Dziennik Urzędowy
Unii Europejskiej

PL
Seria L

2025/1943

30.9.2025

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2025/1943

z dnia 29 września 2025 r.

ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do norm referencyjnych dotyczących kwalifikowanych certyfikatów podpisów elektronicznych i kwalifikowanych certyfikatów 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. 28 ust. 6 i art. 38 ust. 6,

a także mając na uwadze, co następuje:

(1) Kwalifikowane certyfikaty podpisów elektronicznych i kwalifikowane certyfikaty pieczęci elektronicznych odgrywają kluczową rolę w cyfrowym otoczeniu biznesu, poprzez wspieranie przejścia od tradycyjnych procesów opartych na dokumentacji papierowej do ich elektronicznych odpowiedników. Poprzez powiązanie danych służących do walidacji podpisu elektronicznego lub danych służących walidacji pieczęci elektronicznej odpowiednio z osobą fizyczną lub prawną oraz poprzez potwierdzenie imienia i nazwiska tej osoby kwalifikowane certyfikaty zwiększają pewność co do tożsamości podpisującego i podmiotu składającego pieczęć.

(2) Domniemanie zgodności określone w art. 28 ust. 6 i art. 38 ust. 6 rozporządzenia (UE) nr 910/2014 powinno mieć zastosowanie wyłącznie w przypadku, gdy kwalifikowane usługi zaufania w zakresie wydawania kwalifikowanych certyfikatów podpisów elektronicznych i kwalifikowanych usług zaufania w odniesieniu do wydawania kwalifikowanych certyfikatów 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 oraz treści kwalifikowanych certyfikatów.

(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.

(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.

([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).

([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).

(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) 910/2014,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Normy referencyjne i specyfikacje dotyczące kwalifikowanych certyfikatów podpisów elektronicznych i pieczęci elektronicznych

1. Normy referencyjne i specyfikacje, o których mowa w art. 28 ust. 6 rozporządzenia (UE) nr 910/2014, określono w załączniku I do niniejszego rozporządzenia.

2. Normy referencyjne i specyfikacje, o których mowa w art. 38 ust. 6 rozporządzenia (UE) nr 910/2014, określono w załączniku II 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

([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 I

Wykaz norm referencyjnych i specyfikacji dla kwalifikowanych certyfikatów podpisów elektronicznych

Normy ETSI EN 319 411-2 V2.6.1 („ETSI EN 319 411-2"), ETSI EN 319 412-1 V1.6.1 („ETSI EN 319 412-1"), ETSI EN 319 412-2 V2.4.1 („ETSI EN 319 412-2") oraz ETSI EN 319 412-5 V2.5.1 („ETSI EN 319 412-5") stosuje się z zastrzeżeniem następujących dostosowań:

1. W przypadku normy ETSI EN 319 411-2

   1) 2.1 Odniesienia normatywne

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

      — [2] ETSI EN 319 411-1 V1.5.1 (2025-04) „Podpisy elektroniczne i infrastruktura zaufania (ESI); Wymagania polityki i bezpieczeństwa dla dostawców usług zaufania wydających certyfikaty; Część 1: Wymagania ogólne", z następującymi dostosowaniami:

        W pkt 2.1 Odniesienia normatywne normy ETSI EN 319 411-1 V1.5.1 wprowadza się następujące zmiany:

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

        — [10] ETSI EN 319 412-2 V2.4.1 „Podpisy elektroniczne i infrastruktura (ESI); Profile certyfikatu; Część 2: Profil certyfikatu dla certyfikatów wydawanych osobom fizycznym",

        — [14] ETSI EN 319 412-1 V1.6.1 „Podpisy elektroniczne i infrastruktura (ESI); Profile certyfikatu; Część 1: Opis ogólny oraz ogólne struktury danych",

      — [3] ETSI EN 319 412-5 V2.5.1 „Podpisy elektroniczne i infrastruktura zaufania (ESI); Profile certyfikatu; Część 5: Deklaracja dla certyfikatów kwalifikowanych",

      — [5] ETSI EN 319 412-1 V1.6.1 „Podpisy elektroniczne i infrastruktura zaufania (ESI); Profile certyfikatu; Część 1: Opis ogólny oraz ogólne struktury danych",

      — [6] CEN/TS 419261:2015 „Wymogi bezpieczeństwa dotyczące wiarygodnych systemów zarządzania certyfikatami i znacznikami czasu",

