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

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) Europejskie ramy tożsamości cyfrowej ustanowione rozporządzeniem (UE) nr 910/2014 stanowią kluczowy element budowy bezpiecznego i interoperacyjnego ekosystemu tożsamości cyfrowej w całej Unii. Ramy te – których podstawę stanowią europejskie portfele tożsamości cyfrowej („portfele") – mają na celu ułatwienie dostępu do usług w państwach członkowskich osobom fizycznym i prawnym, jednocześnie zapewniając ochronę danych osobowych i prywatności.

(2) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 ([2]) oraz – w stosownych przypadkach – dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady ([3]) mają zastosowanie do wszystkich czynności przetwarzania danych osobowych na podstawie niniejszego rozporządzenia.

(3) W art. 5a ust. 23 rozporządzenia (UE) nr 910/2014 upoważniono Komisję, w razie potrzeby, do ustanowienia odpowiednich specyfikacji i procedur. Ustanawia się je za pomocą czterech rozporządzeń wykonawczych dotyczących: protokołów i interfejsów [rozporządzenie wykonawcze Komisji 2024/2982 ([4]) 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], integralności i podstawowych funkcji [rozporządzenie wykonawcze Komisji (UE) 2024/2979 ([5]) ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do integralności i podstawowych funkcji europejskich portfeli tożsamości cyfrowej], danych identyfikujących osobę i elektronicznego poświadczenia atrybutów [rozporządzenie wykonawcze Komisji (UE) 2024/2977 ([6]) w sprawie ustanowienia zasad 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], a także notyfikowania Komisji [rozporządzenie wykonawcze Komisji (UE) 2024/2980 ([7]) 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]. W niniejszym rozporządzeniu ustanawia się odpowiednie wymogi dotyczące integralności i podstawowych funkcji europejskich portfeli tożsamości cyfrowej.

([1]) Dz.U. L 257 z 28.8.2014, s. 73, ELI: https://eur-lex.europa.eu/eli/reg/2014/910/oj.

([2]) 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).

([3]) Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (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).

([4]) 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).

([5]) 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).

([6]) 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).

([7]) 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).

(4) Komisja regularnie przeprowadza ocenę nowych technologii, praktyk, norm lub specyfikacji technicznych. Aby zapewnić maksymalną harmonizację działań państw członkowskich w zakresie opracowywania i certyfikacji portfeli, specyfikacje techniczne określone w niniejszym rozporządzeniu opierają się na pracach przeprowadzonych na podstawie zalecenia 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 ([8]), w szczególności na podstawie architektury i ram odniesienia. Zgodnie z motywem 75 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1183 ([9]) Komisja powinna, w razie potrzeby, poddawać niniejsze rozporządzenie wykonawcze przeglądowi i aktualizacji, aby zachować aktualność względem globalnych zmian, architektury i ram odniesienia oraz przestrzegać najlepszych praktyk na rynku wewnętrznym.

(5) W celu zapewnienia precyzyjnej komunikacji, rozróżnienia technicznego i jasnego podziału obowiązków konieczne jest wyszczególnienie różnych komponentów i konfiguracji portfeli. Rozwiązanie w zakresie portfela należy rozumieć jako kompletny system zapewniony przez dostawcę portfela, który jest niezbędny do obsługi portfela. Powinno to obejmować komponenty oprogramowania i sprzętu, a także usługi, ustawienia i konfiguracje niezbędne do zapewnienia prawidłowego funkcjonowania portfela. Rozwiązanie w zakresie portfela może znajdować się na urządzeniach i w środowiskach użytkowników oraz w strukturze zaplecza dostawcy. Jednostkę portfela należy rozumieć jako specyficzną konfigurację rozwiązania w zakresie portfela dostosowaną do indywidualnego użytkownika. Powinna ona obejmować aplikację zainstalowaną na urządzeniu lub w środowisku użytkownika portfela, z którą użytkownik portfela wchodzi w bezpośrednią interakcję („instancja portfela"), oraz niezbędne zabezpieczenia w celu ochrony danych i transakcji użytkowników. Zabezpieczenia te powinny obejmować specjalne oprogramowanie lub sprzęt do szyfrowania i zabezpieczania informacji szczególnie chronionych. Instancja portfela powinna być częścią jednostki portfela i umożliwiać użytkownikowi portfela dostęp do funkcji jego portfela.

