ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2026/1735

z dnia 15 lipca 2026 r.

zmieniające rozporządzenie wykonawcze (UE) 2025/1569 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. 45d ust. 5, art. 45e ust. 2 oraz art. 45f ust. 6 i 7,

a także mając na uwadze, co następuje:

(1) Aby zapewnić najwyższy poziom harmonizacji między państwami członkowskimi w zakresie rozwoju 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 znacznym zmianom od czasu przyjęcia rozporządzenia wykonawczego Komisji (UE) 2025/1569 ([3]), należy obecnie odpowiednio zmienić rozporządzenie wykonawcze (UE) 2025/1569, aby dostosować je do nowych norm i specyfikacji.

(2) Zgodnie z celami rozporządzenia (UE) nr 910/2014 wybrano szereg norm, aby spełnić wymogi mające zastosowanie do wydawania i weryfikacji elektronicznych poświadczeń atrybutów oraz zarządzania nimi. Przedmiotowe normy powinny odzwierciedlać utrwalone praktyki i być powszechnie uznawane w odpowiednich sektorach. W razie potrzeby normy te należy dostosować lub uzupełnić, aby zapewnić wysoki poziom bezpieczeństwa i integralności elektronicznych poświadczeń atrybutów, a jednocześnie ułatwić interoperacyjność transgraniczną i skuteczne funkcjonowanie rynku wewnętrznego. Zgodnie z tym celem w niniejszym rozporządzeniu aktualizuje się wymogi mające zastosowanie do wydawania i unieważniania kwalifikowanych elektronicznych poświadczeń atrybutów i elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu oraz wprowadza wymogi dotyczące podpisywania i opatrywania pieczęcią wyników weryfikacji względem źródeł autentycznych.

(3) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 ([4]) oraz – w stosownych przypadkach – dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady ([5]) mają zastosowanie do wszystkich czynności przetwarzania danych osobowych na podstawie niniejszego rozporządzenia.

([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) 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).

([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]) 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) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([6]) skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 17 kwietnia 2026 r. ([7])

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

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Zmiany w rozporządzeniu wykonawczym (UE) 2025/1569

W rozporządzeniu wykonawczym (UE) 2025/1569 wprowadza się następujące zmiany:

1) art. 3 ust. 2 otrzymuje brzmienie:

„2. Dostawcy kwalifikowanych elektronicznych poświadczeń atrybutów i dostawcy elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu, którzy wydają elektroniczne poświadczenia atrybutów objęte schematami zarejestrowanymi w katalogu schematów poświadczania atrybutów, muszą spełniać wymogi odpowiedniego schematu poświadczania atrybutów. Polityki i procedury ustanowione przez wydawców poświadczeń w celu uzyskania zgodności z wymogami schematów poświadczania atrybutów stanowią część oceny zgodności ustanowionej w rozporządzeniu (UE) nr 910/2014.";

2) w art. 4 wprowadza się następujące zmiany:

a) uchyla się ust. 1;

b) ust. 3 otrzymuje brzmienie:

„3. Dostawcy kwalifikowanych elektronicznych poświadczeń atrybutów oraz dostawcy elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu, w każdym przypadku gdy te poświadczenia są wydawane z okresem ważności przekraczającym 24 godziny, unieważniają je przynajmniej w następujących okolicznościach:

a) na wniosek osoby, której wydano elektroniczne poświadczenie atrybutów, lub, w stosownych przypadkach, podmiotu poświadczenia;

b) jeżeli dostawca dowie się o kompromitacji bezpieczeństwa lub wiarygodności kwalifikowanych elektronicznych poświadczeń atrybutów lub elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu;

c) w innych sytuacjach wymaganych przez prawo Unii lub prawo krajowe.";

c) ust. 4 otrzymuje brzmienie:

„4. Dostawcy kwalifikowanych elektronicznych poświadczeń atrybutów i dostawcy elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu ustanawiają techniki unieważniania i metody zarządzania, które zapewniają ochronę prywatności i ograniczają możliwość powiązania lub śledzenia. Techniki unieważniania muszą spełniać wymogi określone w załączniku II.";

([6]) 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).