      — [7] Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa, podgrupa ds. kryptografii: „Uzgodnione mechanizmy kryptograficzne" opublikowane przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa („ENISA") ([1]),

      — [8] Rozporządzenie wykonawcze Komisji (UE) 2024/482 ([2]) ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 w odniesieniu do przyjęcia europejskiego programu certyfikacji cyberbezpieczeństwa opartego na wspólnych kryteriach (EUCC),

      — [9] Rozporządzenie wykonawcze Komisji (UE) 2024/3144 ([3]) w sprawie zmiany rozporządzenia wykonawczego (UE) 2024/482 w odniesieniu do mających zastosowanie norm międzynarodowych i w sprawie sprostowania tego rozporządzenia wykonawczego,

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

      — [11] FIPS PUB 140-3 (2019) „Wymogi bezpieczeństwa dotyczące modułów kryptograficznych"

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

2) 5.2 Wymogi w zakresie oświadczeń na temat praktyk dotyczących certyfikacji

— OVR-5.2-02 W politykach certyfikacji wskazanych w dokumentacji dostawcy usług zaufania należy określać wymagania dotyczące profili certyfikatów, które mają być stosowane.

3) 5.3 Nazwa i identyfikacja polityki certyfikacji

— OVR-5.3-01 W przypadku wprowadzenia jakichkolwiek zmian w polityce certyfikacji, jak opisano w pkt 4.2.2, które mają wpływ na stosowanie, należy zmienić identyfikator polityki.

4) 6.1 Obowiązki związane z publikacją i repozytorium

— OVR-6.1-02 Informacje określone w DIS-6.1-04 w normie ETSI EN 319 411-1 [2] są dostępne publicznie i na szczeblu międzynarodowym.

5) 6.2.2 Wstępna walidacja tożsamości

— REG-6.2.2-01A Gromadzenie atrybutów i dowodów dotyczących tożsamości podmiotu oraz ich walidację określa się zgodnie z aktami wykonawczymi przyjętymi na podstawie art. 24 ust. 1c rozporządzenia (UE) nr 910/2014 [i.1],

— REG-6.2.2-02 [QCP-n] i [QCP-n-qscd] Tożsamość osoby fizycznej oraz, w stosownych przypadkach, wszelkie szczególne atrybuty tej osoby weryfikuje się zgodnie z aktami wykonawczymi przyjętymi na podstawie art. 24 ust. 1c rozporządzenia (UE) nr 910/2014 [i.1],

— UWAGA 1 nieważna.

6) 6.3.3 Wydanie certyfikatu

— GEN-6.3.3-01 Zastosowanie mają wymagania od GEN-6.3.3-01 do GEN-6.3.3-10 określone w normie ETSI EN 319 411-1 [2], pkt 6.3.3,

— GEN-6.3.3-02 [WARUNKOWO] Jeżeli certyfikat jest wydawany osobie fizycznej zidentyfikowanej w powiązaniu z osobą prawną, atrybuty podmiotu identyfikujące organizację w certyfikacie określają osobę prawną lub podjednostkę tej osoby prawnej, a identyfikator podmiotu w certyfikacie jest osobą fizyczną,

— GEN-6.3.3-03 Identyfikatorem polityki certyfikacji jest [WYBÓR]:

a) [QCP-n]

— jak określono w pkt 5.3 lit. a), lub

— identyfikator obiektu, przydzielony przez dostawcę usług zaufania, inną odpowiednią zainteresowaną stronę lub w ramach dalszej standaryzacji na potrzeby polityki certyfikacji zwiększającej odpowiednie mające zastosowanie wymogi polityki określone w niniejszym dokumencie,

b) [QCP-n-qscd]

— jak określono w pkt 5.3 lit. c), lub

— identyfikator obiektu, przydzielony przez dostawcę usług zaufania, inną odpowiednią zainteresowaną stronę lub w ramach dalszej standaryzacji na potrzeby polityki certyfikacji zwiększającej odpowiednie mające zastosowanie wymogi polityki określone w niniejszym dokumencie.