(6) Bezpieczne aplikacje kryptograficzne portfela będące oddzielnymi specjalistycznymi komponentami jednostki portfela są niezbędne nie tylko do ochrony aktywów krytycznych, takich jak prywatne klucze kryptograficzne, lecz również do zapewnienia kluczowych funkcji, takich jak prezentacja elektronicznych poświadczeń atrybutów. Wykorzystanie wspólnych specyfikacji technicznych może ułatwiać dostęp do wbudowanych bezpiecznych elementów ze strony dostawców portfeli. Bezpieczne aplikacje kryptograficzne portfela mogą być dostarczane na różne sposoby i różnym rodzajom bezpiecznych urządzeń kryptograficznych portfela. W przypadku gdy opracowywane na zamówienie bezpieczne aplikacje kryptograficzne portfela są dostarczane przez dostawców portfeli w formie apletu Java Card dla wbudowanych bezpiecznych elementów, dostawcy portfeli powinni przestrzegać norm wymienionych w załączniku I lub równoważnych specyfikacji technicznych.

(7) Jednostki portfela mają umożliwiać dostawcom danych identyfikujących osobę lub elektronicznych poświadczeń atrybutów weryfikację, czy te dane lub poświadczenia są wydawane rzeczywistym jednostkom portfela danego użytkownika portfela.

(8) Aby zapewnić uwzględnienie ochrony danych na etapie projektowania i domyślną ochronę danych, portfele powinny być wyposażone w najnowocześniejsze dostępne technologie zapewniające lepszą ochronę prywatności. Funkcje te powinny umożliwiać korzystanie z portfeli bez możliwości śledzenia użytkownika portfela przez różne strony ufające portfela, jeśli jest to odpowiednie w danym scenariuszu. Na przykład dostawcy portfela powinni rozważyć najnowocześniejsze środki ochrony prywatności w odniesieniu do poświadczeń jednostki portfela, takie jak stosowanie efemerycznych poświadczeń jednostki portfela lub podział wydawania na części. Ponadto wbudowane reguły ujawniania powinny ostrzegać użytkowników portfela przed niewłaściwym lub nielegalnym ujawnieniem atrybutów pochodzących z elektronicznych poświadczeń atrybutów.

(9) Poświadczenia jednostki portfela powinny umożliwiać stronom ufającym portfela, które żądają atrybutów od jednostek portfela, weryfikację statusu ważności jednostki portfela, z którą się komunikują, ponieważ poświadczenia jednostki portfela zostają unieważniane, gdy jednostka portfela przestaje być uznawana za ważną. Informacje dotyczące statusu ważności jednostek portfela powinny być udostępniane w sposób interoperacyjny, aby zagwarantować możliwość korzystania z nich przez wszystkie strony ufające portfela. Ponadto w przypadkach, gdy użytkownicy portfela utracili swoje jednostki portfela lub nie mają już nad nimi kontroli, dostawcy portfela powinni umożliwić użytkownikom portfela wystąpienie z żądaniem o unieważnienie jednostki portfela. Aby zapewnić prywatność i brak możliwości powiązania, państwa członkowskie powinny stosować techniki ochrony prywatności również w odniesieniu do poświadczenia jednostki portfela. Może to obejmować wykorzystanie wielu poświadczeń jednostki portfela do różnych celów, ujawnianie jedynie mało istotnych informacji na temat portfela, które są niezbędne do przeprowadzenia transakcji, lub ograniczenie okresu obowiązywania poświadczenia jednostki portfela jako alternatywy wobec stosowania identyfikatorów unieważnień.

([8]) Dz.U. L 210 z 14.6.2021, s. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([9]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (Dz.U. L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(10) W celu zapewnienia, aby wszystkie portfele były technicznie wyposażone w możliwość odbioru i prezentacji danych identyfikujących osobę i elektronicznych poświadczeń atrybutów w scenariuszach transgranicznych bez uszczerbku dla interoperacyjności, portfele powinny obsługiwać z góry określone rodzaje formatów danych i selektywne ujawnianie. Jak określono w rozporządzeniu (UE) nr 910/2014, selektywne ujawnianie polega na umożliwieniu właścicielowi danych ujawniania jedynie niektórych części większego zbioru danych, aby podmiot otrzymujący mógł uzyskać tylko takie informacje, które są niezbędne do świadczenia usługi żądanej przez użytkownika. Ponieważ portfele mają umożliwiać użytkownikowi selektywne ujawnianie atrybutów, normy wymienione w załączniku II powinny zostać wdrożone w sposób umożliwiający działanie tej funkcji portfeli. Ponadto portfele mogą obsługiwać inne formaty i funkcjonalności, aby ułatwić realizację specyficznych przypadków użycia.

