 pkt 46 rozporządzenia (UE) nr 910/2014.

5) 5.2.10.1. General requirements

— EAA-5.2.10.1-04: nieważny.

— EAA-5.2.10.1-05: nieważny.

— EAA-5.2.10.1-06: Element statusu może zawierać element status_list, jak określono w pkt 6.2 IETF draft-ietf-oauth-status-20 [25].

— EAA-5.2.10.1-07: nieważny.

— EAA-5.2.10.1-08: nieważny.

— EAA-5.2.10.1-09: nieważny.

— EAA-5.2.10.1-10: nieważny.

— EAA-5.2.10.1-11: nieważny.

— EAA-5.2.10.1-12: nieważny.

6) 6.2.10.1. General requirements

— EAA-6.2.10.1-01: Jeżeli elektroniczne poświadczenie atrybutów zgodne z normą ISO/IEC mdoc wykorzystuje mechanizm wykazu statusów poświadczeń określony w EAA-6.2.10.1-02.2 lub mechanizm wykazu unieważnień poświadczeń określony w EAA-6.2.10.1-02.3, jego obiekt bezpieczeństwa mobilnego (MSO) zawiera strukturę statusu określoną w EAA-6.2.10.1-17, obejmującą informacje o unieważnieniu MSO.

— EAA-6.2.10.1-01.1: W przypadku stosowania mechanizmu wykazu identyfikatorów element statusu zawiera element »identifier_list« określony w EAA-6.2.10.1-11.

— EAA-6.2.10.1-01.2: W przypadku stosowania mechanizmu wykazu statusów element statusu zawiera element »status_list« określony w EAA-6.2.10.1-13.

— *UWAGA:*

  — Struktura statusu zawiera odniesienie do wykazu unieważnień MSO.

  — Wykaz unieważnień MSO stanowi strukturę COSE_Sign1 wskazującą, czy dany MSO został unieważniony.

  — Struktura statusu zawiera wszystkie informacje niezbędne stronie ufającej portfela do ustalenia autentyczności wykazu unieważnień MSO.

— EAA-6.2.10.1-02: Dostawca danych identyfikujących osobę, dostawca kwalifikowanych elektronicznych poświadczeń atrybutów lub dostawca elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu stosuje jedną z następujących metod unieważniania danych identyfikujących osobę, kwalifikowanych elektronicznych poświadczeń atrybutów lub elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu:

— EAA-6.2.10.1-02.1: W przypadku gdy krótkoterminowe elektroniczne poświadczenia atrybutów są wydawane z okresem ważności nieprzekraczającym 24 godzin, unieważnianie nie jest wymagane.

— EAA-6.2.10.1-02.2: W celu zakodowania informacji o unieważnieniu jako wykaz statusów stosuje się mechanizm wykazu statusów poświadczeń.

— EAA-6.2.10.1-02.2.1: Mechanizm wykazu statusów powoduje unieważnienie obiektu bezpieczeństwa mobilnego (MSO) w zależności od tego, czy bit na pozycji określonej przez wystawcę w MSO ma wartość »true« w wykazie statusów.

— EAA-6.2.10.1-02.2.2: Mechanizm wykazu statusów określono w specyfikacji wykazu statusów tokenów (draft-ietf-oauth-status-list-20).

— EAA-6.2.10.1-02.3: W celu zakodowania informacji o unieważnieniu jako wykaz identyfikatorów stosuje się mechanizm wykazu unieważnień poświadczeń.

— EAA-6.2.10.1-02.3.1: Mechanizm wykazu identyfikatorów powoduje unieważnienie obiektu bezpieczeństwa mobilnego (MSO) w zależności od tego, czy identyfikator określony przez wystawcę w MSO znajduje się w wykazie identyfikatorów.

— EAA-6.2.10.1-02.3.2: EAA-6.2.10.1-06, EAA-6.2.10.1-08, EAA-6.2.10.1-09, EAA-6.2.10.1-10 i EAA-6.2.10.1-11 określają mechanizm wykazu identyfikatorów oparty na wymaganiach specyfikacji wykazu statusów tokenów, w tym na wspólnych elementach mechanizmu wykazu statusów i wykazu identyfikatorów.

— EAA-6.2.10.1-03: W przypadku gdy element statusu jest stosowany w odniesieniu do danych identyfikujących osobę, kwalifikowanych elektronicznych poświadczeń atrybutów lub elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu, stosuje się wyłącznie status »revoked«.

— EAA-6.2.10.1-03.1: W przypadku wykazu statusów oznacza to, że stosuje się wyłącznie wartości »valid« i »invalid«, jak określono w specyfikacji wykazu statusów tokenów.

— EAA-6.2.10.1-03.2: W przypadku wykazu identyfikatorów w wykazie umieszcza się wyłącznie unieważnione obiekty bezpieczeństwa mobilnego (MSO), a nie MSO zawieszone tymczasowo.

— EAA-6.2.10.1-04: W przypadku unieważnienia obiektu bezpieczeństwa mobilnego (MSO) unieważnienie ma charakter trwały.

— EAA-6.2.10.1-05: Weryfikacja wykazu unieważnień MSO jest nieobowiązkowa dla strony ufającej portfela i, w stosownych przypadkach, musi odbywać się zgodnie z wymaganiami weryfikacji określonymi w specyfikacji wykazu statusów tokenów oraz w specyfikacji struktury statusu określonej w EAA-6.2.10.1-01.

— EAA-6.2.10.1-05.1: W przypadku gdy strona ufająca portfela musi mieć możliwość weryfikacji statusu unieważnienia danych identyfikujących osobę lub elektronicznych poświadczeń atrybutów, obsługuje ona zarówno mechanizm wykazu statusów poświadczeń, jak i mechanizm wykazu unieważnień poświadczeń określone w EAA-6.2.10.1-02.

— EAA-6.2.10.1-06: Elementy »identifier_list« i »status_list« w MSO mogą zawierać element »certificate«.

— EAA-6.2.10.1-06.1: W przypadku gdy element »certificate« jest obecny, zawiera on certyfikat obejmujący klucz publiczny użyty do podpisania lub opatrzenia pieczęcią certyfikatu najwyższego poziomu w elemencie »x5chain« w strukturze wykazu unieważnień MSO.

