

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2025/848**z dnia 6 maja 2025 r.****ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE)
nr 910/2014 w odniesieniu do rejestracji stron ufających portfela**

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. 5b ust. 11,

a także mając na uwadze, co następuje:

- (1) Do celów rejestracji stron ufających, które zamierzają polegać na europejskich portfelach tożsamości cyfrowej („portfele”) na potrzeby świadczenia cyfrowych usług publicznych lub prywatnych zgodnie z wymogami rozporządzenia (UE) nr 910/2014, państwa członkowskie powinny ustanowić i prowadzić krajowe rejestry stron ufających portfela mających siedzibę na ich terytorium.
- (2) Komisja regularnie przeprowadza ocenę nowych technologii, praktyk, norm i 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 ⁽²⁾, w szczególności na podstawie architektury i ram odniesienia. Zgodnie z motywem 75 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1183 ⁽³⁾ Komisja powinna poddawać przeglądowi i w razie potrzeby aktualizować niniejsze rozporządzenie, aby zachować jego aktualność względem globalnych zmian, architektury i ram odniesienia oraz przestrzegać najlepszych praktyk na rynku wewnętrznym.
- (3) Aby zapewnić szeroki dostęp do rejestrów i osiągnąć interoperacyjność, państwa członkowskie powinny stworzyć interfejsy nadające się zarówno do odczytu przez człowieka, jak i do odczytu maszynowego, zgodne ze specyfikacjami technicznymi określonymi w niniejszym rozporządzeniu. Dostawcy certyfikatów dostępu strony ufającej portfela i certyfikatów rejestracji strony ufającej portfela, o ile są one dostępne, powinni również – do celów wydawania tych certyfikatów – mieć możliwość polegania na tych interfejsach.
- (4) Ponieważ polityki rejestracji zapewniają stronom ufającym portfela jasne wytyczne dotyczące procesu rejestracji, państwa członkowskie powinny określić i opublikować polityki rejestracji mające zastosowanie do krajowych rejestrów ustanowionych na ich terytorium.
- (5) Celem rejestracji stron ufających portfela jest budowanie zaufania do korzystania z portfeli dzięki większej przejrzystości. Państwa członkowskie powinny zatem podawać adekwatne informacje do wiadomości publicznej w sposób nadający się zarówno do odczytu przez człowieka, jak i do odczytu maszynowego. W związku z tym strony ufające portfela powinny przekazać niezbędne informacje, w tym swoje uprawnienia, w celu włączenia do rejestrów krajowych.
- (6) Oprócz tego, do celów przejrzystości strony ufające portfela powinny oświadczyć, czy zamierzają korzystać z identyfikacji elektronicznej osób fizycznych.
- (7) W celu zapewnienia, aby proces rejestracji był racjonalny pod względem kosztów i proporcjonalny do ryzyka, podmioty rejestrujące powinny ustanowić łatwe w obsłudze, internetowe i, w stosownych przypadkach, zautomatyzowane procesy rejestracji dla stron ufających portfela. Podmioty rejestrujące powinny weryfikować wnioski o rejestrację bez zbędnej zwłoki.

⁽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 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>).

- (8) Państwa członkowskie mają zapewnić, aby portfele były w stanie uwierzytelniać strony ufające portfela, niezależnie od tego, gdzie mają one siedzibę w Unii. W tym celu podczas potwierdzania swojej tożsamości wobec jednostek portfela strony ufające portfela powinny korzystać z certyfikatów dostępu strony ufającej portfela. Aby zagwarantować interoperacyjność tych certyfikatów we wszystkich portfelach zapewnianych w Unii, certyfikaty dostępu stron ufających portfela powinny spełniać wspólne wymagania określone w załączniku. Komisja powinna opracować zharmonizowane polityki dotyczące certyfikacji i oświadczenie dotyczące praktyk certyfikacji, które powinny być wdrażane przez państwa członkowskie. Komisja, we współpracy z państwami członkowskimi, powinna ściśle monitorować opracowywanie nowych lub alternatywnych norm, w oparciu o które można wdrożyć certyfikaty dostępu strony ufającej. W szczególności należy ocenić modele zaufania, które dowiodły swojej skuteczności i bezpieczeństwa w państwach członkowskich.
- (9) Jak określono w rozporządzeniu (UE) nr 910/2014, 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 procesie rejestracji. Użytkownicy portfela powinni mieć możliwość weryfikacji danych rejestracyjnych stron ufających portfela. Aby umożliwić użytkownikom portfela zweryfikowanie, czy atrybuty żądane przez stronę ufającą portfela wchodzą w zakres ich zarejestrowanych atrybutów, państwa członkowskie mogą wymagać wydawania certyfikatów rejestracji strony ufającej portfela zarejestrowanym stronom ufającym portfela. Aby zapewnić interoperacyjność certyfikatów rejestracji strony ufającej portfela, państwa członkowskie powinny dopilnować, aby certyfikaty te spełniały wymogi i normy określone w załączniku. W szczególności strony ufające portfela powinny oświadczyć, czy zamierzają korzystać z identyfikacji elektronicznej osób fizycznych w celu spełnienia jednego z wymogów określonych w art. 6 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 ⁽⁴⁾ do celów przejrzystości. Ponadto strony ufające nie mogą odmówić używania pseudonimów, w przypadkach gdy identyfikacja użytkownika nie jest wymagana na podstawie prawa Unii lub prawa krajowego.
- (10) Aby chronić użytkowników przed nadmiernym udostępnianiem informacji stronom ufającym portfela i ostrzegać ich w takich przypadkach, państwa członkowskie powinny włączyć do swojej polityki certyfikacji wspólne polityki dostępu, które umożliwiłyby informowanie użytkownika portfela przez rozwiązanie w zakresie portfela za każdym razem, gdy strona ufająca portfela zwraca się o udostępnienie większej ilości informacji niż te, które zarejestrowała lub do których ma prawo dostępu.
- (11) Aby chronić użytkowników portfela, podmioty rejestrujące powinny mieć możliwość zawieszenia lub cofnięcia rejestracji każdej strony ufającej portfela bez uprzedniego powiadomienia, jeżeli podmioty rejestrujące mają powody, by sądzić, że rejestracja zawiera informacje, które są nieścisłe, nieaktualne lub wprowadzające w błąd; że strona ufająca portfela nie przestrzega polityki rejestracji; lub że strona ufająca portfela w inny sposób narusza prawo Unii lub prawo krajowe lub Europejską deklarację praw i zasad cyfrowych w cyfrowej dekadzie ⁽⁵⁾ w zakresie, który odnosi się do jej roli jako strony ufającej portfela, na przykład jeżeli strona ufająca portfela nie ograniczyła w sposób właściwy zbioru atrybutów, o dostęp do których występuje. Aby zapewnić stabilność ekosystemu europejskich portfeli tożsamości cyfrowej („ekosystem portfeli”), decyzja o zawieszeniu lub cofnięciu rejestracji powinna być proporcjonalna do zakłócenia usługi spowodowanego jej zawieszeniem lub cofnięciem oraz do związanych z tym kosztów i niedogodności dla dostawcy usług i użytkownika. Organy nadzoru mają być również uprawnione do zawieszania i cofania rejestracji, jeżeli jest to wymagane, zgodnie z art. 46a ust. 4 lit. f) rozporządzenia (UE) nr 910/2014.
- (12) Do celów monitorowania *ex post*, dochodzeń prowadzonych przez organy ścigania i rozstrzygania sporów podmioty rejestrujące powinny przez okres 10 lat prowadzić ewidencję wszystkich informacji przekazanych przez strony ufające portfela zarejestrowane w ich krajowym rejestrze.
- (13) Rozporządzenie (UE) 2016/679 oraz – w stosownych przypadkach – dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady ⁽⁶⁾ mają zastosowanie do wszystkich czynności przetwarzania danych osobowych na podstawie niniejszego rozporządzenia.