(11) Rejestrowanie transakcji jest ważnym narzędziem zapewniającym przejrzystość, umożliwiając użytkownikowi portfela uzyskanie wglądu do transakcji. Co więcej, rejestry powinny być wykorzystywane do umożliwienia szybkiej i łatwej wymiany niektórych informacji, na wniosek użytkownika portfela, z właściwymi organami nadzorczymi ustanowionymi na podstawie art. 51 rozporządzenia (UE) 2016/679 w przypadku podejrzanego zachowania stron ufających portfela.

(12) Aby użytkownik portfela mógł złożyć podpis elektroniczny, należy mu wydać kwalifikowany certyfikat powiązany z kwalifikowanym urządzeniem do składania podpisu elektronicznego. Użytkownik portfela powinien mieć dostęp do aplikacji służącej do składania podpisu. Chociaż wydawanie kwalifikowanych certyfikatów jest usługą kwalifikowanych dostawców usług zaufania, dostawcy portfela lub inne podmioty powinni mieć możliwość oferowania również pozostałych komponentów. Przykładowo kwalifikowane urządzenia do składania podpisu elektronicznego mogą być zarządzane przez kwalifikowanych dostawców usług zaufania w charakterze usługi lub mogą być zainstalowane lokalnie na urządzeniu użytkownika portfela, na przykład jako karta inteligentna. Podobnie aplikacje służące do składania podpisu mogą być zintegrowane z instancją portfela, mogą stanowić odrębną aplikację na urządzeniu użytkownika portfela lub być dostarczane zdalnie.

(13) Obiekty związane z eksportem i przenoszeniem danych mogą rejestrować dane identyfikujące osobę i elektroniczne poświadczenia atrybutów wydane danej jednostce portfela. Obiekty te umożliwiają użytkownikom portfela pobieranie odpowiednich danych z ich jednostki portfela w celu wzmocnienia ich prawa do przenoszenia danych. Dostawców portfela zachęca się do stosowania tych samych rozwiązań technicznych, aby również wdrażać procesy tworzenia kopii zapasowych i odzyskiwania jednostek portfela, umożliwiając odzyskiwanie utraconych jednostek portfela lub przekazywanie informacji od jednego dostawcy portfela do drugiego, w stosownych przypadkach i w zakresie, w jakim można tego dokonać bez naruszania prawa do ochrony danych i bezpieczeństwa ekosystemu tożsamości cyfrowej.

(14) Generowanie pseudonimów specyficznych dla danej strony ufającej portfela powinno umożliwić użytkownikom portfela uwierzytelnianie bez dostarczania niepotrzebnych informacji stronom ufającym portfela. Jak określono w rozporządzeniu (UE) nr 910/2014, użytkownikom portfeli nie można utrudniać dostępu do usług pod pseudonimem, jeżeli nie występuje prawny wymóg podania oficjalnej tożsamości w celu uwierzytelnienia. Portfele mają zatem zawierać funkcję generowania pseudonimów wybranych i zarządzanych przez użytkownika, służących do uwierzytelniania podczas dostępu do usług online. Wdrożenie specyfikacji określonych w załączniku V powinno odpowiednio umożliwić działanie tych funkcji. Co więcej, strony ufające portfela nie mogą zwracać się do użytkowników o udostępnienie jakichkolwiek danych innych niż te, które zostały wskazane do celów zamierzonego użycia portfeli w rejestrze stron ufających. Użytkownicy portfela powinni mieć możliwość weryfikacji danych rejestracyjnych stron ufających w dowolnym momencie.

(15) Zgodnie z rozporządzeniem (UE) 2024/1183 państwa członkowskie nie mogą, bezpośrednio ani pośrednio, ograniczać dostępu do usług publicznych lub prywatnych dla osób fizycznych lub prawnych, które nie decydują się na korzystanie z portfeli, powinny natomiast udostępnić odpowiednie alternatywne rozwiązania.

(16) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([10]) skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 30 września 2024 r.

([10]) 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).

