ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2025/1946

z dnia 29 września 2025 r.

ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do kwalifikowanych usług konserwacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych

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. 34 ust. 2 i art. 40,

a także mając na uwadze, co następuje:

(1) Kwalifikowane usługi konserwacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych zapewniają długoterminową integralność, autentyczność, dowód istnienia i dostępność dowodów konserwacji przedmiotowych podpisów elektronicznych i pieczęci elektronicznych. Umożliwia to wykazanie ich ważności prawnej przez długi czas i gwarantuje, że będą one mogły być weryfikowane niezależnie od przyszłych zmian technologicznych. Usługi te są świadczone niezależnie lub w ramach innej kwalifikowanej usługi zaufania, takiej jak kwalifikowane usługi archiwizacji elektronicznej.

(2) Domniemanie zgodności określone w art. 34 ust. 1a i art. 40 rozporządzenia (UE) nr 910/2014 powinno mieć zastosowanie wyłącznie w przypadku, gdy kwalifikowane usługi konserwacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych są zgodne z normami określonymi w niniejszym rozporządzeniu. Przedmiotowe normy powinny odzwierciedlać utrwalone praktyki i być powszechnie uznawane w odpowiednich sektorach. Należy je dostosować w taki sposób, aby obejmowały dodatkowe kontrole zapewniające bezpieczeństwo i wiarygodność kwalifikowanych usług zaufania, a także zdolność do weryfikacji statusu kwalifikowanego i ważności technicznej podpisów elektronicznych i pieczęci elektronicznych.

(3) Jeżeli dostawca usług zaufania spełnia wymogi określone w załączniku do niniejszego rozporządzenia, organy nadzoru powinny domniemywać zgodność z odpowiednimi wymogami rozporządzenia (UE) nr 910/2014 i należycie uwzględniać takie domniemanie w odniesieniu do przyznania lub potwierdzenia statusu kwalifikowanego usługi zaufania. Kwalifikowany dostawca usług zaufania może jednak nadal polegać na innych praktykach w celu wykazania zgodności z wymogami rozporządzenia (UE) nr 910/2014.

(4) Komisja regularnie przeprowadza ocenę nowych technologii, praktyk, norm lub specyfikacji technicznych. Zgodnie z motywem 75 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1183 ([2]) Komisja powinna, w razie potrzeby, poddawać niniejsze rozporządzenie wykonawcze przeglądowi i aktualizacji, aby zachować aktualność względem globalnych zmian, nowych technologii, norm lub specyfikacji technicznych oraz przestrzegać najlepszych praktyk na rynku wewnętrznym.

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

([2]) 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).

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

(6) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([5]) skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 6 czerwca 2025 r.

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

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Normy referencyjne i specyfikacje

Normy referencyjne i specyfikacje, o których mowa w art. 34 ust. 2 i art. 40 rozporządzenia (UE) nr 910/2014, określono w załączniku do niniejszego rozporządzenia.

Artykuł 2

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 29 września 2025 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

([3]) 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).

([4]) 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).

([5]) 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).

ZAŁĄCZNIK

Wykaz norm referencyjnych, o których mowa w art. 2

Normy ETSI TS 119 511 V1.1.1 (2019-06) („ETSI TS 119 511") oraz ETSI TS 119 172-4 V1.1.1 (2021-05) („ETSI TS 119 172-4") stosuje się z zastrzeżeniem następujących dostosowań:

1. W przypadku normy ETSI TS 119 511

   1) 2.1 Odniesienia normatywne:

      — [1] ETSI EN 319 401 V3.1.1 (2024-06) „Podpisy elektroniczne i infrastruktura (ESI); Ogólne wymagania polityki dla dostawców usług zaufania",

      — [2] ETSI TS 119 612 (V2.3.1) „Podpisy i infrastruktura (ESI); Zaufane listy",

      — [5] FIPS PUB 140-3 (2019) „Wymagania bezpieczeństwa dotyczące modułów kryptograficznych",

      — [6] Rozporządzenie wykonawcze Komisji (UE) 2024/482 ([1]) ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 w odniesieniu do przyjęcia europejskiego programu certyfikacji cyberbezpieczeństwa opartego na wspólnych kryteriach (EUCC),

      — [7] Rozporządzenie wykonawcze Komisji (UE) 2024/3144 ([2]) w sprawie zmiany rozporządzenia wykonawczego (UE) 2024/482 w odniesieniu do mających zastosowanie norm międzynarodowych i w sprawie sprostowania tego rozporządzenia wykonawczego,

      — [8] Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa, podgrupa ds. kryptografii: „Uzgodnione mechanizmy kryptograficzne" opublikowane przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa („ENISA") ([3]),

      — [9] ETSI TS 119 172-4 V1.1.1 (2021-05) „Podpisy elektroniczne i infrastruktura (ESI); Zasady składania podpisów; Część 4: Zasady stosowania podpisu (polityka walidacji) w odniesieniu do europejskich kwalifikowanych podpisów elektronicznych/pieczęci z wykorzystaniem zaufanych list,

      — [10] ISO/IEC 15408:2022 (części 1–5) „Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Kryteria oceny zabezpieczeń informatycznych"

   2) 3.1 Terminy

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

   3) 6.4 Profile konserwacji

      — OVR-6.4-08A [WTS][WOS] Oczekiwany czas trwania dowodów musi być zgodny z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA[8],

      — UWAGA 3 nieważna.