([7]) EDPS Formal comments on the draft Commission Implementing Regulation as regards applicable standards and specifications for the registration of wallet-relying parties [Formalne uwagi EIOD do projektu rozporządzenia wykonawczego Komisji w odniesieniu do mających zastosowanie norm i specyfikacji dotyczących rejestracji stron ufających portfela] | Europejski Inspektor Ochrony Danych.

3) w art. 9 wprowadza się następujące zmiany:

   a) po ust. 2 dodaje się ust. 2a w brzmieniu:

      „2a. Mechanizm weryfikacji musi być zgodny ze specyfikacjami określonymi w załączniku IV.";

   b) ust. 4 otrzymuje brzmienie:

      „4. W wyniku weryfikacji określa się, czy atrybut został zweryfikowany, oraz wskazuje się podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub, w stosownych przypadkach, podmiot sektora publicznego wyznaczony do działania w imieniu źródła autentycznego, w odniesieniu do którego zweryfikowano atrybut.

      Wynik weryfikacji jest podpisywany lub opatrywany pieczęcią przez organ sektora publicznego odpowiedzialny za źródło autentyczne lub przez wyznaczonego pośrednika uznanego na szczeblu krajowym przy użyciu, odpowiednio, co najmniej zaawansowanego podpisu elektronicznego opartego na kwalifikowanym certyfikacie podpisu elektronicznego lub zaawansowanej pieczęci elektronicznej opartej na kwalifikowanym certyfikacie pieczęci elektronicznej.";

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

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

6) tekst załącznika III do niniejszego rozporządzenia dodaje się jako załącznik IV.

Artykuł 2

Wejście w życie

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

Art. 1 pkt 3 stosuje się od dnia 1 stycznia 2027 r.

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 I

Wykaz norm referencyjnych, o których mowa w art. 3

ETSI TS 119 471 V1.1.1 (2025-05) ma zastosowanie z następującymi dostosowaniami:

1) 2.1. Odniesienia normatywne:

   [1] ETSI EN 319 401 V3.2.1 (2026-01): »Podpisy elektroniczne i infrastruktura zaufania (ESI); Ogólne wymagania polityki dla dostawców usług zaufania«;

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

   [3] FIPS PUB 140-3 (2019) »Wymogi bezpieczeństwa dotyczące modułów kryptograficznych«;

   [4] rozporządzenie wykonawcze Komisji (UE) 2024/482 ([1]);

   [5] rozporządzenie wykonawcze Komisji (UE) 2024/3144 ([2]);

   [6] ISO/IEC 15408:2022 (części 1–5): »Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Kryteria oceny zabezpieczeń informatycznych«.

2) 3.1. Terminy:
   dodaje się termin w brzmieniu:

   — bezpieczne urządzenie kryptograficzne: urządzenie, które przechowuje prywatny klucz użytkownika, chroni ten klucz przed kompromitacją i wykonuje funkcje podpisywania lub odszyfrowywania w imieniu użytkownika.

3) 4. Usługi zaufania w zakresie elektronicznego poświadczania atrybutów (EAA)

   — Pkt 4.2.2.2 »Weryfikacja atrybutów na podstawie źródeł autentycznych« nie ma zastosowania.

   — REQ-EAASP-4.2.2.3-02: Dostawca usług w zakresie elektronicznego poświadczania atrybutów (EAASP) uwierzytelnia instancję EUDIW (europejski portfel tożsamości cyfrowej), wdrażając mechanizmy wzajemnego uwierzytelniania wykorzystujące ważny certyfikat dostępu.

   — REQ-EAASP-4.2.2.3-03: EAASP waliduje jednostkę EUDIW oraz weryfikuje *czy instancja EUDIW została cofnięta*.

   — Pkt *4.3.2. »EUDIW Specific« nie ma zastosowania.*

4) 6.1. Oświadczenie na temat praktyk w zakresie usług elektronicznego poświadczenia atrybutów (EAAS):

   — REQ-EAASP-6.1-02: EAASP dokumentuje mechanizm unieważniania w oświadczeniu na temat praktyk w zakresie EAAS.