7) 6.3.5 Para kluczy i wykorzystanie certyfikatu

— SDP-6.3.5-02A [WARUNKOWO] Jeżeli dostawca usług zaufania zarządza kwalifikowanym urządzeniem do składania podpisu (QSCD) w odniesieniu do podmiotu, jest on kwalifikowanym dostawcą usług zaufania świadczącym kwalifikowaną usługę zaufania w zakresie zarządzania kwalifikowanym urządzeniem do składania podpisu elektronicznego na odległość, zgodnie z rozporządzeniem (UE) nr 910/2014 [i.1]

— SDP-6.3.5-11A Jeżeli abonent lub podmiot generuje klucze podmiotu, obowiązki abonenta (zob. pkt 6.3.4) obejmują:

a) obowiązek generowania kluczy podmiotu z wykorzystaniem algorytmu zgodnego z Uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa [7] i opublikowanymi przez ENISA na potrzeby wykorzystania certyfikowanego klucza określonego w polityce certyfikacji;

b) obowiązek stosowania długości klucza i algorytmu zgodnych z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa [7] i opublikowanymi przez ENISA do zastosowań certyfikowanego klucza określonego w polityce certyfikacji w okresie ważności certyfikatu.

8) 6.3.10 Usługi w zakresie statusu certyfikatów

— CSS-6.3.10-08 [WARUNKOWO] Jeżeli zapewnione są listy unieważnionych certyfikatów, dostawca usług zaufania zachowuje integralność i dostępność ostatniej takiej listy co najmniej przez okres określony w oświadczeniu na temat praktyk dotyczących certyfikacji zgodnie z CSS-6.3.10-12.

9) 6.4.4 Kontrole personelu

— OVR-6.4.4-02 Personel dostawcy usług zaufania 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-6.4.4-03 Zgodność z OVR-6.4.4-02 obejmuje regularne (co najmniej raz na 12 miesięcy) aktualizacje dotyczące nowych zagrożeń i obecnych praktyk w zakresie bezpieczeństwa,

— OVR-6.4.4-04 Oprócz zaufanych funkcji określonych w normie ETSI EN 319 401 [1], (klauzula 7.2-15), wspiera się zaufane role urzędników odpowiedzialnych za rejestrację i unieważnienie rejestracji, których obowiązki określono w TS 419261 [6]. W przypadkach gdy kwalifikowany dostawca usług zaufania jest zarządzany bezpośrednio przez państwo członkowskie lub organ sektora publicznego lub działa w ich imieniu, te dodatkowe zaufane funkcje mogą być pełnione przez co najmniej jednego formalnego przedstawiciela działającego na rzecz i w imieniu urzędników ds. rejestracji i unieważniania działających w administracji lokalnej lub regionalnej.

10) 6.4.9 Zakończenie działalności urzędów certyfikacji lub urzędów rejestracji

— OVR-6.4.9-02 Plan zakończenia działalności musi spełniać wymogi określone w aktach wykonawczych przyjętych na podstawie art. 24 ust. 5 rozporządzenia (UE) nr 910/2014 [i.1].

11) 6.5.1 Generowanie i instalacja pary kluczy

— OVR-6.5.1-01A Generowanie par kluczy urzędu certyfikacji odbywa się przy użyciu algorytmu zgodnego z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA [7] do celów podpisywania przez urząd certyfikacji,

— OVR-6.5.1-01B Wybrana długość klucza i algorytm dla klucza podpisu urzędu certyfikacji muszą być zgodne z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA[7] do celów podpisania przez urząd certyfikacji,

— OVR-6.5.1-01C [WARUNKOWO] Jeżeli urząd certyfikacji generuje klucze podmiotu, klucze podmiotu wygenerowane przez urząd certyfikacji muszą być zgodne z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA[7] do celów określonych w polityce certyfikacji w okresie ważności certyfikatu.

12) 6.5.2 Zabezpieczenie klucza prywatnego i kontrole techniczne modułu kryptograficznego

— GEN-6.5.2-01 Zastosowanie mają wszystkie wymagania określone w normie ETSI EN 319 411-1 [2], pkt 6.5.2, z wyjątkiem wymogów OVR-6.5.2-01, OVR-6.5.2-03 i OVR-6.5.2-04,

— GEN-6.5.2-02 Generowanie par kluczy dostawcy usług zaufania, w tym kluczy używanych w usługach unieważniania i rejestracji, odbywa się za pomocą bezpiecznego urządzenia kryptograficznego, które jest wiarygodnym systemem certyfikowanym zgodnie z:

— wspólnymi kryteriami oceny bezpieczeństwa technologii informacyjnych, określonymi w normie ISO/IEC 15408 [10] lub we wspólnych kryteriach oceny bezpieczeństwa technologii informacyjnych, wersja CC:2002, 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

— europejskim programem certyfikacji cyberbezpieczeństwa opartym na wspólnych kryteriach (EUCC) [8][9] i certyfikowany zgodnie z EAL na poziomie 4 lub wyższym; lub

— do dnia 31.12.2030 r. FIPS PUB 140–3 [11] 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 [8][9], urządzenie to musi być skonfigurowane i używane zgodnie z tą certyfikacją.