   4) 6.5 Polityka dowodów konserwacji

      — OVR-6.5-04A Stosowane algorytmy kryptograficzne muszą być zgodne z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA[8],

      — UWAGA 1 nieważna.

([1]) Dz.U. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([2]) Dz.U. L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.
([3]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

5) 7.2 Zasoby ludzkie

— OVR-7.2-02 Personel dostawcy usług konserwacji (PSP) pełniący zaufane funkcje oraz, w stosownych przypadkach, jego podwykonawcy pełniący zaufane funkcje muszą być w stanie spełnić wymóg „posiadania wiedzy eksperckiej, doświadczenia i kwalifikacji" zdobytych w ramach formalnego szkolenia i dokumentów uwierzytelniających lub doświadczenia, lub obu tych elementów,

— OVR-7.2-03 Zgodność z OVR-7.2-02 obejmuje regularne aktualizacje (co najmniej raz na 12 miesięcy) dotyczące nowych zagrożeń i obecnych praktyk w zakresie bezpieczeństwa.

6) 7.5 Kontrole kryptograficzne

— OVR-7.5-05 [WARUNKOWO] Jeżeli PSP podpisze (część) dowodu konserwacji, klucz prywatnego podpisu dostawcy usług konserwacji przechowuje się i wykorzystuje w bezpiecznym urządzeniu kryptograficznym, które jest wiarygodnym systemem certyfikowanym zgodnie ze:

a) wspólnymi kryteriami oceny bezpieczeństwa technologii informacyjnych, określonymi w normie ISO/IEC 15408 [10] lub we wspólnych kryteriach oceny bezpieczeństwa technologii informacyjnych, wersja CC:2022, części 1–5, opublikowanych przez uczestników porozumienia w sprawie uznawania certyfikatów wspólnych kryteriów w dziedzinie bezpieczeństwa informatycznego i certyfikowanych zgodnie z EAL na poziomie 4 lub wyższym; lub

b) EUCC [6][7] i certyfikowany zgodnie z EAL na poziomie 4 lub wyższym; lub

c) do dnia 31.12.2030 r. FIPS PUB 140-3 [5] poziom 3,

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 [6][7], urządzenie to musi być skonfigurowane i używane zgodnie z tą certyfikacją,

— OVR-7.5-06 [WARUNKOWO] nieważny,

— OVR-7.5-07 [WARUNKOWO] Jeżeli PSP podpisze (część) dowodu konserwacji, wszelkie kopie zapasowe kluczy podpisu prywatnego PSP są chronione przed przechowywaniem na zewnątrz tego urządzenia w celu zapewnienia integralności i poufności podpisu za pomocą bezpiecznego urządzenia kryptograficznego,

— OVR-7.5-08 Prywatny klucz podpisu PSP jest eksportowany i importowany do innego bezpiecznego urządzenia kryptograficznego tylko wtedy, gdy ten eksport i import są realizowane w sposób bezpieczny i zgodnie z certyfikacją tych urządzeń.

7) 7.8 Bezpieczeństwo sieci

— OVR-7.8-03 Wymagany w pkt REQ-7.8-13 normy ETSI EN 319 401 [1] skan podatności przeprowadza się co najmniej raz na kwartał,

— OVR-7.8-04 Wymagany w pkt REQ-7.8-17X ETSI normy EN 319 401 [1] test penetracyjny przeprowadza się co najmniej raz w roku,

— OVR-7.8-05 Zapory sieciowe należy skonfigurować tak, aby uniemożliwić wszelkie protokoły i dostępy, które nie są wymagane do funkcjonowania PSP.

8) 7.14 Monitorowanie kryptograficzne

— OVR-7.14-03A Ocena algorytmów kryptograficznych w OVR-7.14.01 i OVR-7.14.02 musi być zgodna z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA [8],

— UWAGA nieważna.

9) 7.12 Zakończenie działalności dostawcy usług zaufania i plany zakończenia działalności

— OVR-7.12-01A Plan zakończenia działalności dostawcy usług zaufania musi spełniać wymogi określone w aktach wykonawczych przyjętych na podstawie art. 24 ust. 5 rozporządzenia (UE) nr 910/2014 [i.2].