5) 6.3. Polityka bezpieczeństwa informacji:

   — REQ-EAASP-6.3-02: EAASP ustanawia procedury powiadamiania organu nadzoru o wszelkich zmianach w świadczeniu usługi zaufania w zakresie elektronicznego poświadczenia atrybutów oraz o zamiarze zaprzestania tej działalności, zgodnie z wymogami biznesowymi oraz odpowiednimi przepisami ustawowymi i wykonawczymi, w tym zgodnie z wymogami aktów wykonawczych przyjętych na podstawie art. 24 ust. 5 rozporządzenia (UE) nr 910/2014. EAASP powiadamia organ nadzoru co najmniej:

      — na miesiąc przed wprowadzeniem jakiejkolwiek zmiany;

      — na trzy miesiące przed planowanym zaprzestaniem świadczenia usług zaufania.

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

([2]) Rozporządzenie wykonawcze Komisji (UE) 2024/3144 z dnia 18 grudnia 2024 r. w sprawie zmiany rozporządzenia wykonawczego (UE) 2024/482 w odniesieniu do mających zastosowanie norm międzynarodowych i w sprawie sprostowania tego rozporządzenia wykonawczego (Dz.U. L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

6) 7.5. Kontrole kryptograficzne

— REQ-EAASP-7.5.2-05: nieważny

— REQ-EAASP-7.5.2-06: nieważny

— REQ-EAASP-7.5.3-01A: W celu zarządzania wszelkimi kluczami kryptograficznymi, algorytmami kryptograficznymi i urządzeniami kryptograficznymi w całym ich cyklu życia wprowadza się odpowiednie środki kontroli bezpieczeństwa, w stosownych przypadkach zgodnie z podejściem opartym na zręczności kryptograficznej.

— REQ-EAASP-7.5.3-01B: W celu świadczenia usług zaufania EAASP wybiera i stosuje odpowiednie techniki kryptograficzne zgodne z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA [2].

— REQ-EAASP-7.5.3-02: EAASP zapewnia, aby bezpieczne urządzenie kryptograficzne, którego używa do podpisu cyfrowego lub pieczęci EAA, było kwalifikowanym urządzeniem do składania podpisu lub pieczęci oraz aby wszystkie inne podpisy cyfrowe lub pieczęcie wykorzystywane do świadczenia odpowiedniej usługi zaufania w zakresie elektronicznego poświadczenia atrybutów lub jej części były tworzone za pomocą bezpiecznego urządzenia kryptograficznego, które jest wiarygodnym systemem certyfikowanym zgodnie z:

  a) wspólnymi kryteriami oceny bezpieczeństwa technologii informacyjnych, określonymi we wspólnych kryteriach oceny bezpieczeństwa technologii informacyjnych, wersja 3.1 (CC3.1) do dnia 31.08.2027 r. lub wersja CC:2022, części 1–5, opublikowanych przez uczestników porozumienia w sprawie uznawania certyfikatów wspólnych kryteriów w dziedzinie bezpieczeństwa informatycznego lub określonymi w normie ISO/IEC 15408 [6] i certyfikowanych zgodnie z EAL na poziomie 4 lub wyższym; lub

  b) europejskim programem certyfikacji cyberbezpieczeństwa opartym na wspólnych kryteriach (EUCC) [4][5] i certyfikowanym zgodnie z EAL na poziomie 4 lub wyższym; lub

  c) FIPS-140-2 poziom 3 stosowanym do dnia 31.08.2027 r. w odniesieniu do istniejących certyfikowanych systemów lub FIPS PUB 140-3 [3] poziom 3 do dnia 31.12.2030 r.

  Certyfikacja ta dotyczy celu lub profilu zabezpieczeń lub projektu modułu i dokumentacji bezpieczeństwa, które spełniają wymogi niniejszego dokumentu, w oparciu o analizę ryzyka i z uwzględnieniem fizycznych i innych nietechnicznych środków bezpieczeństwa.

  Jeżeli bezpieczne urządzenie kryptograficzne korzysta z certyfikacji EUCC [4][5], urządzenie to musi być skonfigurowane i używane zgodnie z tą certyfikacją.