— EAA-6.2.10.1-06.1.1: Instancja strony ufającej portfela wykorzystuje ten certyfikat jako kotwicę zaufania do weryfikacji elementu »x5chain« w strukturze wykazu unieważnień MSO.

— EAA-6.2.10.1-06.2: W przypadku gdy element »certificate« nie występuje, certyfikat najwyższego poziomu w elemencie »x5chain« w strukturze wykazu unieważnień MSO zostaje podpisany lub opatrzony pieczęcią przy użyciu certyfikatu zastosowanego do podpisania certyfikatu w elemencie »x5chain« MSO.

— EAA-6.2.10.1-06.2.1: Instancja strony ufającej portfela wykorzystuje ten certyfikat jako kotwicę zaufania do weryfikacji elementu »x5chain« w strukturze wykazu unieważnień MSO.

— EAA-6.2.10.1-07: Wykaz unieważnień MSO wdraża się zgodnie ze specyfikacją wykazu statusów tokenów jako token wykazu statusów w formacie CWT.

— EAA-6.2.10.1-08: W odniesieniu do wykazu unieważnień MSO stosowanego w mechanizmie wykazu identyfikatorów i wykazu statusów zastosowanie mają następujące wymogi:

  — element danych »exp« musi być obecny;

  — element danych »ttl« może być obecny;

  — element danych »aggregation_uri« w elemencie danych IdentifierList lub StatusList może być obecny, a dostawca danych identyfikujących osobę, dostawca kwalifikowanych elektronicznych poświadczeń atrybutów lub dostawca elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora

publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu może wykorzystywać ten element do wskazania obsługi mechanizmu agregacji określonego w specyfikacji wykazu statusów tokenów;

— CWT stanowi obiekt COSE_Sign1 wykorzystujący jeden z następujących algorytmów do obliczenia podpisu:

a) »ES256« (ECDSA z krzywą NIST P-256 i SHA-256);

b) »ES384« (ECDSA z krzywą NIST P-384 i SHA-384);

c) »ES512« (ECDSA z krzywą NIST P-521 i SHA-512);

d) »ESB256« (ECDSA z krzywą brainpoolP256r1 i SHA-256);

e) »ESB384« (ECDSA z krzywą brainpoolP384r1 i SHA-384);

f) »ESB512« (ECDSA z krzywą brainpoolP512r1 i SHA-512);

— CWT zawiera element »x5chain« w chronionym nagłówku, obejmujący certyfikat lub łańcuch certyfikatów umożliwiających weryfikację podpisu wykazu unieważnień MSO;

— rozszerzone użycie klucza identyfikatora obiektu określonego w specyfikacji wykazu statusów tokenów może być stosowane w certyfikacie podpisującym wykaz statusów i wykaz identyfikatorów, a instancje strony ufającej portfela mogą obsługiwać rozszerzone użycie klucza identyfikatorów obiektów określonych w tej specyfikacji; w odniesieniu do identyfikatora obiektu, dostawca kwalifikowanych elektronicznych poświadczeń atrybutów lub dostawca elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego lub w jego imieniu nie oznacza pola »extended key usage« jako krytycznego w przypadku stosowania identyfikatora OID określonego w specyfikacji wykazu statusów tokenów.

— EAA-6.2.10.1-09: W drodze odstępstwa od wymogów specyfikacji wykazu statusów tokenów w odniesieniu do mechanizmu wykazu identyfikatorów zastosowanie mają następujące wymogi:

— wartość elementu danych »type« wynosi »application/identifierlist+cwt«;

— element danych »StatusList« nie występuje w zbiorze elementów danych CWT;

— struktura »IdentifierList« określona w EAA-6.2.10.1-11 występuje jako element danych w zbiorze elementów danych CWT przy użyciu klucza 65530.

— EAA-6.2.10.1-10: Struktura »IdentifierList« stanowi strukturę CBOR o następującej notacji CDDL:

```
IdentifierList = {

    'identifiers': { * Identifier => IdentifierInfo },

    ? 'aggregation_uri': Aggregation_uri

    * tstr => RFU

}

IdentifierInfo = { tstr/int => RFU }

Identifier = bstr

Aggregation_uri = tstr
```

— EAA-6.2.10.1-10.1: W przypadku gdy identyfikator w strukturze »IdentifierList« jest obecny, obiekt bezpieczeństwa mobilnego (MSO), który zawiera ten identyfikator w elemencie statusu, uznaje się za unieważniony.

— EAA-6.2.10.1-10.2: Element danych »Aggregation_uri« określono w pkt 9.2 specyfikacji wykazu statusów tokenów.

— EAA-6.2.10.1-10.3: Typ zawartości wykazu identyfikatorów ma postać »application/identifierlist+cwt«, zgodnie z wymogami określonymi w pkt 8.2 specyfikacji wykazu statusów tokenów.

— EAA-6.2.10.1-11: Do elementu »identifier_list« w MSO mają zastosowanie następujące wymogi (zob. EAA-6.2.10.1-17).

— EAA-6.2.10.1-11.1: Element »identifier_list« stanowi strukturę CBOR o następującej notacji CDDL:

```
IdentifierListInfo = {

        'id': Identifier ,

        'uri': URI,

        ? 'certificate': Certificate

        * tstr => RFU

}

URI = tstr

Certificate = bstr
```

— EAA-6.2.10.1-11.2: REV-11.2: Aby zapobiec wykorzystywaniu identyfikatora jako korelacji między prezentacjami, musi on być niepowtarzalny dla każdego MSO.

— EAA-6.2.10.1-12: Do wykazu statusów mają zastosowanie następujące wymogi:

  — EAA-6.2.10.1-12.1: Element »bits« w strukturze »StatusList« ma wartość 1.

— EAA-6.2.10.1-13: Do elementu »status_list« w MSO mają zastosowanie następujące wymogi (zob. EAA-6.2.10.1-17):

  — EAA-6.2.10.1-13.1: Element »status_list« musi być zgodny z wymogami dotyczącymi struktury »StatusListInfo« określonymi w specyfikacji wykazu statusów tokenów i dodaje się opcjonalny element certyfikatu określony w EAA-6.2.10.1-06.

  — EAA-6.2.10.1-13.2: Aby zapobiec wykorzystaniu indeksu statusu do korelacji między prezentacjami, kombinacja indeksu statusu i URI musi być niepowtarzalna dla każdego MSO.