10) 7.17 Łańcuch dostaw

— OVR-7.17-01 Stosuje się wymagania określone w normie ETSI EN 319 401 [1], pkt 7.14.

11) Załącznik A (normatywny): kwalifikowana usługa konserwacji kwalifikowanych podpisów elektronicznych zgodnie z definicją zawartą w art. 34 rozporządzenia (UE) nr 910/2014

— OVR-A-02 [PDS][PDS+PGD]

a) usługa konserwacji zachowuje wszystkie informacje niezbędne do sprawdzenia statusu kwalifikowanego podpisu elektronicznego lub pieczęci elektronicznej, które nie byłyby publicznie dostępne do końca okresu konserwacji;

b) usługa konserwacji zapewnia, aby w dowolnym momencie okresu konserwacji zachowane informacje były takie, że po ich przekazaniu jako dane wejściowe do procesu określonego w pkt 4.4 ETSI TS 119 172-4 [9] wyniki tego procesu jasno określały, czy podpis cyfrowy lub pieczęć cyfrowa były, w momencie ich konserwacji, technicznie odpowiednie do wdrożenia kwalifikowanego podpisu elektronicznego UE lub kwalifikowanej pieczęci elektronicznej UE,

— OVR-A-03 [PDS][PDS+PGD] Znaczniki czasu wykorzystywane w ramach dowodów konserwacji są kwalifikowanymi znacznikami czasu zgodnie z rozporządzeniem (UE) nr 910/2014 [i.2].

2. W przypadku ETSI TS 119 172-4

1) 2.1 Odniesienia normatywne:

— [1] ETSI EN 319 102-1 V1.4.1 (2024-06) „Podpisy elektroniczne i infrastruktura zaufania (ESI); Procedury tworzenia i zatwierdzania podpisów cyfrowych AdES; Część 1: Tworzenie i walidacja”,

— Wszystkie odniesienia do normy „ETSI TS 119 102-1 [1]” należy rozumieć jako odniesienia do normy „ETSI EN 319 102-1 [1]”,

— [2] ETSI TS 119 612 (V2.3.1) „Podpisy i infrastruktura (ESI); Zaufane listy”,

— [13] ETSI TS 119 101 V1.1.1 (2016-03) „Podpisy elektroniczne i infrastruktura (ESI); Wymogi polityki i bezpieczeństwa dla wniosków o tworzenie i zatwierdzanie podpisów”.

2) 4.2 Ograniczenia walidacji i procedury walidacji, wymóg REQ-4.2-03, sekcja „Ograniczenia walidacji X.509”, lit. c):

— (i) Jeżeli certyfikat pozycji końcowej stanowi kotwicę zaufania, nie stosuje się RevocationCheckingConstraints,

— (ii) Jeżeli certyfikat podmiotu końcowego nie stanowi kotwicy zaufania, RevocationCheckingConstraints ustawia się na „eitherCheck”, jak zdefiniowano w normie ETSI TS 119 172-1 [3], pkt A.4.2.1, tabela A.2 wiersze m)2.1,

— (iii) Jeżeli certyfikat podmiotu końcowego stanowi kotwicę zaufania, nie stosuje się ograniczeń RevocationFreshnessConstraints określonych w normie ETSI TS 119 172-1 [3], pkt A.4.2.1, tabela A.2 wiersze m)2.2,

— (iv) Jeżeli certyfikat podmiotu końcowego nie stanowi kotwicy zaufania, stosuje się ograniczenia RevocationFreshnessConstraints określone w normie ETSI TS 119 172-1 [3], pkt A.4.2.1, tabela A.2 wiersze m)2.2, o maksymalnej wartości 0 dla certyfikatu podpisu, zapewniając, że informacje o unieważnieniu są akceptowane tylko wtedy, gdy zostały wydane po upływie najkrótszego czasu składania podpisu. W przypadku certyfikatów innych niż certyfikat podpisu, w tym certyfikatów potwierdzających znaczniki czasu, nie ustala się żadnej wartości dla RevocationFreshnessConstraints.

3) 4.3 Wymogi dotyczące walidacji podpisów i zasad stosowania w zakresie kontroli praktyk

— REQ-4.3-02 Wnioski o walidację podpisu muszą być zgodne z normą ETSI TS 119 101 [13].

4) 4.4 Proces sprawdzania przydatności technicznej (przepisów)

— REQ-4.4.2-03 Jeżeli którakolwiek z kontroli określonych w REQ-4.4.2-01 nie powiedzie się, wówczas:

— zaprzestaje się procesu,

— podpis jest określany technicznie jako nieokreślony, tj. ani jako kwalifikowany podpis elektroniczny UE, ani jako kwalifikowana pieczęć elektroniczna UE,

— powyższy wynik i wyniki procesów wszystkich procesów pośrednich muszą być odzwierciedlone w zasadach stosowania podpisu w sprawozdaniu sprawdzającym.