— REQ-EAASP-7.5.5-01: nieważny

— REQ-EAASP-7.5.5-02: nieważny

— REQ-EAASP-7.5.5-04: nieważny

7) 7.9. Zarządzanie podatnością na zagrożenia i incydentami

— REQ-EAASP-7.9-02: Działania monitorujące muszą uwzględniać wrażliwość wszelkich gromadzonych lub analizowanych informacji.

8) 7.12. Zakończenie działalności i plan zakończenia działalności EAASP i EAAS

— REQ-EAASP-7.12-04: Plan zakończenia działalności EAASP musi spełniać wymogi określone w aktach wykonawczych przyjętych na podstawie art. 24 ust. 5 rozporządzenia (UE) nr 910/2014 [i.1].”.

ZAŁĄCZNIK II

„ZAŁĄCZNIK II

Specyfikacje techniczne, o których mowa w art. 3 i 4

Dostawcy kwalifikowanych elektronicznych poświadczeń atrybutów i dostawcy elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu wydają swoje poświadczenia zgodnie z co najmniej jedną z norm wymienionych w załączniku II do rozporządzenia wykonawczego Komisji (UE) 2024/2979 ([1]) oraz stosują odpowiednie techniki unieważniania, również określone w załączniku II do rozporządzenia wykonawczego Komisji (UE) 2024/2979."

([1]) 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).

ZAŁĄCZNIK III

„ZAŁĄCZNIK IV

Wykaz norm i specyfikacji technicznych, o których mowa w art. 9

Mechanizmy weryfikacji, o których mowa w art. 9, muszą być zgodne z jednymi lub obiema następującymi specyfikacjami, z następującymi dostosowaniami:

a) specyfikacje techniczne określone w pkt 6.1.1 normy ETSI TS 119 478 V.1.1.1 (2026-01) – Podpisy elektroniczne i infrastruktura zaufania (ESI); specyfikacja interfejsów związanych ze źródłami autentycznymi;

— REQ-ASIP-6.1.1.2-04-01 [WARUNKOWO]: w przypadku gdy attributeVerificationResult to albo http://uri.etsi.org/19478/VerificationResult/Match, albo http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, attributeVerificationResult może zawierać element attributeValue;

— REQ-ASIP-6.1.1.2-04-02 [WARUNKOWO]: w przypadku gdy odesłany attributeVerificationResult to http://uri.etsi.org/19478/VerificationResult/Match, a attributeVerificationResult zawiera element attributeValue, element attributeValue musi zawierać wartość podaną w żądaniu;

— REQ-ASIP-6.1.1.2-04-03 [WARUNKOWO]: w przypadku gdy odesłany attributeVerificationResult to http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, a attributeVerificationResult zawiera element attributeValue, element attributeValue musi zawierać wartość atrybutu przechowywaną w źródle autentycznym;

— REQ-ASIP-6.1.1.2-06-04-01 [WARUNKOWO]: w przypadku gdy fragmentVerificationResult to albo http://uri.etsi.org/19478/VerificationResult/Match, albo http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, attributeVerificationResult może zawierać element fragmentValue;

— REQ-ASIP-6.1.1.2-06-04-02 [WARUNKOWO]: w przypadku gdy odesłany fragmentVerificationResult to http://uri.etsi.org/19478/VerificationResult/Match, a attributeVerificationResult zawiera element fragmentValue, element fragmentValue musi zawierać wartość podaną w żądaniu;

— REQ-ASIP-6.1.1.2-06-04-03 [WARUNKOWO]: w przypadku gdy odesłany fragmentVerificationResult to http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, a attributeVerificationResult zawiera element fragmentValue, element fragmentValue musi zawierać wartość fragmentu atrybutu przechowywaną w źródle autentycznym;

b) specyfikacje techniczne określone w pkt 6.2.3 normy ETSI TS 119 478 V.1.1.1 (2026-01) – Podpisy elektroniczne i infrastruktura zaufania (ESI); specyfikacja interfejsów związanych ze źródłami autentycznymi.

— REQ-ASIP-6.2.3.2.1-08-04: Element AttributeVerificationResponse może obejmować dokładnie jeden z elementów bezpośrednio podrzędnych spośród TextValue, XMLValue lub AttributeProperties.”