— EAA-6.2.10.1-14: Dostawca portfela stosuje drugą (EAA-6.2.10.1-02.2) lub trzecią (EAA-6.2.10.1-02.3) spośród metod określonych w EAA-6.2.10.1-02 w celu unieważnienia poświadczenia instancji portfela oraz unieważnienia poświadczenia klucza.

— EAA-6.2.10.1-15: Dostawca portfela wdraża mechanizmy unieważniania poświadczeń określone w EAA-6.2.10.1-02 w swoim rozwiązaniu w zakresie portfela.

— EAA-6.2.10.1-16: Dostawca danych identyfikujących osobę i dostawca elektronicznych poświadczeń atrybutów muszą obsługiwać zarówno mechanizm wykazu statusów poświadczeń, jak i mechanizm wykazu unieważnień poświadczeń określone w EAA-6.2.10.1-02 na potrzeby weryfikacji statusu unieważnienia poświadczenia instancji portfela i poświadczenia klucza.

— EAA-6.2.10.1-17: Struktura »status« w MSO stanowi strukturę CBOR o następującej notacji CDDL:

Status = {

? 'identifier_list': IdentifierListInfo,

? 'status_list': StatusListInfo,

* tstr => RFU

}”.

ZAŁĄCZNIK V

„ZAŁĄCZNIK III

Specyfikacje techniczne, o których mowa w art. 10

— Specyfikacje techniczne:

  — pkt 4.2.5 normy ETSI TS 119 472-3 V1.1.1 (2026-03).”

ZAŁĄCZNIK VI

W załączniku IV do rozporządzenia wykonawczego (UE) 2024/2979 wprowadza się następujące zmiany:

1) pkt 1 otrzymuje brzmienie:

„1. Obowiązkowy format podpisu lub pieczęci:

a) PAdES (ang. PDF Advanced Electronic Signature, zaawansowany podpis elektroniczny do podpisywania plików w formacie PDF), jak określono w normie ETSI EN 319 142-1 V1.2.1 (2024-01); Podpisy elektroniczne i infrastruktura (ESI); Podpisy cyfrowe PAdES; Część 1: Elementy składowe i podstawowe profile podpisów PAdES.";

2) pkt 3 otrzymuje brzmienie:

„3. Interfejs programowania aplikacji:
ETSI TS 119 432 v1.3.1 (2026-03), pkt 6.4.3, A.6, A.7 i A.8.".

ZAŁĄCZNIK VII

”ZAŁĄCZNIK VI

Unijny znak zaufania dla portfela tożsamości cyfrowej w wersji kolorowej

”

ZAŁĄCZNIK VIII

”ZAŁĄCZNIK VII

Unijny znak zaufania dla portfela tożsamości cyfrowej w wersji czarno-białej

”

ZAŁĄCZNIK IX

„ZAŁĄCZNIK VIII

Dane dotyczące unijnego znaku zaufania dla portfela tożsamości cyfrowej

Dane	Opis	Kodowanie	Status
TrustMarkResourceURL	Adres URL grafiki unijnego znaku zaufania dla portfela tożsamości cyfrowej oraz zasobów informacyjnych dla użytkownika w interfejsie użytkownika portfela.	URL	obowiązkowe
ListOfCertifiedWalletsURL	Adres URL publicznego wykazu certyfikowanych rozwiązań w zakresie portfela w UE określonego w rozporządzeniu wykonawczym Komisji (UE) 2025/849 ([1]).	URL	obowiązkowe
ListOfCertifiedWalletsQRCode	QR Code zawierający informacje z ListOfCertifiedWalletsURL.	ISO-8859-1 Byte mode QR code	opcjonalne
WalletSolutionInfoPageURL	Adres URL strony informacyjnej certyfikowanego rozwiązania w zakresie portfela na stronie wykazu certyfikowanych rozwiązań w zakresie portfela, stanowiący ListOfCertifiedWalletsURL uzupełniony znakiem »?« oraz identyfikatorem WalletSolutionID danego rozwiązania w zakresie portfela.	URL	obowiązkowe
WalletSolutionInfoPageQRCode	Kod QR zawierający informacje o WalletSolutionInfoPageUR.	ISO-8859-1 Byte mode QR code	opcjonalne
WalletVerifierToolURL*	Adres URL prowadzący do punktu końcowego narzędzia weryfikacji portfela */.well-known/openid-credential-issuer*, wykorzystywanego do pobierania metadanych dostawcy poświadczeń.	URL	opcjonalny

([1]) Rozporządzenie wykonawcze Komisji (UE) 2025/849 z dnia 6 maja 2025 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do przekazywania informacji Komisji i grupie współpracy na potrzeby wykazu certyfikowanych europejskich portfeli tożsamości cyfrowej (Dz.U. L, 2025/849, 7.5.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/849/oj)."

ZAŁĄCZNIK X

W załączniku II do rozporządzenia wykonawczego (UE) 2024/2980 wprowadza się następujące zmiany:

1) sekcja 1 pkt 1 lit. i) w załączniku II otrzymuje brzmienie:

„(i) co najmniej jeden certyfikat zgodny z normą ETSI EN 319 412-2 V2.4.1 (2025-06) lub normą ETSI EN 319 412-3 V1.3.1 (2023-09), który można wykorzystać do zweryfikowania podpisu lub pieczęci złożonych przez podmiot rejestrujący na danych w rejestrze, w przypadku których certyfikowane dane tożsamości zawierają nazwę podmiotu rejestrującego oraz, w razie potrzeby, jego numer rejestrowy, zgodnie odpowiednio z lit. c) i d);";

2) sekcja 2 pkt 1 lit. h) w załączniku II otrzymuje brzmienie:

„h) co najmniej jeden certyfikat zgodny z normą ETSI EN 319 412-2 V2.4.1 (2025-06) lub normą ETSI EN 319 412-3 V1.3.1 (2023-09), który można wykorzystać do uwierzytelnienia i walidacji poświadczeń jednostki portfela wydanych przez dostawcę portfela, oraz w przypadku których certyfikowane dane na temat tożsamości zawierają nazwę dostawcy portfela oraz, w stosownych przypadkach, jego numer rejestrowy, zgodnie odpowiednio z lit. a) i b);";