(17) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią komitetu, o którym mowa w art. 48 rozporządzenia (UE) nr 910/2014,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

PRZEPISY OGÓLNE

Artykuł 1

Przedmiot i zakres stosowania

W niniejszym rozporządzeniu ustanawia się przepisy dotyczące integralności i podstawowych funkcji portfeli; przedmiotowe przepisy podlegają regularnej aktualizacji w celu zapewnienia zgodności z rozwojem technologii i opracowywanymi normami oraz z pracami prowadzonymi na podstawie zalecenia Komisji (UE) 2021/946, w szczególności z architekturą i ramami odniesienia.

Artykuł 2

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „bezpieczna aplikacja kryptograficzna portfela" oznacza aplikację, która zarządza aktywami krytycznymi, łącząc się z funkcjami kryptograficznymi i niekryptograficznymi zapewnianymi przez bezpieczne urządzenie kryptograficzne portfela oraz korzystając z tych funkcji;

2) „jednostka portfela" oznacza niepowtarzalną konfigurację rozwiązania w zakresie portfela, która obejmuje instancje portfela, bezpieczne aplikacje kryptograficzne portfela i bezpieczne urządzenia kryptograficzne portfela dostarczane przez dostawcę portfela indywidualnemu użytkownikowi portfela;

3) „aktywa krytyczne" oznaczają aktywa wewnątrz jednostki portfela lub z nią związane o tak istotnym znaczeniu, że naruszenie ich dostępności, poufności lub integralności miałoby bardzo poważny, szkodliwy wpływ na zdolność do polegania na danej jednostce portfela;

4) „dostawca danych identyfikujących osobę" oznacza osobę fizyczną lub prawną odpowiedzialną za wydanie i unieważnienie danych identyfikujących osobę oraz za zapewnienie, aby dane identyfikujące osobę odnoszące się do użytkownika były powiązane kryptograficznie z jednostką portfela;

5) „użytkownik portfela" oznacza użytkownika, który kontroluje jednostkę portfela;

6) „strona ufająca portfela" oznacza stronę ufającą, która zamierza polegać na jednostkach portfela w celu świadczenia usług publicznych lub prywatnych za pośrednictwem cyfrowej interakcji;

7) „dostawca portfela" oznacza osobę fizyczną lub prawną, która dostarcza rozwiązania w zakresie portfela;

8) „poświadczenie jednostki portfela" oznacza obiekt danych, który opisuje komponenty jednostki portfela lub umożliwia uwierzytelnienie oraz walidację tych komponentów;

9) „wbudowane reguły ujawniania" oznaczają zbiór zasad wbudowanych w elektronicznym poświadczeniu atrybutów przez dostawcę tego poświadczenia; zasady te określają warunki, jakie musi spełnić strona ufająca portfela, aby uzyskać dostęp do elektronicznego poświadczenia atrybutów;

10) „instancja portfela" oznacza aplikację zainstalowaną i skonfigurowaną na urządzeniu lub w środowisku użytkownika portfela, która jest częścią jednostki portfela i z której użytkownik portfela korzysta do interakcji z daną jednostką portfela;

11) „rozwiązanie w zakresie portfela" oznacza połączenie oprogramowania, sprzętu, usług, ustawień i konfiguracji, z uwzględnieniem instancji portfela, co najmniej jednej bezpiecznej aplikacji kryptograficznej portfela oraz co najmniej jednego bezpiecznego urządzenia kryptograficznego portfela;

12) „bezpieczne urządzenie kryptograficzne portfela" oznacza urządzenie odporne na manipulacje, które zapewnia otoczenie połączone z bezpieczną aplikacją kryptograficzną portfela i przez nią wykorzystywane, aby chronić aktywa krytyczne i zapewniać funkcje kryptograficzne na potrzeby bezpiecznego wykonywania operacji krytycznych;

13) „operacja kryptograficzna portfela" oznacza mechanizm kryptograficzny niezbędny w kontekście uwierzytelniania użytkownika portfela oraz wydawania lub prezentacji danych identyfikujących osobę lub elektronicznych poświadczeń atrybutów;

14) „certyfikat dostępu strony ufającej portfela" oznacza certyfikat pieczęci lub podpisów elektronicznych uwierzytelniający i walidujący stronę ufającą portfela, wydany przez dostawcę certyfikatów dostępu strony ufającej portfela;

15) „dostawca certyfikatów dostępu strony ufającej portfela" oznacza osobę fizyczną lub prawną upoważnioną przez państwo członkowskie do wydawania certyfikatów dostępu strony ufającej stronom ufającym portfela zarejestrowanym w tym państwie członkowskim.