⁽⁴⁾ 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>).

⁽⁵⁾ Dz.U. C 23 z 23.1.2023, s. 1.

⁽⁶⁾ 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>).

- (14) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ⁽⁷⁾ skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 31 stycznia 2025 r.
- (15) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią komitetu ustanowionego na podstawie art. 48 rozporządzenia (UE) nr 910/2014,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Przedmiot i zakres stosowania

Niniejsze rozporządzenie ustanawia zasady rejestracji stron ufających portfela.

Artykuł 2

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

- 1) „strona ufająca portfela” oznacza stronę ufającą, która zamierza polegać na jednostkach portfela w celu świadczenia usług publicznych lub prywatnych za pośrednictwem cyfrowej interakcji;
- 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) „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;
- 4) „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;
- 5) „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;
- 6) „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;
- 7) „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;
- 8) „dostawca portfela” oznacza osobę fizyczną lub prawną, która dostarcza rozwiązania w zakresie portfela;
- 9) „użytkownik portfela” oznacza użytkownika, który kontroluje jednostkę portfela;
- 10) „krajowy rejestr stron ufających portfela” oznacza krajowy elektroniczny rejestr wykorzystywany przez państwo członkowskie do udostępniania publicznie informacji na temat stron ufających portfela zarejestrowanych w tym państwie członkowskim, jak określono w art. 5b ust. 5 rozporządzenia (UE) nr 910/2014;
- 11) „dostawca certyfikatów dostępu strony ufającej portfela” oznacza osobę fizyczną lub prawną upoważnioną przez państwo członkowskie do wydawania certyfikatów dostępu strony ufającej portfela stronom ufającym portfela zarejestrowanym w tym państwie członkowskim;

⁽⁷⁾ 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>).

- 12) „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;
- 13) „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;
- 14) „podmiot rejestrujący strony ufające portfela” oznacza organ odpowiedzialny za sporządzenie i prowadzenie wykazu zarejestrowanych stron ufających portfela, mających siedzibę na jego terytorium i wyznaczony przez państwo członkowskie;
- 15) „certyfikat rejestracji strony ufającej portfela” oznacza obiekt danych, który opisuje zamierzone użycie strony ufającej i wskazuje atrybuty, które zarejestrowała strona ufająca w zamiarze żądania od użytkowników;
- 16) „dostawca certyfikatów rejestracji strony ufającej portfela” oznacza osobę fizyczną lub prawną upoważnioną przez państwo członkowskie do wydawania certyfikatów rejestracji strony ufającej stronom ufającym portfela zarejestrowanym w tym państwie członkowskim.

Artykuł 3

Rejestry krajowe

1. Państwa członkowskie ustanawiają i prowadzą co najmniej jeden krajowy rejestr stron ufających portfela zawierający informacje dotyczące zarejestrowanych stron ufających portfela mających siedzibę w danym państwie członkowskim.
2. Rejestr musi zawierać co najmniej informacje określone w załączniku I.
3. Państwa członkowskie wyznaczają co najmniej jeden podmiot rejestrujący do zarządzania co najmniej jednym krajowym rejestrem stron ufających portfela i jego obsługi.
4. Państwa członkowskie udostępniają publicznie w internecie informacje określone w załączniku I dotyczące zarejestrowanych stron ufających portfela zarówno w formie nadającej się do odczytu przez człowieka, jak i w formie przeznaczonej do automatycznego przetwarzania.
5. Informacje, o których mowa w ust. 2, są dostępne za pośrednictwem jednego wspólnego interfejsu programowania aplikacji („API”) oraz za pośrednictwem krajowej strony internetowej. Są one elektronicznie podpisane lub opatrzone pieczęcią elektroniczną przez podmiot rejestrujący lub w jego imieniu, zgodnie ze wspólnymi wymogami dla jednego API określonymi w pkt 1 załącznika II.
6. Państwa członkowskie zapewniają, aby API, o którym mowa w ust. 5, był zgodny ze wspólnymi wymogami określonymi w pkt 2 załącznika II.
7. Państwa członkowskie zapewniają, aby rejestry były zgodne z odpowiednimi wspólnymi politykami rejestracji określonymi zgodnie z art. 4.