3) sekcja 3 pkt 1 lit. h) w załączniku II otrzymuje brzmienie:

„h) co najmniej jeden certyfikat zgodny z normą ETSI EN 319 412-2 V2.4.1 (2025-06) lub normą ETSI EN 319 412-3 V1.3.1 (2023-09), który można wykorzystać do weryfikacji podpisu lub pieczęci złożonych przez dostawcę danych identyfikujących osobę na przekazywanych przez niego danych identyfikujących osobę, w przypadku których certyfikowane dane tożsamości zawierają imię i nazwisko lub nazwę dostawcy danych identyfikujących osobę oraz, w stosownych przypadkach, jego numer rejestrowy, zgodnie z odpowiednio lit. a) i b).";

4) sekcja 4 pkt 1 lit. g) w załączniku II otrzymuje brzmienie:

„g) co najmniej jeden certyfikat zgodny z normą ETSI EN 319 412-2 V2.4.1 (2025-06) lub normą ETSI EN 319 412-3 V1.3.1 (2023-09), który można wykorzystać do weryfikacji podpisu lub pieczęci złożonych przez dostawcę certyfikatów dostępu strony ufającej portfela na certyfikacie dostępu zapewnianym stronom ufającym portfela, w stosownych przypadkach wraz z informacjami wymaganymi do odróżnienia certyfikatów dostępu strony ufającej portfela od innych certyfikatów.";

5) w załączniku II dodaje się pkt 5 w brzmieniu:

„5. Przekazywanie informacji o dostawcach certyfikatów rejestracji strony ufającej portfela

1. Państwa członkowskie przekują Komisji następujące informacje na temat dostawców certyfikatów rejestracji strony ufającej portfela:

a) nazwę dostawcy certyfikatów rejestracji strony ufającej portfela;

b) w stosownych przypadkach, numer rejestrowy dostawcy certyfikatów rejestracji strony ufającej portfela;

c) państwo członkowskie, w którym dostawca certyfikatów rejestracji strony ufającej portfela ma swoją siedzibę;

d) adres e-mail i numer telefonu kontaktowego dostawcy certyfikatów rejestracji strony ufającej portfela w sprawach związanych z certyfikatami rejestracji, które przekazuje on stronom ufającym portfela;

e) w stosownych przypadkach adres URL strony internetowej dostawcy certyfikatów rejestracji strony ufającej portfela, która zawiera dodatkowe informacje na temat dostawcy oraz certyfikatów rejestracji, które przekazuje on stronom ufającym portfela;

f) adres URL strony internetowej zawierającej politykę oraz warunki mające zastosowanie w przypadku zapewniania certyfikatów rejestracji stronom ufającym portfela oraz korzystania z tych certyfikatów;

g) co najmniej jeden certyfikat zgodny z normą ETSI EN 319 412-2 V2.4.1 (2025-06) lub normą ETSI EN 319 412-3 V1.3.1 (2023-09), który można wykorzystać do weryfikacji podpisu lub pieczęci złożonych przez dostawcę certyfikatów rejestracji strony ufającej portfela na certyfikatach rejestracji zapewnianych stronom ufającym portfela, w stosownych przypadkach wraz z informacjami wymaganymi do odróżnienia certyfikatów dostępu strony ufającej portfela od innych certyfikatów.

2. Informacje, o których mowa w ppkt 1, przekazuje się w podziale na dostawców certyfikatów rejestracji strony ufającej portfela.”.

ZAŁĄCZNIK XI

„ZAŁĄCZNIK I

Protokoły i interfejsy, o których mowa w art. 4

Specyfikacja techniczna ETSI TS 119 472-3 V1.1.1 (2026-03) ma zastosowanie z następującymi dostosowaniami:

1) 4.1. General requirements

— GEN-REQ-4.1-05: nieważny.

— *UWAGA:* nieważny.

2) 4.2.3. Provision of registration certificates of PID/EAA Provider to EUDI Wallet

— ISS-MDATA-REG_CERT-4.2.3-04: Jeden z elementów tablicy parametrów issuer_info musi zawierać certyfikat rejestracji dostawcy PID/EAA.

— ISS-MDATA-REG_CERT-4.2.3-07: nieważny

— ISS-MDATA-REG_CERT-4.2.3-08: nieważny

— ISS-MDATA-REG_CERT-4.2.3-09: nieważny

— ISS-MDATA-REG_CERT-4.2.3-10: nieważny

— ISS-MDATA-REG_CERT-4.2.3-11: nieważny

— ISS-MDATA-REG_CERT-4.2.3-12: nieważny

— ISS-MDATA-REG_CERT-4.2.3-13: nieważny

3) 4.2.4.2. ARF pre-defined PID/EAA reuse policy

— ISS-MDATA-EAA-REUSE-POL-4.2.4.2-09: W przypadku gdy element »id« ma wartość »arf_annex_ii«, a tablica przypisana do etykiety »details« zawiera wartość »once_only« lub »per-relying-party«, obiekt JSON zawierający tę tablicę przypisaną do etykiety »details« zawiera również liczbę JSON przypisaną do etykiety »reissue_trigger_unused«.

4) Załącznik A nie ma zastosowania.”

ZAŁĄCZNIK XII

„ZAŁĄCZNIK II

Specyfikacje techniczne, o których mowa w art. 5

Zastosowanie ma specyfikacja techniczna określona w załączniku C do normy ISO/IEC 18013-7:2025.

Specyfikacje techniczne określone w pkt 4.1, 4.2, 5, i 6 normy ETSI TS 119 472-2 V1.2.1 (2026-03) mają zastosowanie z następującymi dostosowaniami, z uwzględnieniem dodania nowego pkt 4.3:

1) 1. Scope

— Niniejszy dokument określa dwa profile protokołów umożliwiające stronom ufającym (zwanym dalej »RP«) żądanie EAAP lub danych identyfikujących osobę (zwanych dalej »PID«) od europejskiego portfela tożsamości cyfrowej oraz umożliwiające mu przekazanie żądanych EAAP/PID do RP. Każdy z profili obsługuje dwa mechanizmy transmisji, mianowicie: z wykorzystaniem API oraz bez wykorzystania API, jak przedstawiono poniżej:

a) Profil opiera się na:

— ISO/IEC 18013-5 [10] wyłącznie w odniesieniu do mechanizmu transmisji bez wykorzystania API, oraz

— załączniku C do ISO/IEC 18013-7 [16] w odniesieniu do mechanizmu transmisji z wykorzystaniem API.