ROZDZIAŁ II

INTEGRALNOŚĆ EUROPEJSKICH PORTFELI TOŻSAMOŚCI CYFROWEJ

Artykuł 3

Integralność jednostki portfela

1. Jednostki portfela nie mogą wykonywać żadnych funkcji wymienionych w art. 5a ust. 4 rozporządzenia (UE) nr 910/2014, z wyjątkiem uwierzytelniania użytkownika portfela w celu uzyskania dostępu do jednostki portfela, do czasu gdy jednostka portfela skutecznie uwierzytelni użytkownika portfela.

2. Dostawcy portfela – w odniesieniu do każdej jednostki portfela – podpisują lub opatrują pieczęcią co najmniej jedno poświadczenie jednostki portfela zgodne z wymogami określonymi w art. 6. Certyfikat stosowany do podpisywania lub opatrywania pieczęcią poświadczenia jednostki portfela wydaje się na podstawie certyfikatu wymienionego w zaufanej liście, o której mowa w rozporządzeniu wykonawczym (UE) 2024/2980.

Artykuł 4

Instancje portfela

1. Instancje portfela wykorzystują co najmniej jedno bezpieczne urządzenie kryptograficzne portfela do zarządzania aktywami krytycznymi.

2. Dostawcy portfela zapewniają integralność, autentyczność i poufność komunikacji między instancjami portfela a bezpiecznymi aplikacjami kryptograficznymi portfela.

3. W przypadku gdy aktywa krytyczne odnoszą się do przeprowadzania identyfikacji elektronicznej na wysokim poziomie bezpieczeństwa, operacje kryptograficzne portfela lub inne operacje przetwarzania aktywów krytycznych przeprowadza się zgodnie z wymogami dotyczącymi cech charakterystycznych i konstrukcji środków identyfikacji elektronicznej na wysokim poziomie bezpieczeństwa, jak określono w rozporządzeniu wykonawczym Komisji (UE) 2015/1502 ([11]).

Artykuł 5

Bezpieczne aplikacje kryptograficzne portfela

1. Dostawcy portfela zapewniają, aby bezpieczne aplikacje kryptograficzne portfela:

a) wykonywały operacje kryptograficzne portfela wykorzystujące aktywa krytyczne inne niż te, które są potrzebne jednostce portfela do uwierzytelnienia użytkownika portfela, wyłącznie w przypadkach, gdy aplikacje te skutecznie uwierzytelniły użytkowników portfela;

([11]) Rozporządzenie wykonawcze Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów bezpieczeństwa w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz.U. L 235 z 9.9.2015, s. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

b) jeżeli uwierzytelniają użytkowników portfela w kontekście przeprowadzania identyfikacji elektronicznej na wysokim poziomie bezpieczeństwa; dokonywały uwierzytelnienia użytkowników portfela zgodnie z wymogami dotyczącymi cech charakterystycznych i konstrukcji środków identyfikacji elektronicznej na wysokim poziomie bezpieczeństwa określonymi w rozporządzeniu wykonawczym (UE) 2015/1502;

c) były w stanie bezpiecznie generować nowe klucze kryptograficzne;

d) były w stanie w bezpieczny sposób usuwać aktywa krytyczne;

e) były w stanie wygenerować dowód posiadania kluczy prywatnych;

f) chroniły klucze prywatne generowane przez te bezpieczne aplikacje kryptograficzne portfela podczas funkcjonowania kluczy;

g) spełniały wymogi dotyczące cech charakterystycznych i konstrukcji środków identyfikacji elektronicznej na wysokim poziomie bezpieczeństwa określone w rozporządzeniu wykonawczym (UE) 2015/1502;

h) były jedynymi komponentami zdolnymi do wykonywania operacji kryptograficznych portfela i wszelkich innych operacji z wykorzystaniem aktywów krytycznych w kontekście przeprowadzania identyfikacji elektronicznej na wysokim poziomie bezpieczeństwa.

2. W przypadku gdy dostawcy portfeli zdecydują się dostarczyć bezpieczną aplikację kryptograficzną portfela dla wbudowanego bezpiecznego elementu, przedmiotowi dostawcy portfeli opierają swoje rozwiązanie techniczne na specyfikacjach technicznych wymienionych w załączniku I lub na innych równoważnych specyfikacjach.