Artykuł 4

Polityki rejestracji

1. Państwa członkowskie ustanawiają i publikują co najmniej jedną krajową politykę rejestracji mającą zastosowanie do krajowych rejestrów ustanowionych na ich terytorium.
2. Państwa członkowskie mogą uwzględnić lub ponownie wykorzystać istniejące sektorowe lub krajowe polityki rejestracji.
3. Krajowa polityka rejestracji musi zawierać przynajmniej informacje dotyczące:
 - a) procedury identyfikacji i uwierzytelniania mające zastosowanie do stron ufających portfela podczas procesu rejestracji;
 - b) wymaganej dokumentacji potwierdzającej w zakresie tożsamości, rejestracji działalności gospodarczej, mających zastosowanie uprawnień oraz innych istotnych informacji na temat strony ufającej portfela;
 - c) źródeł autentycznych lub innych oficjalnych rejestrów elektronicznych, w przypadku gdy można polegać na tych źródłach lub rejestrach w celu dostarczenia dokładnych danych;

- d) jakichkolwiek innych informacji lub innych dowodów wymaganych w ramach procesu rejestracji;
 - e) w stosownych przypadkach, zautomatyzowanych środków umożliwiających stronom ufającym portfela rejestrację lub aktualizację istniejącej rejestracji;
 - f) środków odwoławczych dostępnych dla stron ufających portfela na podstawie przepisów i procedur państwa członkowskiego, w którym utworzono rejestr krajowy;
 - g) zasady i procedury weryfikacji tożsamości zarejestrowanych stron ufających portfela oraz wszelkich innych istotnych informacji przekazanych przez tę stronę.
4. Procedury i dokumentacja, o których mowa w ust. 3 lit. a) i b), umożliwiają stronie ufającej portfela wskazanie konkretnych uprawnień, na podstawie których działa, jak określono w załączniku I.
5. W stosownych przypadkach wymogi określone w krajowej polityce rejestracji nie mogą utrudniać zautomatyzowanego procesu rejestracji.

Artykuł 5

Informacje, które należy przekazywać do rejestrów krajowych

1. Strony ufające portfela przekazują do rejestrów krajowych co najmniej informacje określone w załączniku I.
2. Strony ufające portfela zapewniają, aby przekazywane informacje były dokładne w momencie rejestracji.
3. Strony ufające portfela bez zbędnej zwłoki aktualizują wszelkie informacje uprzednio zarejestrowane w krajowym rejestrze stron ufających portfela.

Artykuł 6

Procesy rejestracji

1. Podmioty rejestrujące ustanawiają łatwe w użycie elektroniczne i w miarę możliwości zautomatyzowane procesy rejestracji dla stron ufających portfela.
2. Podmioty rejestrujące bez zbędnej zwłoki rozpatrują wnioski o rejestrację i udzielają wnioskodawcy odpowiedzi na wniosek o rejestrację w terminie określonym w mającej zastosowanie polityce rejestracji, z wykorzystaniem odpowiednich środków oraz zgodnie z przepisami i procedurami państwa członkowskiego, w którym ustanowiono rejestr krajowy.
3. W miary możliwości podmioty rejestrujące dokonują weryfikacji w sposób zautomatyzowany:
 - a) dokładność, ważność, autentyczność i integralność informacji wymaganych na mocy art. 5;
 - b) w stosownych przypadkach pełnomocnictwo przedstawicieli stron ufających portfela sporządzone i przedłożone zgodnie z przepisami i procedurami państwa członkowskiego, w którym utworzono rejestr;
 - c) rodzaj uprawnień lub uprawnień stron ufających portfela, jak określono w załączniku I;
 - d) brak istniejącej rejestracji w innym rejestrze krajowym.
4. Podmioty rejestrujące weryfikują informacje, o których mowa w ust. 3, na podstawie dokumentacji potwierdzającej dostarczonej przez strony ufające portfela oraz na podstawie odpowiednich źródeł autentycznych lub innych oficjalnych rejestrów elektronicznych w państwie członkowskim, w którym utworzono rejestr krajowy, do których podmioty rejestrujące mają dostęp zgodnie z mającymi zastosowanie przepisami i procedurami krajowymi.
5. Weryfikacja uprawnień stron ufających portfela, o których mowa w ust. 3 lit. c), odbywa się zgodnie z załącznikiem III.
6. Jeżeli podmiot rejestrujący nie może zweryfikować informacji zgodnie z ust. 3–5, podmiot rejestrujący odrzuca rejestrację.

7. Jeżeli strona ufająca portfela nie zamierza już polegać na jednostkach portfela w celu świadczenia usług publicznych lub prywatnych w ramach konkretnej rejestracji, bez zbędnej zwłoki powiadamia o tym odpowiedni podmiot rejestrujący i zwraca się o cofnięcie tej rejestracji.

Artykuł 7

Certyfikaty dostępu strony ufającej portfela

1. Państwa członkowskie upoważniają co najmniej jeden urząd certyfikacji do wydawania certyfikatów dostępu strony ufającej portfela.
2. Państwa członkowskie zapewniają, aby dostawcy certyfikatów dostępu strony ufającej portfela wydawali certyfikaty dostępu strony ufającej portfela wyłącznie zarejestrowanym stronom ufającym portfela.
3. Państwa członkowskie ustanawiają w sposób zharmonizowany pod względem syntaktycznymi i semantycznym polityki certyfikacji i oświadczenia dotyczące praktyk certyfikacji w odniesieniu do certyfikatów dostępu strony ufającej portfela, zgodnie z wymogami określonymi w załączniku IV.