Profil ten nosi nazwę profilu ISO/IEC-mdoc i jest określony w pkt 5 niniejszego dokumentu.

b) Profil opiera się na:

OpenID4VC-HAIP [11] w odniesieniu do obu mechanizmów transmisji (z wykorzystaniem API i bez wykorzystania API), w następujący sposób:

— pkt 5, 5.1, 5.3, 7 i 8 [11] w odniesieniu do transmisji poprzez przekierowania lub mechanizm bez wykorzystania API, oraz

— pkt 5, 5.2, 5.3, 7 i 8 [11] w odniesieniu do mechanizmu transmisji z wykorzystaniem API.

Profil ten nosi nazwę profilu OpenID4VC-HAIP i jest określony w pkt 6 niniejszego dokumentu.

2) 2.1. Normative references

— [15] ISO 639: »Language code«.

— [16] ISO/IEC 18013-7:2025 „Personal identification – ISO – compliant driving licence – Part 7: Mobile driving licence (mDL) add-on functions”.

3) 4.1. EAAP implementation based on SD-JWT VC

— EAAP-SD-JWT VC-04: nieważny.

4) 4.2. EAAP implementation based on ISO/IEC-mdoc

— EAAP-ISO/IEC-mdoc-01: nieważny.

— Note2: nieważny.

— EAAP-ISO/IEC-mdoc-02: nieważny.

5) 4.3. EAAP implementation with mediating API

— EAAP-API-GEN-01: Europejski portfel tożsamości cyfrowej musi obsługiwać pośredniczący API, który obsługuje oba protokoły określone w pkt 5.2 [11] i w załączniku C do [16].

— *UWAGA:* W przypadku gdy urządzenie, na którym zainstalowano europejski portfel tożsamości cyfrowej, nie obsługuje obu protokołów, wymóg ten nie może zostać spełniony i powoduje niezgodność ze względu na fakt, że podstawowe systemy operacyjne i przeglądarki nie wdrażają niezbędnych funkcji interoperacyjności.

— EAAP-API-GEN-02: Europejski portfel tożsamości cyfrowej obsługuje API pośredniczący co najmniej w odniesieniu do rodzajów PID i EAA zarejestrowanych w katalogu systemów określonym w rozporządzeniu wykonawczym (UE) 2025/1569 oraz co najmniej w odniesieniu do wszystkich formatów określonych w załączniku II do rozporządzenia wykonawczego (UE) 2024/2979.

— *UWAGA 1:* Wymóg ten nie może zostać spełniony, jeżeli podstawowy system operacyjny, przeglądarka, pośredniczące API lub jakakolwiek inna warstwa techniczna pozostająca poza kontrolą europejskiego portfela tożsamości cyfrowej limituje, filtruje, wstępnie wybiera lub w inny sposób ogranicza formaty poświadczeń oraz rodzaje PID i EAA zarejestrowane w katalogu systemów. W przypadku gdy takie ograniczenie uniemożliwia europejskiemu portfelowi tożsamości cyfrowej obsługę zarejestrowanego rodzaju lub formatu poświadczenia, wynikającą z tego niezgodność można przypisać niedostarczeniu niezbędnych funkcji interoperacyjności przez te podstawowe systemy operacyjne, przeglądarki, pośredniczący API lub inną odpowiednią warstwę techniczną.

6) 4.4. Walidacja strony ufającej portfela i kontrole nadmiernych zapytań

— WRP-VALIDATION-01: Europejski portfel tożsamości cyfrowej zatwierdza certyfikat rejestracji strony ufającej portfela otrzymany w żądaniu przed przedstawieniem żądanego PID lub elektronicznego poświadczenia atrybutów użytkownikowi portfela do zatwierdzenia.

— WRP-VALIDATION-02: W przypadku gdy walidacja certyfikatu rejestracji strony ufającej portfela nie powiedzie się, w tym w przypadku gdy certyfikat wygasł, został cofnięty, nie został wydany przez ważnego zaufanego dostawcę certyfikatów rejestracji strony ufającej portfela, został zniekształcony lub nie może zostać zweryfikowany kryptograficznie, europejski portfel tożsamości cyfrowej ostrzega użytkownika portfela, że strona ufająca portfela nie mogła zostać zwalidowana, i nie może przedstawić wniosku jako pomyślnie zwalidowanego. Użytkownik portfela wyraźnie zatwierdza wniosek strony ufającej. Milczenie lub domyślnie zaznaczone pola nie wystarczają do wyraźnego zatwierdzenia.

— WRP-VALIDATION-03: Dostawca portfela określa, na podstawie swojej analizy ryzyka i polityki bezpieczeństwa, czy i na jakich warunkach użytkownik portfela może ominąć określone nieudane kontrole walidacyjne.

— WRP-OVERASKING-01: Europejski portfel tożsamości cyfrowej porównuje poświadczenia i atrybuty wymagane przez stronę ufającą portfela z zarejestrowanymi poświadczeniami i atrybutami w certyfikacie rejestracji strony ufającej portfela.

— WRP-OVERASKING-02: W przypadku gdy strona ufająca portfela żąda PID lub elektronicznych poświadczeń atrybutów lub elementów, które nie są objęte certyfikatem rejestracji strony ufającej portfela, europejski portfel tożsamości cyfrowej wyraźnie ostrzega użytkownika portfela przed jakimkolwiek ujawnieniem. W ostrzeżeniu wskazuje się, że strona ufająca portfela żąda więcej informacji, niż zarejestrowała. Użytkownik portfela wyraźnie zatwierdza wniosek strony ufającej. Milczenie lub domyślnie zaznaczone pola nie wystarczają do wyraźnego zatwierdzenia.

— WRP-OVERASKING-03: Dostawca portfela określa, na podstawie swojej analizy ryzyka, polityki bezpieczeństwa i mającego zastosowanie prawa, czy użytkownik portfela może kontynuować działalność pomimo takiego ostrzeżenia, czy można ujawnić jedynie podzbiór żądanych danych objętych certyfikatem rejestracji, czy też wniosek należy odrzucić.