— GEN-6.5.2-03 Prywatny klucz podpisu urzędu certyfikacji jest przechowywany i używany w bezpiecznym urządzeniu kryptograficznym spełniającym wymogi określone w pkt GEN-6.5.2-01 i GEN-6.5.2-02.

13) 6.5.7 Kontrole zabezpieczeń sieci

— OVR-6.5.7-02 Wymagany w pkt REQ-7.8-13 normy ETSI EN 319 401 [1] skan podatności przeprowadza się co najmniej raz na kwartał,

— OVR-6.5.7-03 Wymagany w pkt REQ-7.8-17X normy ETSI EN 319 401 [1] test penetracyjny przeprowadza się co najmniej raz w roku,

— OVR-6.5.7-04 Zapory sieciowe należy skonfigurować tak, aby uniemożliwić wszelkie protokoły i dostępy, które nie są wymagane do funkcjonowania dostawcy usług zaufania.

14) 6.6.1 Profil certyfikatu

— GEN-6.6.1-05 Certyfikat musi zawierać jeden z identyfikatorów polityki określonych w GEN-6.3.3-03 [WYBÓR]. Certyfikat może zawierać inne identyfikatory obiektu przydzielone przez dostawcę usług zaufania.

2. W przypadku normy ETSI EN 319 412-2:

1) 2.1 Odniesienia normatywne

— [2] ETSI EN 319 412-5 V2.5.1 „Podpisy elektroniczne i infrastruktura zaufania (ESI); Profile certyfikatu; Część 5: Deklaracje dla certyfikatów kwalifikowanych”,

— [9] Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa, podgrupa ds. kryptografii, „Uzgodnione mechanizmy kryptograficzne” opublikowane przez ENISA.

2) 4.2.2 Podpis

— GEN-4.2.2-2 Algorytm podpisu należy wybierać zgodnie z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA [9],

— UWAGA nieważna.

3) 4.2.3.1 Wydawcy będący osobami prawnymi

— GEN-4.2.3.1-3 Jeżeli wiadomo, że istnieje odpowiedni numer rejestracyjny, to dane identyfikujące wydawcę muszą zawierać organizationIdentifier z wartością tego numeru rejestracyjnego, zgodnie z odpowiednim oficjalnym rejestrem, w którym ten numer został nadany.

4) 4.2.5 Dane dotyczące klucza publicznego podmiotu

— GEN-4.2.5-2 Klucz publiczny podmiotu należy wybierać zgodnie z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA [9],

— UWAGA nieważna.

5) 4.2.6 Numer seryjny

— GEN-4.2.6-01 Atrybut serialNumber certyfikatu (jak określono w IETF RFC 5280 [1], pkt 4.1.2.2) musi być niepowtarzalny dla każdego certyfikatu wydanego przez dostawcę usług zaufania.

ZAŁĄCZNIK II

Wykaz norm referencyjnych i specyfikacji dla kwalifikowanych certyfikatów pieczęci elektronicznych

Normy ETSI EN 319 411-2 V2.6.1 („ETSI EN 319 411-2"), ETSI EN 319 412-1 V1.6.1 („ETSI EN 319 412-1"), ETSI EN 319 412-3 V1.3.1 („ETSI EN 319 412-3"), ETSI EN 319 412-2 V2.4.1 („ETSI EN 319 412-2") oraz ETSI EN 319 412-5 V2.5.1 („ETSI EN 319 412-5") stosuje się z zastrzeżeniem następujących dostosowań:

1. W przypadku normy ETSI EN 319 411-2

   1) 2.1 Odniesienia normatywne

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

      — [2] ETSI EN 319 411-1 V1.5.1 (2025-04) „Podpisy elektroniczne i infrastruktura zaufania (ESI); Wymagania polityki i bezpieczeństwa dla dostawców usług zaufania wydających certyfikaty; Część 1: Wymagania ogólne", z następującymi dostosowaniami:

        W pkt 2.1 Odniesienia normatywne normy ETSI EN 319 411-1 V1.5.1 wprowadza się następujące zmiany:

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

        — [10] ETSI EN 319 412-2 V2.4.1 „Podpisy elektroniczne i infrastruktura (ESI); Profile certyfikatu; Część 2: Profil certyfikatu dla certyfikatów wydawanych osobom fizycznym",

        — [14] ETSI EN 319 412-1 V1.6.1 „Podpisy elektroniczne i infrastruktura (ESI); Profile certyfikatu; Część 1: Opis ogólny oraz ogólne struktury danych",

      — [3] ETSI EN 319 412-5 V2.5.1 „Podpisy elektroniczne i infrastruktura zaufania (ESI); Profile certyfikatu; Część 5: Deklaracje dla certyfikatów kwalifikowanych",

      — [5] ETSI EN 319 412-1 V1.6.1 „Podpisy elektroniczne i infrastruktura zaufania (ESI); Profile certyfikatu; Część 1: Opis ogólny oraz ogólne struktury danych",

      — [6] CEN/TS 419261:2015 „Wymogi bezpieczeństwa dotyczące wiarygodnych systemów zarządzania certyfikatami i znacznikami czasu" (opracowana przez CEN),

      — [7] Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa, podgrupa ds. kryptografii: „Uzgodnione mechanizmy kryptograficzne" opublikowane przez ENISA,

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

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

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

      — [11] FIPS PUB 140-3 (2019) „Wymogi bezpieczeństwa dotyczące modułów kryptograficznych"

   2) 5.2 Wymogi w zakresie oświadczeń na temat praktyk dotyczących certyfikacji

      — OVR-5.2-02 W politykach certyfikacji wskazanych w dokumentacji dostawcy usług zaufania należy określać wymagania dotyczące profili certyfikatów, które mają być stosowane.

3) 5.3 Nazwa i identyfikacja polityki certyfikacji

— OVR-5.3-01 W przypadku wprowadzenia jakichkolwiek zmian w polityce certyfikacji, jak opisano w pkt 4.2.2, które mają wpływ na stosowanie, należy zmienić identyfikator polityki.

4) 6.1 Obowiązki związane z publikacją i repozytorium

— OVR-6.1-02 Informacje określone w pkt DIS-6.1-04 normy ETSI EN 319 411-1 [2] muszą być dostępne publicznie i na szczeblu międzynarodowym.

5) 6.2.2 Wstępna walidacja tożsamości

— REG-6.2.2-01A Gromadzenie atrybutów i dowodów dotyczących tożsamości podmiotu oraz ich walidację określa się zgodnie z aktami wykonawczymi przyjętymi na podstawie art. 24 ust. 1c rozporządzenia (UE) nr 910/2014 [i.1],

— REG-6.2.2-03 [QCP-l] i [QCP-l-qscd] Tożsamość osoby prawnej oraz, w stosownych przypadkach, wszelkie szczególne atrybuty tej osoby weryfikuje się zgodnie z aktami wykonawczymi przyjętymi na podstawie art. 24 ust. 1c rozporządzenia (UE) nr 910/2014 [i.1],

— UWAGA 3 zob. przypis 2.

6) 6.3.3 Wydanie certyfikatu

— GEN-6.3.3-01 Zastosowanie mają wymagania od GEN-6.3.3-01 do GEN-6.3.3-10 określone w normie ETSI EN 319 411-1 [2], pkt 6.3.3,

— GEN-6.3.3-02 Identyfikatorem polityki certyfikacji jest [WYBÓR]:

a) [QCP-l]

— jak określono w pkt 5.3 lit. b), lub

— identyfikator obiektu, przydzielony przez dostawcę usług zaufania, inną odpowiednią zainteresowaną stronę lub w ramach dalszej standaryzacji na potrzeby polityki certyfikacji zwiększającej odpowiednie mające zastosowanie wymogi polityki określone w niniejszym dokumencie,

b) [QCP-l-qscd]

— jak określono w pkt 5.3 lit. d), lub

— identyfikator obiektu, przydzielony przez dostawcę usług zaufania, inną odpowiednią zainteresowaną stronę lub w ramach dalszej standaryzacji na potrzeby polityki certyfikacji zwiększającej mające zastosowanie wymogi polityki określone w niniejszym dokumencie.