Artykuł 8

Certyfikaty rejestracji strony ufającej portfela

1. Państwa członkowskie mogą upoważnić co najmniej jeden urząd certyfikacji do wydawania certyfikatów rejestracji strony ufającej portfela.
2. W przypadku gdy państwo członkowskie zezwoliło na wydanie certyfikatu rejestracji strony ufającej portfela, to państwo członkowskie:
 - a) wymaga, aby dostawcy certyfikatów rejestracji strony ufającej portfela wydawali certyfikaty rejestracji strony ufającej portfela wyłącznie zarejestrowanym stronom ufającym portfela;
 - b) zapewnia, aby każde planowane wykorzystanie było wyrażone w certyfikatach rejestracji strony ufającej portfela;
 - c) zapewnia, aby certyfikaty rejestracji strony ufającej portfela zawierały ogólną politykę dostępu, harmonizowaną w całej Unii pod względem syntaktycznym i semantycznym, zawierającą informację dla użytkowników, że strona ufająca portfela może żądać wyłącznie danych określonych w certyfikatach rejestracji w odniesieniu do zamierzonego użycia zarejestrowanego w certyfikatach rejestracji.
 - d) zapewnia, aby dostawcy rozwiązań w zakresie portfela mający siedzibę w danym państwie członkowskim spełniali wymogi ogólnej polityki dostępu przez informowanie użytkowników, gdy strona ufająca portfela żąda danych, których nie określono w certyfikacie rejestracji;
 - e) wdraża certyfikaty rejestracji strony ufającej portfela w sposób zharmonizowany pod względem syntaktycznym i semantycznym zgodnie z wymogami określonymi w załączniku V;
 - f) wdraża specjalne polityki certyfikacji i oświadczenia dotyczące praktyk certyfikacji w odniesieniu do certyfikatów rejestracji strony ufającej portfela zgodnie z wymogami określonymi w załączniku V;
 - g) zapewnia, aby strony ufające portfela podawały URL polityki prywatności w odniesieniu do zamierzonego użycia.
3. Polityka, o której mowa lit. g) wyraża się w certyfikacie rejestracji strony ufającej portfela.

Artykuł 9

Zawieszenie i anulowanie rejestracji

1. Podmioty rejestrujące zawieszają lub cofają rejestrację strony ufającej portfela, jeżeli o takie zawieszenie lub cofnięcie rejestracji wnosi organ nadzoru zgodnie z art. 46a ust. 4 lit. f) rozporządzenia (UE) nr 910/2014.
2. Podmioty rejestrujące mogą zawiesić lub cofnąć rejestrację strony ufającej portfela, jeżeli mają jeden z poniższych powodów, by sądzić, że:
 - a) rejestracja zawiera informacje, które są nieścisłe, nieaktualne lub wprowadzające w błąd;

- b) strona ufająca portfela nie przestrzega polityki rejestracji;
 - c) strona ufająca portfela zwraca się o większą liczbę atrybutów niż zarejestrowała zgodnie z art. 5 i 6;
 - d) strona ufająca portfela działa w inny sposób z naruszeniem prawa Unii lub prawa krajowego w sposób związany z jej rolą jako strony ufającej portfela.
3. Podmioty rejestrujące zawieszają lub cofają rejestrację strony ufającej portfela, jeżeli wniosek o zawieszenie lub cofnięcie rejestracji został złożony przez tę samą stronę ufającą portfela.
4. Rozważając zawieszenie lub cofnięcie rejestracji zgodnie z ust. 2, podmiot rejestrujący przeprowadza ocenę proporcjonalności i bierze pod uwagę wpływ na prywatność, bezpieczeństwo i poufność użytkowników w ekosystemie, a także dotkliwość przewidywanego zakłócenia spowodowanego zawieszeniem lub cofnięciem rejestracji oraz związane z tym koszty, zarówno dla strony ufającej portfela, jak i dla użytkownika. Na podstawie wyników tej oceny podmiot rejestrujący może zawiesić lub cofnąć rejestrację z uprzednim powiadomieniem zainteresowanej strony ufającej portfela lub bez takiego powiadomienia.
5. Jeżeli rejestracja strony ufającej portfela zostaje zawieszona lub cofnięta, podmiot rejestrujący bez zbędnej zwłoki i nie później niż 24 godziny po zawieszeniu lub cofnięciu rejestracji informuje dostawcę odpowiednich certyfikatów dostępu strony ufającej portfela, dostawcę odpowiednich certyfikatów rejestracji strony ufającej portfela oraz stronę ufającą portfela, której dotyczy zgłoszenie, o takim działaniu. Notyfikacja ta zawiera informacje o przyczynach zawieszenia lub cofnięcia rejestracji oraz o dostępnych środkach dochodzenia roszczeń lub środkach odwoławczych.
6. Dostawca certyfikatów dostępu strony ufającej portfela oraz dostawca certyfikatów dostępu strony ufającej portfela, w stosownych przypadkach, bez zbędnej zwłoki unieważnia certyfikaty dostępu strony ufającej portfela oraz certyfikaty rejestracji strony ufającej portfela, w odniesieniu do której rejestracja została zawieszona lub cofnięta.

Artykuł 10

Prowadzenie dokumentacji

Ewidencję informacji dostarczonych przez strony ufające portfela i zarejestrowanych zgodnie z załącznikiem I w celu rejestracji strony ufającej portfela oraz wydania certyfikatów dostępu strony ufającej portfela i certyfikatu rejestracji strony ufającej portfela, a także wszelkich późniejszych zmian tych informacji podmioty rejestrujące prowadzą przez okres 10 lat.

Artykuł 11

Wejście w życie

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

Niniejsze rozporządzenie stosuje się od dnia 24 grudnia 2026 r.

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

Sporządzono w Brukseli dnia 6 maja 2025 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