7) 5.1. Introduction

— Pkt 5 oraz jego podpunkty określają profil protokołu umożliwiającego stronie ufającej (RP) żądanie EAAP lub danych identyfikujących osobę (PID) od europejskiego portfela tożsamości cyfrowej oraz umożliwiającego mu przekazywanie żądanych EAAP/PID do RP przy użyciu mechanizmu transmisji bez wykorzystania API, opartego na ISO/IEC 18013-5 [10], lub mechanizmu transmisji z wykorzystaniem API, opartego na załączniku C do ISO/IEC 18013-7 [16], służącego do przekazywania struktur danych określonych w ISO/IEC 18013-5 [10] w odpowiednio opakowanej postaci.

— Pozostała część pkt 5 ma następującą strukturę:

— w pkt 5.2 określono wymagania dotyczące obsługi profilu i mechanizmów transmisji przez strony ufające (RP) i europejski portfel tożsamości cyfrowej;

— w pkt 5.3 określono wymagania właściwe dla mechanizmu transmisji bez wykorzystania API;

— pkt 5.4 oraz jego podpunkty określają wymagania właściwe dla mechanizmu transmisji z wykorzystaniem API.

8) 5.2. Requirements on EUDI Wallet and RP support

— ISO/IEC 18013-SUPPORT-01: Jednostki portfela, dostawcy PID, dostawcy poświadczeń, dostawcy portfela i strony ufające nie obsługują pobierania z serwera określonego w ISO/IEC 18013-5 [10] na potrzeby żądania i prezentacji PID lub atrybutów poświadczeń.

— ISO/IEC 18013-SUPPORT-02: Europejski portfel tożsamości cyfrowej musi spełniać wymagania określone w pkt 5.3 i 5.4 niniejszego dokumentu.

— ISO/IEC 18013-SUPPORT-04: Strona ufająca powinna wdrożyć profil określony w pkt 5.4 niniejszego dokumentu.

9) 5.3.2. ISO/IEC-mdoc EAAP Request contents

— ISO/IEC 18013-5-REQ-04: Żądania urządzenia przesyłane do europejskich portfeli tożsamości cyfrowej zawierają parę klucz–wartość »requestInfo« określoną w pkt 8.3.2.1.2.1 [10]. Wartość tej pary musi być typu RequestInfo.

— ISO/IEC 18013-5-REQ-05: Typ RequestInfo jest zgodny z poniższą definicją CDDL.

RequestInfo = {

'euWrprc': bstr; zawiera certyfikat rejestracji (zob. wymogi poniżej)

}

— ISO/IEC 18013-5-REQ-06: Wspomniany element requestInfo zawiera element z oznaczeniem »euWrprc«.

— ISO/IEC 18013-5-REQ-07: Wartość »euWrprc« jest zakodowanym w CBOR zaświadczeniem o rejestracji.

— ISO/IEC 18013-5-REQ-08: nieważny.

— *UWAGA 3:* nieważny.

— ISO/IEC 18013-5-REQ-09: nieważny.

— ISO/IEC 18013-5-REQ-10: nieważny.

— ISO/IEC 18013-5-REQ-11: nieważny.

10) 5.3.3 ISO/IEC-mdoc EAAP Response profile

— W tym punkcie określono wymagania dotyczące typu komunikatu DeviceResponse, wspólne dla obu typów mechanizmów transmisji (z wykorzystaniem API i bez wykorzystania API).

— *UWAGA 1:* W przypadku stosowania mechanizmu bez wykorzystania API, opartego na ISO/IEC 18013-5 [10], odpowiedź EAAP stanowi dokładnie instancję DeviceResponse zgodnie z profilem określonym w tym punkcie. W przypadku stosowania mechanizmu z wykorzystaniem API, opartego na załączniku C do ISO/IEC 18013-7 [16], instancja DeviceRequest jest opakowana zgodnie z załącznikiem C do [16].

— ISO/IEC 18013-5-RESP-02: Dostawca danych identyfikujących osobę i elektronicznych poświadczeń atrybutów nie włącza żadnych elementów danych do mapy KeyAuthorizations w obiekcie bezpieczeństwa mobilnego wydawanych przez siebie danych identyfikujących osobę i elektronicznych poświadczeń atrybutów, z wyjątkiem elementów danych dostarczonych przez stronę ufającą portfela w danych transakcyjnych w żądaniu mdoc, przeznaczonych do podpisania lub opieczętowania przez jednostkę portfela z wykorzystaniem klucza prywatnego danych identyfikujących osobę lub elektronicznych poświadczeń atrybutów.

— *UWAGA 2:* W rezultacie jednostki portfela nie mogą przedstawiać stronom ufającym portfela żadnych elementów danych podpisanych przez urządzenie, z wyjątkiem podpisania danych dostarczonych przez stronę ufającą portfela, na przykład w przypadkach wykorzystania do bezpiecznego uwierzytelniania użytkownika.

— *UWAGA 3:* Norma ISO/IEC 18013-5:2021 nie określa, w jaki sposób strony ufające portfela mogą włączać dane transakcyjne do żądania mdoc. Włączenie danych transakcyjnych do żądania mdoc następuje poprzez dodanie specyfikacji technicznych.

— ISO/IEC 18013-5-RESP-03: Dostawcy danych identyfikujących osobę nie zezwalają na wykorzystywanie klucza prywatnego danych identyfikujących osobę do podpisywania elementów danych dostarczonych przez stronę ufającą portfela w danych transakcyjnych w żądaniu mdoc.

11) 5.4 Requirements for API mediated mechanism

5.4.1 ISO/IEC 18013-7-related requirements

W tym punkcie określono wymogi dotyczące mechanizmu transmisji z wykorzystaniem API, powiązane z wymogami określonymi w załączniku C do [16].

— ISO/IEC 18013-7-API-01: Profil obsługujący prezentacje z wykorzystaniem API musi spełniać wymagania określone w załączniku C do ISO/IEC 18013-7 [16], zgodnie z dalszym uszczegółowieniem w pkt 5.3 i 5.4 niniejszego dokumentu.

— ISO/IEC 18013-7-API-02: Wszystkie obowiązkowe wymagania określone w załączniku C [16] mają zastosowanie zgodnie z dalszym uszczegółowieniem w pkt 5.3 i 5.4 niniejszego dokumentu.