Artykuł 6

Autentyczność i ważność jednostki portfela

1. Dostawcy portfela mają obowiązek zapewnić, aby każda jednostka portfela zawierała poświadczenia jednostki portfela.

2. Dostawcy portfela zapewniają, aby poświadczenia jednostki portfela, o których mowa w ust. 1, zawierały klucze publiczne oraz aby odpowiadające im klucze prywatne były chronione przez bezpieczne urządzenie kryptograficzne portfela.

3. Dostawcy portfela:

a) informują użytkowników portfela o ich prawach i obowiązkach w odniesieniu do ich jednostki portfela;

b) zapewniają niezależne od jednostek portfela mechanizmy bezpiecznej identyfikacji i uwierzytelniania użytkowników portfela;

c) zapewniają użytkownikom portfela prawo do żądania unieważnienia poświadczeń jednostki portfela przy użyciu mechanizmów uwierzytelniania, o których mowa w lit. b).

Artykuł 7

Unieważnienie poświadczeń jednostki portfela

1. Dostawcy portfela są jedynymi podmiotami uprawnionymi do unieważnienia poświadczeń jednostki portfela wydanych jednostkom portfela, które dostarczyli.

2. Dostawcy portfela ustanawiają publicznie dostępną politykę określającą warunki i ramy czasowe unieważniania poświadczeń jednostki portfela.

3. W przypadku gdy dostawcy portfela unieważnią poświadczenia jednostki portfela, informują o tym użytkowników portfela, których to dotyczy, w ciągu 24 godzin od unieważnienia ich jednostek portfela, m.in. podając przyczynę unieważnienia oraz jego konsekwencje dla użytkownika portfela. Informacje te należy przekazać w formie zwięzłej, łatwo dostępnej oraz używając jasnego i przystępnego języka.

4. W przypadku gdy dostawcy portfela unieważnili poświadczenia jednostki portfela, udostępniają publicznie status ważności poświadczenia jednostki portfela w sposób zapewniający ochronę prywatności i opisują lokalizację tych informacji w poświadczeniu jednostki portfela.

ROZDZIAŁ III

PODSTAWOWE FUNKCJE I CECHY EUROPEJSKICH PORTFELI TOŻSAMOŚCI CYFROWEJ

Artykuł 8

Formaty danych identyfikujących osobę i elektronicznych poświadczeń atrybutów

Dostawcy portfela zapewniają, aby rozwiązania w zakresie portfela umożliwiały korzystanie z danych identyfikujących osobę i elektronicznych poświadczeń atrybutów wydanych zgodnie z wykazem norm określonym w załączniku II.

Artykuł 9

Dzienniki transakcji

1. Niezależnie od tego, czy transakcja zakończyła się pomyślnie, instancje portfela rejestrują wszystkie transakcje ze stronami ufającymi portfela i innymi jednostkami portfela, w tym składanie podpisów i pieczęci elektronicznych.

2. Zarejestrowane informacje muszą obejmować co najmniej:

a) czas i datę transakcji;

b) imię i nazwisko lub nazwę oraz niepowtarzalny identyfikator odpowiedniej strony ufającej portfela i państwo członkowskie, w którym strona ta ma siedzibę, lub, w przypadku innych jednostek portfela, odpowiednie informacje z poświadczenia jednostki portfela;

c) rodzaj lub rodzaje danych żądanych i przedstawionych w ramach transakcji;

d) w przypadku transakcji nieukończonych – przyczynę braku ich ukończenia.

3. Dostawcy portfela zapewniają integralność, autentyczność i poufność zarejestrowanych informacji.

4. Instancje portfela rejestrują zgłoszenia przesłane przez użytkownika portfela organom ochrony danych za pośrednictwem jednostki portfela.

5. Rejestry, o których mowa w ust. 1 i 2, są dostępne dla dostawcy portfela, jeżeli jest to konieczne do świadczenia usług portfela, na podstawie wyraźnej uprzedniej zgody użytkownika portfela.

6. Rejestry, o których mowa w ust. 1 i 2, pozostają dostępne tak długo, jak wymagają tego przepisy Unii lub prawo krajowe.

7. Dostawcy portfela umożliwiają użytkownikom portfela eksportowanie zarejestrowanych informacji, o których mowa w ust. 2.