ZAŁĄCZNIK I

Informacje dotyczące stron ufających portfela

1. W stosownych przypadkach nazwa strony ufającej portfela podana zgodnie z oficjalnym rejestrem wraz z danymi identyfikacyjnymi zawartymi w tym oficjalnym rejestrze.
 - a) jeżeli powyższe nie ma zastosowania, stosuje się pkt 2.
2. Przyjazna dla użytkownika nazwa strony ufającej portfela, która może być nazwą handlową lub nazwą usługi rozpoznawalną dla użytkownika.
3. W stosownych przypadkach, co najmniej jeden identyfikator strony ufającej portfela podany w oficjalnym rejestrze wraz z danymi identyfikacyjnymi tego oficjalnego rejestru, wyrażony jako:
 - a) numer rejestracyjny i identyfikacyjny przedsiębiorcy (EORI), o którym mowa w rozporządzeniu wykonawczym Komisji (UE) nr 1352/2013 ⁽¹⁾;
 - b) numer rejestracyjny podany w krajowym rejestrze działalności gospodarczej;
 - c) identyfikator podmiotu prawnego (LEI), o którym mowa w rozporządzeniu wykonawczym Komisji (UE) 2022/1860 ⁽²⁾;
 - d) numer identyfikacyjny podatku od wartości dodanej (VAT);
 - e) numer akcyzowy, o którym mowa w art. 2 pkt 12 rozporządzenia Rady (UE) nr 389/2012 ⁽³⁾;
 - f) numer identyfikacji podatkowej;
 - g) niepowtarzalny identyfikator europejski (EUID), o którym mowa w rozporządzeniu wykonawczym Komisji (UE) 2021/1042 ⁽⁴⁾;
 - h) inny krajowy identyfikator lub inne krajowe identyfikatory.
4. Adres fizyczny, pod którym znajduje się siedziba strony ufającej portfela.
5. W stosownych przypadkach ujednolicony adres URL należący do strony ufającej portfela.
6. W przypadku gdy identyfikator jest wyrażony zgodnie z pkt 3 lit. a), d), f) lub h), identyfikator kraju państwa członkowskiego, w którym ma siedzibę strona ufająca portfela, jest opatrywany prefiksem, w którym wykorzystuje się kody ISO 3166-1 alfa 2, z wyjątkiem identyfikatora kraju w przypadku Grecji, który ma wartość „EL”.
7. Dane kontaktowe strony ufającej portfela, co najmniej jedna informacja z poniższych:
 - a) strona internetowa, za pomocą której można skontaktować się ze stroną ufającą portfela w sprawach dotyczących pomocy i wsparcia;
 - b) numer telefonu, pod którym można skontaktować się ze stroną ufającą portfela w sprawach dotyczących jej rejestracji i planowanego wykorzystania jednostek portfela;
 - c) adres e-mail, pod którym można skontaktować się ze stroną ufającą portfela w sprawach dotyczących jej rejestracji i planowanego wykorzystania jednostki portfela.
8. Opis rodzaju usług, które świadczy strona ufająca portfela.

⁽¹⁾ 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).

⁽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 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>).

⁽⁴⁾ Rozporządzenie wykonawcze Komisji (UE) 2021/1042 z dnia 18 czerwca 2021 r. ustanawiające zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2017/1132 w odniesieniu do specyfikacji technicznych i procedur dotyczących systemu integracji rejestrów oraz uchylające rozporządzenie wykonawcze Komisji (UE) 2020/2244 (Dz.U. L 225 z 25.6.2021, s. 7, ELI: http://data.europa.eu/eli/reg_impl/2021/1042/oj).

9. Dla każdego przypadku zamierzonego użycia wykaz danych, w tym poświadczeń i atrybutów, o które strona ufająca zamierza wystąpić, wyrażonych jako nazwa przyjazna dla użytkownika oraz nazwa techniczna, rodzaj poświadczenia i wszelkie inne syntaktyki, w które dane są pogrupowane, w formacie nadającym się do odczytu maszynowego i automatycznego przetwarzania.
10. Dla każdego przypadku zamierzonego użycia – opis zamierzonego użycia danych, o które strona ufająca portfela zamierza wystąpić do jednostek portfela.
11. Wskazanie, czy strona ufająca portfela jest podmiotem sektora publicznego.
12. Uprawnienie lub uprawnienia strony ufającej portfela wyrażone w następujący sposób:
 - a) „Service_Provider” oznacza uprawnienie strony ufającej portfela jako dostawcy usług;
 - b) „QEAA_Provider” oznacza uprawnienie strony ufającej portfela jako kwalifikowanego dostawcy usług zaufania wydającego kwalifikowane elektroniczne poświadczenia atrybutów;
 - c) „Non_Q_EAA_Provider” oznacza uprawnienie strony ufającej portfela jako dostawcy usług zaufania wydającego niekwalifikowane elektroniczne poświadczenia atrybutów.
 - d) „PUB_EAA_Provider” oznacza uprawnienie strony ufającej portfela jako dostawcy elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu;
 - e) „PID_Provider” oznacza uprawnienie strony ufającej portfela jako dostawcy danych identyfikujących osobę;
 - f) „QCert_for_eSeal_Provider” oznacza uprawnienie strony ufającej portfela jako kwalifikowanego dostawcy usług zaufania wydającego kwalifikowane certyfikaty pieczęci elektronicznych;
 - g) „QCert_for_ESig_Provider” oznacza uprawnienie strony ufającej portfela jako kwalifikowanego dostawcy usług zaufania wydającego kwalifikowane certyfikaty podpisów elektronicznych;
 - h) „rQSigCDs_Provider” oznacza uprawnienie strony ufającej portfela jako kwalifikowanego dostawcy usług zaufania świadczącego kwalifikowane usługi zaufania na potrzeby zarządzania kwalifikowanym urządzeniem do składania podpisu elektronicznego na odległość;
 - i) „rQSealCDs_Provider” oznacza uprawnienie strony ufającej portfela jako kwalifikowanego dostawcy usług zaufania świadczącego kwalifikowane usługi zaufania na potrzeby zarządzania kwalifikowanym urządzeniem do składania pieczęci elektronicznej na odległość;
 - j) „ESig_ESeal_Creation_Provider” oznacza uprawnienie strony ufającej portfela jako niekwalifikowanego dostawcy usług zaufania świadczącego niekwalifikowaną usługę zaufania na potrzeby tworzenia podpisów elektronicznych lub pieczęci elektronicznych na odległość.
13. Odnośnie do pkt 12 lit. c) państwa członkowskie mogą przewidzieć dodatkowe uprawnienia szczególne w celu określenia, które poświadczenia musi wydawać określony niekwalifikowany wydawca elektronicznego poświadczenia atrybutów.
14. W stosownych przypadkach wskazanie, że strona ufająca portfela polega na pośredniku działającym w imieniu strony ufającej, która zamierza polegać na portfelu.
15. W stosownych przypadkach powiązanie z pośrednikiem, na który polega strona ufająca portfela działającym w imieniu strony ufającej, która zamierza polegać na portfelu.