— ISO/IEC 18013-7-API-03: Wszystkie wymagania fakultatywne określone w załączniku C do [16] pozostają nieobowiązkowe, chyba że niniejszy dokument stanowi inaczej.

12) 5.4.2. Dodatkowe wymagania

— W tym punkcie określono dodatkowe wymagania dotyczące mechanizmu transmisji z wykorzystaniem API.

— ISO/IEC 18013-ADD-API-01: Europejski portfel tożsamości cyfrowej domyślnie ujawnia pośredniczącemu API działającemu zgodnie z załącznikiem C do [16] informację o obecności wszystkich przechowywanych typów elektronicznych poświadczeń atrybutów, jednak nie ujawnia atrybutów ani ich wartości w tych elektronicznych poświadczeniach atrybutów.

  — *UWAGA 1:* Ograniczenie dotyczące wartości atrybutów ma zastosowanie nawet wtedy, gdy takie ujawnienie mogłoby usprawnić usługi świadczone przez system operacyjny na rzecz europejskiego portfela tożsamości cyfrowej, na przykład wybór poświadczeń w kontekście pośredniczącego API.

— Z systemami operacyjnymi i przeglądarkami wiążą się pewne aspekty niepodlegające kontroli podmiotów wdrażających, które można uwzględnić, jak wskazano w poniższych uwagach 2–4:

  — *UWAGA 2:* Żądanie prezentacji od strony ufającej portfela stosującej załącznik C do [16] może być przetwarzane przez przeglądarkę lub system operacyjny w celu wyszukiwania dostępnych elektronicznych poświadczeń atrybutów (EAA).

  — *UWAGA 3:* Oczekuje się, że żądanie prezentacji od strony ufającej portfela stosującej załącznik C do [16] będzie przetwarzane przez przeglądarkę lub system operacyjny w celach zapewnienia bezpieczeństwa użytkownika.

— *UWAGA 4:* Oczekuje się, że żądanie prezentacji od strony ufającej portfela stosującej załącznik C do [16] nie będzie przetwarzane przez przeglądarkę ani system operacyjny w celach analizy rynku (w tym jako cel drugorzędny) ani do celów wewnętrznych przeglądarki lub systemu operacyjnego.

— ISO/IEC 18013-ADD-API-02: W przypadku gdy europejski portfel tożsamości cyfrowej usuwa na żądanie użytkownika PID lub EAA uprzednio ujawnione pośredniczącemu API, które działa zgodnie z załącznikiem C do [16], europejski portfel tożsamości cyfrowej informuje pośredniczące API, że nie przechowuje już tych danych.

— ISO/IEC 18013-ADD-API-03: Jeżeli użytkownik odinstaluje swój europejski portfel tożsamości cyfrowej, europejski portfel tożsamości cyfrowej informuje pośredniczące API działające zgodnie z załącznikiem C do [16], że nie przechowuje już żadnych wcześniej ujawnionych PID ani EAA.

— ISO/IEC 18013-ADD-API-04: Europejski portfel tożsamości cyfrowej zapewnia globalne ustawienia użytkownika umożliwiające wyłączenie ujawniania przechowywanych EAA za pośrednictwem pośredniczącego API, zgodnie z normą ISO/IEC 18013-ADD-API-01. Jeżeli ustawienie to jest wyłączone, europejski portfel tożsamości cyfrowej nie ogłasza ani nie odpowiada na żądania prezentacji lub wydania realizowane z wykorzystaniem API.

— ISO/IEC 18013-ADD-API-05: Europejskie portfele tożsamości cyfrowej weryfikują w przepływach między urządzeniami za pomocą API pośredniczącego, czy urządzenie wchodzące w interakcję znajduje się w bliskiej odległości fizycznej od europejskiego portfela tożsamości cyfrowej, korzystając z bezpiecznego, bezpośredniego i kierowanego przez użytkownika lokalnego kanału komunikacji, takiego jak technologia komunikacji bezprzewodowej bliskiego zasięgu, w celu przeprowadzenia kontroli fizycznej bliskości.

— *UWAGA:* CTAP 2.3 umożliwia wykorzystanie BLE do przeprowadzenia kontroli bliskiej odległości fizycznej, a po wdrożeniu przez oba urządzenia umożliwia również przesyłanie danych między urządzeniami za pomocą technologii transmisji krótkiego zasięgu. Podstawowe systemy operacyjne, przeglądarki, pośredniczące API lub wszelkie inne warstwy techniczne pozostające poza kontrolą europejskiego portfela tożsamości cyfrowej powinny preferować przeprowadzanie zarówno kontroli bliskiej odległości fizycznej, jak i przekazywanie danych między tymi dwoma urządzeniami przy użyciu lokalnego kanału komunikacji, co umożliwia CTAP 2.3, przed korzystaniem z usług hybrydowego tunelu CTAP.

13) 6.2. Wymagania dotyczące europejskiego portfela tożsamości cyfrowej i wsparcia dla stron ufających

— OIDFVP-HAIP-SUPPORT-02: Europejski portfel tożsamości cyfrowej musi spełniać wymogi określone w pkt 6.5 niniejszego załącznika.

— OIDFVP-HAIP-SUPPORT-03: Europejski portfel tożsamości cyfrowej nie powinien obsługiwać mechanizmu opartego na przekierowaniach określonego w pkt 6.4 w odniesieniu do przepływów prezentacji między urządzeniami.

— *UWAGA 3:* Korzystanie z tego mechanizmu jest podatne na ataki, np. ataki typu »session fixation«. Łagodzenie takich ataków leży w gestii stron ufających. Wdrożenie tego mechanizmu nie powinno prowadzić do niezgodności z przepisami.

— OIDFVP-HAIP-SUPPORT-05: Strona ufająca musi spełniać wymagania określone w pkt 6.5 niniejszego załącznika.

— *UWAGA 5:* nieważny.

14) 6.3.1. General requirements

— OIDFVP-HAIP-GEN-01: Stosuje się wszystkie obowiązkowe wymagania określone w pkt 5, 5.3, 7 i 8 HAIP [11].

— *UWAGA 1:* »HAIP [11] sekcja 5« odnosi się wyłącznie do wymagań, które znajdują się bezpośrednio pod nagłówkiem sekcji 5. Nie obejmuje to sekcji 5.1, 5.2 i 5.3.