Artykuł 10

Wbudowane ujawnianie

1. Dostawcy portfela zapewniają, aby elektroniczne poświadczenia atrybutów zawierające wspólne wbudowane reguły ujawniania określone w załączniku III mogły być przetwarzane przez jednostki portfela, które dostarczają.

2. Instancje portfela są w stanie przetwarzać i prezentować wbudowane reguły ujawniania, o których mowa w ust. 1, w połączeniu z danymi otrzymanymi od strony ufającej portfela.

3. Instancje portfela weryfikują, czy strona ufająca portfela spełnia wymogi zawarte we wbudowanych regułach ujawniania informacji, i informują użytkownika portfela o wyniku takiej weryfikacji.

Artykuł 11

Kwalifikowane podpisy i pieczęcie elektroniczne

1. Dostawcy portfela zapewniają, aby użytkownicy portfela mogli otrzymywać kwalifikowane certyfikaty kwalifikowanych podpisów lub pieczęci elektronicznych, które są powiązane z kwalifikowanymi urządzeniami do składania podpisu lub pieczęci mającymi charakter lokalny, zewnętrzny albo zdalny względem instancji portfela.

2. Dostawcy portfela zapewniają, aby rozwiązania w zakresie portfela były w stanie bezpiecznie łączyć się z jednym z następujących rodzajów kwalifikowanych urządzeń do składania podpisu lub pieczęci: lokalnymi, zewnętrznymi lub zdalnie zarządzanymi kwalifikowanymi urządzeniami do składania podpisu lub pieczęci na potrzeby korzystania z kwalifikowanych certyfikatów, o których mowa w ust. 1.

3. Dostawcy portfela zapewniają, aby użytkownicy portfela będący osobami fizycznymi otrzymali – przynajmniej do celów nieprofesjonalnych – bezpłatny dostęp do aplikacji służących do składania podpisu, które umożliwiają tworzenie bezpłatnych kwalifikowanych podpisów elektronicznych z wykorzystaniem certyfikatów, o których mowa w ust. 1.

Artykuł 12

Aplikacje służące do składania podpisu

1. Aplikacje służące do składania podpisu wykorzystywane przez jednostki portfela mogą być dostarczane przez dostawców portfela, dostawców usług zaufania albo przez strony ufające portfela.

2. Aplikacje służące do składania podpisu pełnią takie funkcje, jak:

a) podpisywanie lub opatrywanie pieczęcią danych przekazanych przez użytkownika portfela;

b) podpisywanie lub opatrywanie pieczęcią danych przekazanych przez stronę ufającą portfela;

c) składanie podpisów lub pieczęci zgodnie z co najmniej obowiązkowymi formatami, o których mowa w załączniku IV;

d) informowanie użytkowników portfela o wynikach procesu składania podpisu lub pieczęci.

3. Aplikacje służące do składania podpisu mogą być zintegrowane z instancjami portfela albo mieć względem nich charakter zewnętrzny. W przypadku gdy aplikacje służące do składania podpisu polegają na kwalifikowanych urządzeniach do składania podpisu na odległość i gdy są zintegrowane z instancjami portfela, wspierają interfejs programowania aplikacji, o którym mowa w załączniku IV.

Artykuł 13

Eksport i możliwość przenoszenia danych

Jednostki portfela – w przypadku gdy jest to technicznie wykonalne i z wyjątkiem aktywów krytycznych – obsługują bezpieczny eksport i możliwość przenoszenia danych osobowych użytkownika portfela, aby umożliwić mu migrację danych do jednostki portfela w ramach innego rozwiązania w zakresie portfela w sposób zapewniający wysoko poziom ochrony, jak określono w rozporządzeniu wykonawczym (UE) 2015/1502.

Artykuł 14

Pseudonimy

1. Jednostki portfela obsługują generowanie pseudonimów odnoszących się do użytkowników portfela zgodnie ze specyfikacjami technicznymi określonymi w załączniku V.

2. Jednostki portfela obsługują generowanie – na żądanie strony ufającej portfela – pseudonimu charakterystycznego i niepowtarzalnego dla tej strony ufającej portfela oraz przekazują ten pseudonim stronie ufającej portfela – sam albo w połączeniu z danymi identyfikującymi osobę lub z elektronicznym poświadczeniem atrybutów, których żąda strona ufająca portfela.