7) 6.3.5 Para kluczy i wykorzystanie certyfikatu

— SDP-6.3.5-02A [WARUNKOWO] Jeżeli dostawca usług zaufania zarządza kwalifikowanym urządzeniem do składania podpisu (QSCD) w odniesieniu do podmiotu, jest on kwalifikowanym dostawcą usług zaufania świadczącym kwalifikowaną usługę zaufania w zakresie zarządzania kwalifikowanym urządzeniem do składania pieczęci elektronicznej na odległość, zgodnie z rozporządzeniem (UE) nr 910/2014 [i.1]

— SDP-6.3.5-11A Jeżeli abonent lub podmiot generuje klucze podmiotu, obowiązki abonenta (zob. pkt 6.3.4) obejmują:

a) obowiązek generowania kluczy podmiotu z wykorzystaniem algorytmu zgodnego z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA[7] na potrzeby wykorzystania certyfikowanego klucza określonego w polityce certyfikacji; oraz

b) obowiązek stosowania długości klucza i algorytmu zgodnych z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA[7] do zastosowań certyfikowanego klucza określonego w polityce certyfikacji w okresie ważności certyfikatu.

8) 6.3.10 Usługi w zakresie statusu certyfikatów

— CSS-6.3.10-08 [WARUNKOWO] Jeżeli zapewnione są listy unieważnionych certyfikatów, dostawca usług zaufania zachowuje integralność i dostępność ostatniej takiej listy co najmniej przez okres określony w oświadczeniu na temat praktyk dotyczących certyfikacji zgodnie z CSS-6.3.10-12.

9) 6.4.4 Kontrole personelu

— OVR-6.4.4-02 Personel dostawcy usług zaufania 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-6.4.4-03 Zgodność z OVR-6.4.4-02 obejmuje regularne (co najmniej raz na 12 miesięcy) aktualizacje dotyczące nowych zagrożeń i obecnych praktyk w zakresie bezpieczeństwa,

— OVR-6.4.4-04 Oprócz zaufanych funkcji określonych w normie ETSI EN 319 401 [1], (pkt 7.2-15), wspiera się zaufane funkcje urzędników odpowiedzialnych za rejestrację i unieważnienie rejestracji, których obowiązki określono w TS 419261 [6]. W przypadkach gdy kwalifikowany dostawca usługi zaufania jest zarządzany bezpośrednio przez państwo członkowskie lub organ sektora publicznego lub działa w ich imieniu, te dodatkowe zaufane funkcje mogą być pełnione przez co najmniej jednego formalnego przedstawiciela działającego na rzecz i w imieniu urzędników ds. rejestracji i unieważniania działających w administracji lokalnej lub regionalnej.

10) 6.4.9 Zakończenie działalności urzędów certyfikacji lub urzędów rejestracji

— OVR-6.4.9-02 Plan zakończenia działalności musi spełniać wymogi określone w aktach wykonawczych przyjętych na podstawie art. 24 ust. 5 rozporządzenia (UE) nr 910/2014 [i.1].

11) 6.5.1 Generowanie i instalacja par kluczy

— OVR-6.5.1-01A Generowanie par kluczy urzędu certyfikacji odbywa się przy użyciu algorytmu zgodnego z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA [7] do celów podpisywania przez urząd certyfikacji,

— OVR-6.5.1-01B Wybrana długość klucza i algorytm dla klucza podpisu urzędu certyfikacji muszą być zgodne z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA[7] do celów podpisania przez urząd certyfikacji,

— OVR-6.5.1-01C [WARUNKOWO] Jeżeli urząd certyfikacji generuje klucze podmiotu, klucze podmiotu wygenerowane przez urząd certyfikacji muszą być zgodne z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA[7] do celów określonych w polityce certyfikacji w okresie ważności certyfikatu.