ZAŁĄCZNIK II

1. WYMOGI DOTYCZĄCE PODPISÓW LUB PIECZĘCI ELEKTRONICZNYCH STOSOWANYCH W ODNIESIENIU DO INFORMACJI UDOSTĘPNIANYCH PRZEZ PODMIOTY REJESTRUJĄCE STRONY UFAJĄCE PORTFELA, O KTÓRYCH MOWA W ART. 3
 - JavaScript Object Notation („JSON”);
 - IETF 7515 dla podpisów internetowych JSON.
2. WYMOGI DOTYCZĄCE JEDNEGO WSPÓLNEGO API, O KTÓRYM MOWA W ART. 3
 1. Jeden wspólny API:
 - a) stanowi REST API, obsługuje JSON jako format i jest podpisany zgodnie z odpowiednimi wymogami określonymi w pkt 1;
 - b) zezwala każdemu wnioskodawcy, bez uprzedniego uwierzytelnienia, na wyszukiwanie i żądanie pełnych list od rejestru, informacji na temat stron ufających portfela, umożliwiających ich częściowe dopasowanie w oparciu o określone parametry, obejmujące, w stosownych przypadkach, oficjalny numer lub numer w rejestrze działalności gospodarczej strony ufającej portfela, nazwę strony ufającej portfela lub informacje, o których mowa w art. 8 ust. 2 lit. g) i załączniku I pkt 12, 13, 14 i 15;
 - c) zapewnia, aby odpowiedzi na wnioski, o których mowa w pkt (b), które odpowiadają co najmniej jednej stronie ufającej portfela, zawierały co najmniej jedno oświadczenie dotyczące informacji o zarejestrowanych stronach ufających portfela i informacje zgodnie z załącznikiem I, aktualne i historyczne certyfikaty dostępu strony ufającej portfela oraz certyfikaty rejestracji strony ufającej portfela, ale z wyłączeniem danych kontaktowych określonych w pkt 4 załącznika I;
 - d) są publikowane jako OpenAPI, wersja 3, wraz z odpowiednią dokumentacją i specyfikacjami technicznymi zapewniającymi interoperacyjność w całej Unii;
 - e) zapewnia funkcje bezpieczeństwa, w tym bezpieczeństwo na etapie projektowania i bezpieczeństwo domyślne, w celu zapewnienia dostępności i integralności API oraz informacji dostępnych za jego pośrednictwem.
 2. Oświadczenia, o których mowa w lit. c) są w formie elektronicznie podpisanych lub opatrzonych pieczęcią elektroniczną plików JSON, o formacie i strukturze zgodnie z wymogami dotyczącymi podpisów lub pieczęci elektronicznych określonymi w pkt 1.

ZAŁĄCZNIK III

Źródło dowodów w postaci dokumentów na potrzeby weryfikacji uprawnień stron ufających portfela, o których mowa w art. 6

1. Weryfikacja, czy strona ufająca portfela jest dostawcą kwalifikowanych elektronicznych poświadczeń atrybutów, dostawcą kwalifikowanych certyfikatów podpisów lub pieczęci elektronicznych lub dostawcą kwalifikowanej usługi zaufania na potrzeby zarządzania kwalifikowanymi urządzeniami do składania podpisu elektronicznego lub pieczęci na odległość, opiera się na krajowych zaufanych listach opublikowanych zgodnie z art. 22 rozporządzenia (UE) nr 910/2014.
2. Weryfikacja, czy strona ufająca portfela jest dostawcą niekwalifikowanych elektronicznych poświadczeń atrybutów lub dostawcą podpisów lub pieczęci elektronicznych tworzonych na odległość jako niekwalifikowanych usług zaufania, opiera się, w stosownych przypadkach, na krajowych zaufanych listach opublikowanych zgodnie z art. 22 rozporządzenia (UE) nr 910/2014 lub, a w przypadku niekwalifikowanych dostawców usług zaufania, którzy nie są umieszczeni na krajowych zaufanych listach, na procedurach weryfikacji, które państwa członkowskie określiły w swoich strategiach rejestracji określonych w art. 4.
3. Weryfikacja, czy strona ufająca portfela jest dostawcą danych identyfikujących osobę, opiera się na wykazie dostawców danych identyfikujących osobę opublikowanym przez Komisję zgodnie z art. 5a ust. 18 rozporządzenia (UE) nr 910/2014.
4. Weryfikacja, czy strona ufająca portfela jest dostawcą elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu, opiera się na wykazie opublikowanym przez Komisję zgodnie z art. 45f ust. 3 rozporządzenia (UE) nr 910/2014.

ZAŁĄCZNIK IV

Wymogi dotyczące certyfikatów dostępu strony ufającej portfela, o których mowa w art. 7