ROZDZIAŁ IV

PRZEPISY KOŃCOWE

Artykuł 15

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 28 listopada 2024 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

ZAŁĄCZNIK I

WYKAZ NORM, O KTÓRYM MOWA W ART. 5

— SAM.01 Secured Applications for Mobile - Requirements for supporting 3rd party Applets on eSIM and eSE via SAM. v1.1 2023, GSMA;

— GPC_GUI_ 217 GlobalPlatform SAM Configuration Technical specification for implementation of SAM v1.0 2024-04;

— GPC_SPE_0 34 GlobalPlatform Card Specification Technical specification for smart cards v2.3.1 2018-03;

— GPC_SPE_0 07 GlobalPlatform Amendment A Confidential Card Content Management v1.2 2019-07;

— GPC_SPE_0 13 GlobalPlatform Amendment D Secure Channel Protocol 03 v1.2 2020-04;

— GPC_SPE_0 93 GlobalPlatform Amendment F Secure Channel Protocol 11 v1.4 2024-03;

— GPD_SPE_0 75 Open Mobile API Specification OMAPI API for mobile apps to access secure elements on user devices. v3.3 2018-08, GlobalPlatform.

ZAŁĄCZNIK II

WYKAZ NORM, O KTÓRYM MOWA W ART. 8

— ISO/IEC.18013-5:2021

— „Verifiable Credentials Data Model 1.1.” (model weryfikowalnych danych uwierzytelniających 1.1.), zalecenie W3C, 3 marca 2022 r.

ZAŁĄCZNIK III

WYKAZ WSPÓLNYCH WBUDOWANYCH REGUŁ UJAWNIANIA, O KTÓRYCH MOWA W ART. 10

1. „Brak reguły” oznacza, że do elektronicznych poświadczeń atrybutów nie ma zastosowania żadna reguła.
2. „Reguła obejmująca wyłącznie uwierzytelnione strony ufające” wskazuje, że użytkownicy portfela mogą ujawniać elektroniczne poświadczenia atrybutów wyłącznie uwierzytelnionym stronom ufającym, które wyraźnie wskazano w regułach ujawniania.
3. „Szczególne źródło zaufania” oznacza, że użytkownicy portfela powinni ujawniać konkretne elektroniczne poświadczenia atrybutów wyłącznie uwierzytelnionym stronom ufającym portfela, które posiadają certyfikaty dostępu strony ufającej portfela wydane przez konkretne źródło (lub listę konkretnych źródeł) lub certyfikat(y) pośrednie.

ZAŁĄCZNIK IV

FORMATY PODPISU I PIECZĘCI, O KTÓRYCH MOWA W ART. 12

1. Obowiązkowy format podpisu lub pieczęci:

   PAdES (ang. *PDF Advanced Electronic Signature*, zaawansowany podpis elektroniczny do podpisywania plików w formacie PDF), jak określono w „ETSI EN 319 142-1 V1.1.1 (2016-04); Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

2. Wykaz opcjonalnych formatów podpisu lub pieczęci:

   a) XAdES – jak określono w „ETSI EN 319 132-1 V1.2.1 (2022-02) Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures (XAdES)" – do podpisywania plików w formacie XML;

   b) JAdES – jak określono w „ETSI TS 119 182-1 V1.2.1 (2024-07) Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures" – do podpisywania plików w formacie JSON;

   c) CAdES (ang. *CMS Advanced Electronic Signature*, zaawansowany podpis elektroniczny CMS) – jak określono w „ETSI EN 319 122-1 V1.3.1 (2023-06) Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures" – do podpisywania plików w formacie CMS;

   d) ASiC (ang. *Associated Signature Container*, podpis elektroniczny wykorzystujący konteneryzację) – jak określono w „ETSI EN 319 162-1 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers" oraz „ETSI EN 319 162-2 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers" – do podpisywania kontenerów.

3. Interfejs programowania aplikacji:

   — specyfikacja Cloud Signature Consortium (CSC) wersja 2.0 (20 kwietnia 2023 r.).

ZAŁĄCZNIK V

SPECYFIKACJE TECHNICZNE DOTYCZĄCE GENEROWANIA PSEUDONIMÓW, O KTÓRYCH MOWA W ART. 14

Specyfikacje techniczne:

— WebAuthn – Zalecenie W3C, 8 kwietnia 2021 r., poziom 2, https://www.w3.org/TR/2021/REC-webauthn-2-20210408/.