12) 6.5.2 Zabezpieczenie klucza prywatnego i kontrola techniczna modułu kryptograficznego

— GEN-6.5.2-01 Zastosowanie mają wszystkie wymagania określone w normie ETSI EN 319 411-1 [2], pkt 6.5.2, z wyjątkiem wymagań OVR-6.5.2-01, OVR-6.5.2-03 i OVR-6.5.2-04,

— GEN-6.5.2-02 Generowanie par kluczy dostawcy usług zaufania, w tym kluczy używanych w usługach unieważniania i rejestracji, odbywa się za pomocą bezpiecznego urządzenia kryptograficznego, które jest wiarygodnym systemem certyfikowanym zgodnie z:

  — wspólnymi kryteriami oceny bezpieczeństwa technologii informacyjnych, określonymi w normie ISO/IEC 15408 [10] lub we wspólnych kryteriach oceny bezpieczeństwa technologii informacyjnych, wersja CC:2002, 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

  — europejskim programem certyfikacji cyberbezpieczeństwa opartym na wspólnych kryteriach (EUCC) [8][9] i certyfikowany zgodnie z EAL na poziomie 4 lub wyższym; lub

  — do dnia 31.12.2030 r. FIPS PUB 140–3 [11] 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 [8][9], urządzenie to musi być skonfigurowane i używane zgodnie z tą certyfikacją,

— GEN-6.5.2-03 Prywatny klucz podpisu urzędu certyfikacji jest przechowywany i używany w bezpiecznym urządzeniu kryptograficznym spełniającym wymogi pkt GEN-6.5.2-01 i GEN-6.5.2-02.

13) 6.5.7 Kontrole zabezpieczeń sieci

— OVR-6.5.7-02 Wymagany w pkt REQ-7.8-13 normy ETSI EN 319 401 [1] skan podatności przeprowadza się co najmniej raz na kwartał,

— OVR-6.5.7-03 Wymagany w pkt REQ-7.8-17X ETSI EN 319 401 [1] test penetracyjny przeprowadza się co najmniej raz w roku,

— OVR-6.5.7-04 Zapory sieciowe należy skonfigurować tak, aby uniemożliwić wszelkie protokoły i dostępy, które nie są wymagane do funkcjonowania dostawcy usług zaufania.

14) 6.6.1 Profil certyfikatu

— GEN-6.6.1-05 Certyfikat zawiera jeden z identyfikatorów polityki określonych w GEN-6.3.3-02 [WYBÓR].

2. W przypadku normy ETSI EN 319 412-3

1) 2.1 Odniesienia normatywne

— [2] ETSI EN 319 412-2 V2.4.1 „Podpisy elektroniczne i infrastruktura (ESI); Profile certyfikatu; Część 2: Profil certyfikatu dla certyfikatów wydawanych osobom fizycznym”.

2) 4.2.1 Podmiot

— LEG-4.2.1-6 Atrybut organizationIdentifier zawiera identyfikację organizacji będącej podmiotem inną niż nazwa organizacji. Jeżeli wiadomo, że istnieje odpowiedni numer rejestracyjny, atrybut „organizationIdentifier” zawiera wartość tego numeru rejestracyjnego, zgodnie z odpowiednim oficjalnym rejestrem, w którym ten numer rejestracyjny został nadany.

3. W przypadku normy ETSI EN 319 412-2

1) 2.1 Odniesienia normatywne

— [2] ETSI EN 319 412-5 V2.5.1 „Podpisy elektroniczne i infrastruktura zaufania (ESI); Profile certyfikatu; Część 5: Deklaracje dla certyfikatów kwalifikowanych”,

— [9] Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa, podgrupa ds. kryptografii: „Uzgodnione mechanizmy kryptograficzne” opublikowane przez ENISA.

2) 2.2 Odniesienia informacyjne

— [i.7] nieważne.

3) 4.2.2 Podpis

— GEN-4.2.2-2 Algorytm podpisu wybiera się zgodnie z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA [9],

— UWAGA nieważna.

4) 4.2.3.1 Wydawcy będący osobami prawnymi

— GEN-4.2.3.1-3 Jeżeli wiadomo, że istnieje odpowiedni numer rejestracyjny, to dane identyfikujące wydawcę muszą zawierać organizationIdentifier z wartością tego numeru rejestracyjnego, zgodnie z odpowiednim oficjalnym rejestrem, w którym ten numer został nadany.

5) 4.2.5 Dane dotyczące klucza publicznego podmiotu

— GEN-4.2.5-2 Klucz publiczny podmiotu wybiera się zgodnie z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA[9],

— UWAGA nieważna.

6) 4.2.6 Numer seryjny

— GEN-4.2.6-01 Atrybut serialNumber certyfikatu (jak określono w IETF RFC 5280 [1] pkt 4.1.2.2) musi być niepowtarzalny dla każdego certyfikatu wydanego przez dostawcę usług zaufania.