1. Polityka dotycząca certyfikatów dostępu strony ufającej portfela mająca zastosowanie do wydawania certyfikatów dostępu strony ufającej portfela zawiera opis wymogów bezpieczeństwa, które mają zastosowanie do certyfikatu dostępu strony ufającej portfela, oraz zasady, które wskazują na możliwość jego stosowania, tak aby stronom ufającym portfela mogły być wydawane te certyfikaty i aby mogły one z nich korzystać podczas interakcji z rozwiązaniami w zakresie portfela.
2. W oświadczeniu dotyczącym praktyk certyfikacji w odniesieniu do certyfikatów dostępu strony ufającej portfela opisuje się praktyki stosowane przez dostawcę certyfikatów dostępu strony ufającej portfela w zakresie wydawania i unieważniania certyfikatów dostępu strony ufającej portfela, zarządzania nimi i ich ponownego wprowadzania.
3. Polityka certyfikacji i oświadczenie dotyczące praktyk certyfikacji mające zastosowanie do wydawania certyfikatów dostępu strony ufającej portfela muszą być zharmonizowane pod względem syntaktycznymi i semantycznym w całej Unii i, stosownie do przypadku, zgodne co najmniej z wymogami znormalizowanej polityki certyfikacji określonymi w normie ETSI EN 319411-1 wersja 1.4.1 (październik 2023 r.), które obejmują w szczególności:
 - a) jasny opis hierarchii infrastruktury klucza publicznego i ścieżek certyfikacji od certyfikatów dostępu strony ufającej portfela podmiotu końcowego do najwyższego szczebla hierarchii wykorzystywanego do ich wydawania, ze wskazaniem oczekiwanej kotwicy lub oczekiwanych kotwic zaufania w takiej hierarchii oraz ścieżek, które powinny opierać się na ramach zaufania wdrożonych zgodnie z art. 5a ust. 18 rozporządzenia (UE) nr 910/2014;
 - b) wyczerpujący opis procedur wydawania certyfikatów dostępu strony ufającej portfela, w tym weryfikacji tożsamości i wszelkich innych atrybutów strony ufającej portfela, której ma zostać wydany certyfikat strony ufającej portfela;
 - c) obowiązek dostawców certyfikatów dostępu strony ufającej portfela przy wydawaniu certyfikatu dostępu strony ufającej do portfela, polegający na weryfikacji, czy:
 - strona ufająca portfela jest wpisana, z ważnym statusem rejestracyjnym, do krajowego rejestru stron ufających portfela w państwie członkowskim, w którym ma siedzibę ta strona ufająca portfela;
 - wszelkie informacje zawarte w certyfikacie dostępu strony ufającej portfela są dokładne i spójne z informacjami rejestracyjnymi dostępnymi w tym rejestrze;
 - d) wyczerpujący opis procedur unieważnienia certyfikatów dostępu strony ufającej portfela;
 - e) obowiązek dostawców certyfikatów dostępu strony ufającej portfela polegający na wdrożeniu środków i procesów w zakresie:
 - stałego monitorowania wszelkich zmian w krajowym rejestrze stron ufających portfela, w których są zarejestrowane strony ufające portfela, którym wydano certyfikaty dostępu strony ufającej portfela;
 - unieważniania, jeżeli wymagają tego zmiany, wszelkich certyfikatów strony ufającej portfela, które dostawca wydał odpowiedniej stronie ufającej portfela, w szczególności gdy treść certyfikatu nie jest już prawidłowa i zgodna z zarejestrowanymi informacjami lub gdy rejestracja strony ufającej portfela została zawieszona lub unieważniona;
 - f) wyczerpujący opis procedur i mechanizmów zatwierdzania certyfikatów dostępu strony ufającej portfela w całej Unii;
 - g) obowiązek dostawców certyfikatów dostępu strony ufającej portfela polegający na umożliwieniu odpowiednim zainteresowanym stronom, w tym stronom ufającym portfela, w odniesieniu do ich własnych certyfikatów, właściwym organom nadzorczym i organom ochrony danych złożenia wniosku o unieważnienie certyfikatów dostępu strony ufającej portfela;
 - h) obowiązek dostawców certyfikatów dostępu strony ufającej portfela polegający na rejestracji wszystkich takich unieważnień w jego bazie danych certyfikatów oraz publikowania informacji o statusie unieważnienia certyfikatu w odpowiednim czasie, a w każdym razie w ciągu 24 godzin od otrzymania wniosku o unieważnienie.

- i) obowiązek dostawców certyfikatów dostępu strony ufającej portfela polegający na przekazywaniu informacji o statusie ważności lub unieważnienia certyfikatów dostępu strony ufającej portfela wydanych przez tego dostawcę;
 - j) opis, w stosownych przypadkach, w jaki sposób dostawca rejestruje wszystkie certyfikaty dostępu strony ufającej portfela, które wydał, zgodnie z wnioskiem o zgłaszanie uwag grupy zadaniowej ds. inżynierii internetowej (IETF) RFC 9162 Przejrzystość certyfikatów wersja 2.0;
 - k) obowiązek polegający na tym, że w certyfikatach dostępu stron ufających portfela należy podać:
 - miejsce, w którym dostępny jest certyfikat potwierdzający zaawansowany podpis elektroniczny lub zaawansowaną pieczęć elektroniczną na tym certyfikacie, dla całej ścieżki certyfikacji, która ma zostać utworzona aż do oczekiwanej kotwicy zaufania w hierarchii infrastruktury klucza publicznego stosowanej przez dostawcę;
 - przetwarzalne maszynowo odniesienie do mających zastosowanie polityki certyfikacji i kodeksu postępowania certyfikacyjnego;
 - informacje, o których mowa w pkt 1, 2, 3, 5, 6 i w pkt 7 lit. a), b) i c) załącznika I.
4. Określone w pkt 3 lit. g) unieważnienie staje się skuteczne natychmiast po jego opublikowaniu.
5. Informacje określone w pkt 3 lit. h) muszą być dostępne co najmniej na poziomie certyfikatu w automatyczny sposób, który jest wiarygodny, nieodpłatny i wydajny, w każdym momencie i przynajmniej po upływie okresu ważności certyfikatu zgodnie z polityką certyfikacji.
-

ZAŁĄCZNIK V

Wymogi dotyczące certyfikatów rejestracji strony ufającej portfela, o których mowa w art. 8