— OIDFVP-HAIP-GEN-03: Jeżeli niniejszy załącznik zmienia wymaganie z OpenID4VC-HAIP [11], pierwszeństwo ma zmienione wymaganie określone w niniejszym załączniku.

— *UWAGA 2:* Pozwala to na przykład przekształcić wymaganie opcjonalne z OpenID4VC-HAIP [11] w wymaganie obowiązkowe lub rozszerzyć wymagania obowiązkowe.

— OIDFVP-HAIP-GEN-04: Jeżeli format żądanego poświadczenia jest zgodny z [10], strony ufające oraz europejskie portfele tożsamości cyfrowej muszą być zgodne z profilem »ISO mdocs« określonym w pkt 6 [11].

— *UWAGA 3:* Dla jasności: »profil mdocs ISO« w HAIP oznacza, że strony ufające oraz europejskie portfele tożsamości cyfrowej muszą spełniać mające zastosowanie wymagania określone w załączniku B.2 [7].

— OIDFVP-HAIP-GEN-05: Jeżeli format wymaganego poświadczenia jest zgodny z [2], strony ufające oraz europejskie portfele tożsamości cyfrowej muszą być zgodne z profilem »IETF SD-JWT VCs« określonym w pkt 6 [11].

— *UWAGA 4:* Dla jasności: »profil IETF SD-JWT VCs« oznacza, że strony ufające oraz europejskie portfele tożsamości cyfrowej muszą spełniać wymagania określone w załączniku B.3 do [7], a także wymagania określone w pkt 6.1 [11].

15) 6.3.2.1. General requirements

— OIDFVP-HAIP-COMMON-REQ-01: nieważny.

16) 6.3.2.2. Wymagania dotyczące obiektu żądania

— OIDFVP-HAIP-COMMON-REQ-RO-02: nieważny

— OIDFVP-HAIP-COMMON-REQ-RO-03: nieważny

— OIDFVP-HAIP-COMMON-REQ-RO-04: nieważny

— OIDFVP-HAIP-COMMON-REQ-RO-05: nieważny

— OIDFVP-HAIP-COMMON-REQ-RO-06: nieważny.

— OIDFVP-HAIP-COMMON-REQ-RO-07: nieważny

— OIDFVP-HAIP-COMMON-REQ-RO-08: nieważny

— OIDFVP-HAIP-COMMON-REQ-RO-09: nieważny

— OIDFVP-HAIP-COMMON-REQ-RO-10: nieważny

— OIDFVP-HAIP-COMMON-REQ-RO-11: nieważny

— OIDFVP-HAIP-COMMON-REQ-RO-12: nieważny

— *Uwaga 2:* nieważny

— OIDFVP-HAIP-COMMON-REQ-RO-13: Jeden z elementów parametru verifier_info obejmuje certyfikat rejestracji.

— OIDFVP-HAIP-COMMON-REQ-RO-23: Certyfikat końcowy wskazany w pkt 5.9.3 OpenID4VP do stosowania z »x509_hash Client Identifier Prefix« jest certyfikatem dostępu RP, jak określono w ETSI TS 119 475 [14].

17) 6.3.3. Authorization Response (EAAP response) profile

— OIDFVP-HAIP-COMMON-RESP-01: nieważny.

18) 6.4.1. General requirements

— OIDFVP-HAIP-REDIRECTS-04: nieważny.

— *UWAGA:* nieważny.

19) 6.5.2. Additional requirements

— OIDFVP-HAIP-ADD-API-01: Europejski portfel tożsamości cyfrowej domyślnie ujawnia pośredniczącemu API działającemu zgodnie z pkt 5.2 [11] informację o obecności wszystkich przechowywanych typów EAA, jednak nie ujawnia atrybutów ani ich wartości w tych poświadczeniach.

— OIDFVP-HAIP-ADD-API-04: Jeżeli europejski portfel tożsamości cyfrowej obsługuje pośredniczące API działające zgodnie z OIDFVP-HAIP-ADD-API-01, zapewnia on globalne ustawienie użytkownika umożliwiające wyłączenie ujawniania przechowywanych EAA za pośrednictwem tego API. Po ustawieniu wyłączenia ujawniania europejski portfel tożsamości cyfrowej powinien następnie umożliwić użytkownikowi wybór poszczególnych poświadczeń do ujawnienia pośredniczącemu API.

— OIDFVP-HAIP-ADD-API-05: Europejskie portfele tożsamości cyfrowej weryfikują w przepływach między urządzeniami, za pomocą API pośredniczącego, czy urządzenie wchodzące w interakcję znajduje się w bliskiej odległości fizycznej od europejskiego portfela tożsamości cyfrowej, korzystając z bezpiecznego, bezpośredniego i kierowanego przez użytkownika lokalnego kanału komunikacji, takiego jak technologia komunikacji bezprzewodowej bliskiego zasięgu, w celu przeprowadzenia kontroli fizycznej bliskości.

— *UWAGA 5:* CTAP 2.3 umożliwia wykorzystanie BLE do przeprowadzenia kontroli bliskiej odległości fizycznej, a po wdrożeniu przez oba urządzenia umożliwia również przesyłanie danych między urządzeniami za pomocą technologii transmisji krótkiego zasięgu. Podstawowe systemy operacyjne, przeglądarki, pośredniczące API lub wszelkie inne warstwy techniczne pozostające poza kontrolą europejskiego portfela tożsamości cyfrowej powinny preferować przeprowadzanie zarówno kontroli bliskiej odległości fizycznej, jak i przekazywanie danych między tymi dwoma urządzeniami przy użyciu lokalnego kanału komunikacji, co umożliwia CTAP 2.3, przed korzystaniem z usług hybrydowego tunelu CTAP.

20) 6.5.3. Specific requirements when requesting ISO/IEC 18013-5 EAAP

— OIDFVP-HAIP-ISO/IEC_18013_5_REQ-02: Wszystkie wymagania określone w niniejszym dokumencie mające zastosowanie do struktur żądania i odpowiedzi na żądanie dotyczące wyrobów określonych w normie ISO/IEC 18013-5 mają również zastosowanie w przypadku, gdy europejski portfel tożsamości cyfrowej otrzymuje żądanie prezentacji ISO/IEC mdoc za pośrednictwem mechanizmu transmisji z wykorzystaniem API określonego w pkt C.1 [16].”