1. W polityce dotyczącej certyfikatu rejestracji strony ufającej portfela mającej zastosowanie do dostarczania certyfikatów rejestracji strony ufającej portfela opisuje się wymogi bezpieczeństwa, które mają zastosowanie do certyfikatu rejestracji strony ufającej portfela, oraz zasady, które wskazują na możliwość ich stosowania w odniesieniu do ich wydawania i wykorzystywania przez strony ufające portfela w kontaktach w ramach rozwiązań w zakresie portfela. Polityka dotycząca certyfikatów rejestracji strony ufającej portfela jest publikowana w formacie czytelnym dla człowieka.
2. W oświadczeniu dotyczącym praktyk w zakresie certyfikatów rejestracji strony ufającej portfela mającym zastosowanie do zapewniania certyfikatów rejestracji strony ufającej portfela opisuje się praktyki stosowane przez dostawcę certyfikatów rejestracji strony ufającej portfela w zakresie wydawania, unieważniania i ponownego wprowadzania certyfikatów rejestracji strony ufającej portfela oraz zarządzania nimi, a także, w stosownych przypadkach, sposób, w jaki odnoszą się one do certyfikatów rejestracji strony ufającej portfela wydawanych stronom ufającym portfela. Polityka dotycząca certyfikatów rejestracji strony ufającej portfela jest publikowana w formacie czytelnym dla człowieka.
3. Polityka dotycząca certyfikatów rejestracji strony ufającej portfela i oświadczenie dotyczące praktyk certyfikacji mające zastosowanie do dostarczania certyfikatów rejestracji strony ufającej portfela muszą być zharmonizowane pod względem syntaktycznym i semantycznym w całej Unii i zgodne co najmniej z mającymi zastosowanie wymogami znormalizowanej polityki certyfikacji określonymi w normie ETSI EN 319411-1 wersja 1.4.1 (z października 2023 r.), które obejmują w szczególności:
 - a) jasny opis hierarchii infrastruktury klucza publicznego i ścieżek certyfikacji od certyfikatów rejestracji strony ufającej portfela podmiotu końcowego do najwyższego szczebla hierarchii wykorzystywanego do ich wydawania, ze wskazaniem oczekiwanych kotwic zaufania w takiej hierarchii oraz ścieżek;
 - b) wyczerpujący opis procedur wydawania certyfikatów rejestracji strony ufającej portfela, w tym weryfikacji tożsamości i wszelkich atrybutów strony ufającej portfela, której ma zostać wydany certyfikat strony ufającej portfela;
 - c) obowiązek dostawcy certyfikatów rejestracji strony ufającej portfela przy wydawaniu certyfikatu rejestracji strony ufającej portfela, polegający na weryfikacji, czy:
 - strona ufająca portfela jest wpisana, z ważnym statusem rejestracyjnym, do krajowego rejestru stron ufających portfela w państwie członkowskim, w którym ma siedzibę ta strona ufająca portfela;
 - informacje zawarte w certyfikacie rejestracji strony ufającej portfela są dokładne i spójne z informacjami rejestracyjnymi dostępnymi w tym rejestrze;
 - certyfikat dostępu strony ufającej portfela jest ważny;
 - opis procedur unieważnienia certyfikatów rejestracji strony ufającej portfela jest wyczerpujący;
 - d) w ramach obowiązku dostawcy certyfikatów rejestracji strony ufającej portfela są wdrażane środki i procesy dotyczące:
 - stałego automatycznego monitorowania wszelkich zmian w krajowym rejestrze stron ufających portfela, w którym są zarejestrowane strony ufające portfela, którym wydano certyfikaty rejestracji strony ufającej portfela;
 - ponownego wydania certyfikatu rejestracji strony ufającej portfela;
 - unieważnienia certyfikatu rejestracji strony ufającej portfela wydanego odpowiedniej stronie ufającej portfela, jeżeli wymagają tego takie zmiany, w szczególności gdy treść certyfikatu nie jest już prawidłowa i zgodna z zarejestrowanymi informacjami lub gdy rejestracja strony ufającej portfela została zmieniona, zawieszona lub unieważniona;
 - e) wyczerpujący opis procedur i mechanizmów zharmonizowanego zatwierdzania certyfikatów rejestracji strony ufającej portfela;

- f) obowiązek dostawcy certyfikatów rejestracji strony ufającej portfela polegający na umożliwieniu odpowiednim zainteresowanym stronom, w tym stronom ufającym portfela w odniesieniu do ich własnych certyfikatów, właściwym organom nadzorczym i organom ochrony danych złożenia wniosku o unieważnienie certyfikatów rejestracji strony ufającej portfela;
 - g) obowiązek dostawcy certyfikatów rejestracji strony ufającej portfela polegający na rejestracji wszystkich takich unieważnień w jego bazie danych certyfikatów oraz publikowania informacji o statusie unieważnienia certyfikatu w odpowiednim czasie, a w każdym razie w ciągu 24 godzin od otrzymania wniosku o unieważnienie;
 - h) obowiązek dostawcy certyfikatów rejestracji strony ufającej portfela polegający na przekazywaniu informacji o statusie ważności lub unieważnienia certyfikatów rejestracji strony ufającej portfela wydanych przez tego dostawcę;
 - i) w stosownych przypadkach opis sposobu, w jaki dostawca certyfikatów rejestracji podmiotu ufającego portfela rejestruje wszystkie wydane przez siebie zaświadczenia o rejestracji podmiotu ufającego portfela;
 - j) obowiązek polegający na tym, że certyfikaty rejestracji stron ufających portfela:
 - muszą zawierać informację o miejscu, w którym dostępne są dane służące do walidacji zaawansowanego podpisu elektronicznego lub zaawansowanej pieczęci elektronicznej na tym certyfikacie wykorzystywane do podpisu lub opatrzenia pieczęcią certyfikatu rejestracji, dla całego łańcucha zaufania, który ma zostać utworzony aż do oczekiwanej kotwicy zaufania;
 - muszą zawierać nadające się do odczytu maszynowego odniesienie do mających zastosowanie polityki certyfikacji i oświadczenia dotyczącego praktyk certyfikacji;
 - muszą zawierać informacje, o których mowa w pkt 1, 2, 3, 5, 6 oraz 8, 9, 10, 11, 12, 13, 14 i 15 załącznika I;
 - muszą zawierać URL polityki prywatności, o którym mowa w art. 8 ust. 2 lit. g);
 - muszą obejmować ogólną politykę dostępu, o której mowa w art. 8 ust. 3.
4. Format wymiany danych dla certyfikatu rejestracji strony ufającej musi być podpisanym JSON Web Tokens (IETF RFC 7519) i CBOR Web Tokens (IETF RFC 8392).
 5. Unieważnienie, o którym mowa w pkt 3 lit. g) staje się skuteczne natychmiast po jego opublikowaniu.
 6. Informacje, o których mowa w pkt 3 lit. h), są dostępne co najmniej na poziomie certyfikatu w automatyczny sposób, który jest wiarygodny, nieodpłatny i wydajny, w każdym momencie i przynajmniej po upływie okresu ważności certyfikatu zgodnie z polityką certyfikacji.