ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2025/1942

z dnia 29 września 2025 r.

ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do kwalifikowanych usług walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych usług walidacji 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. 33 ust. 2 i art. 40,

a także mając na uwadze, co następuje:

(1) Kwalifikowane usługi walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych zapewniają integralność, autentyczność i poprawność procesu i wyników walidacji, odpowiednio, kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych. Te kwalifikowane usługi zaufania odgrywają kluczową rolę w cyfrowym otoczeniu biznesowym, ponieważ wspierają przejście od tradycyjnych procesów opartych na dokumentacji papierowej do ich elektronicznych odpowiedników.

(2) Domniemanie zgodności określone w art. 33 ust. 2 i art. 40 rozporządzenia (UE) nr 910/2014 powinno mieć zastosowanie wyłącznie w przypadku, gdy kwalifikowane usługi walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych są zgodne z normami technicznymi 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 kwalifikowanych podpisów elektronicznych i kwalifikowanych 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. 33 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 i specyfikacji dotyczących kwalifikowanych usług walidacji kwalifikowanych podpisów elektronicznych oraz kwalifikowanych usług walidacji kwalifikowanych pieczęci elektronicznych

Normy ETSI TS 119 441 V1.2.1 (2023-10) ([1]) („ETSI TS 119 441") oraz ETSI TS 119 172-4 V1.1.1 (2021-05) ([2]) („ETSI TS 119 172-4") stosuje się z zastrzeżeniem następujących dostosowań:

1. W przypadku ETSI TS 119 441

1) 2.1 Odniesienia normatywne

— [1] ETSI TS 119 101 V1.1.1 (2016-03) „Podpisy elektroniczne i infrastruktura (ESI); Wymagania polityki i bezpieczeństwa w odniesieniu do wniosków o składanie i walidację podpisów",

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

— [3] ETSI EN 319 102-1 V1.4.1 (2024-06) „Podpisy elektroniczne i infrastruktura (ESI); Procedury składania i walidacji podpisów cyfrowych AdES; Część 1: Składanie i walidacja",

— [4] ISO/IEC 15408-1:2022 – Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Kryteria oceny zabezpieczeń informatycznych"

— [5] nieważny,

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

— [7] 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) ([3]),

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

— [9] ETSI TS 119 102-2 V1.4.1 (2023-06) „Podpisy elektroniczne i infrastruktura (ESI); Procedury składania i walidacji podpisów cyfrowych AdES; Część 2: Sprawozdanie z walidacji podpisu",

— [10] Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa, podgrupa ds. kryptografii: „Uzgodnione mechanizmy kryptograficzne" opublikowane przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa („ENISA") ([4]),

— [11] Rozporządzenie wykonawcze Komisji (UE) 2024/3144 ([5]) w sprawie zmiany rozporządzenia wykonawczego (UE) 2024/4822 w odniesieniu do mających zastosowanie norm międzynarodowych i w sprawie sprostowania tego rozporządzenia wykonawczego,

— [12] ETSI EN 319 411-1 „Podpisy elektroniczne i infrastruktura (ESI); Wymagania polityki i bezpieczeństwa dla dostawców usług zaufania wydających certyfikaty; Część 1: Wymogi ogólne".

([1]) ETSI TS 119 441 – Podpisy elektroniczne i infrastruktura (ESI); Wymogi polityki dotyczące dostawcy usług zaufania świadczącego usługi walidacji podpisu, V1.2.1 (2023-10).
([2]) ETSI TS 119 172-4 – Podpisy elektroniczne i infrastruktura (ESI); Zasady składania podpisów; Część 4: Zasady stosowania podpisu (polityka walidacji) w odniesieniu do europejskich kwalifikowanych podpisów/pieczęci elektronicznych z wykorzystaniem zaufanych list, V1.1.1 (2021-05).
([3]) Dz.U. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([4]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([5]) Dz.U. L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

2) 2.2 Odniesienia informacyjne

— [i.11] nieważne.

3) 3.3 Skróty

— EUCC – europejski program certyfikacji cyberbezpieczeństwa oparty na wspólnych kryteriach

4) 4.3.3 Proces

— UWAGA 10 Zob. norma ETSI EN 319 102-1 [3] w celu uzyskania wytycznych oraz norma ETSI TS 119 172-4 [8] w celu uzyskania dodatkowych wytycznych dotyczących przypadku kwalifikowanego podpisu lub pieczęci kwalifikowanej UE.

5) 6.1 Oświadczenie na temat praktyk dotyczących usług walidacji podpisów (SVS)

— OVR-6.1-02 Oświadczenie o praktykach SVS musi mieć strukturę zgodną z załącznikiem A,

— OVR-6.1-03 Oświadczenie o praktykach SVS musi zawierać wykaz lub odniesienie do wspieranych polityk SVS (np. za pośrednictwem identyfikatora obiektu) i krótko je opisywać.

6) 6.3 Polityka bezpieczeństwa informacji

— OVR-6.3-02 W polityce bezpieczeństwa należy dokumentować kontrole bezpieczeństwa i prywatności wprowadzone w celu ochrony danych osobowych.

7) 7.2 Zasoby ludzkie

— OVR-7.2-02 Personel SVSP (dostawca usług walidacji podpisów) 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 pkt OVR-7.2-02 obejmuje regularne aktualizacje (co najmniej raz na 12 miesięcy) dotyczące nowych zagrożeń i obecnych praktyk w zakresie bezpieczeństwa.

8) 7.5 Kontrole kryptograficzne

— OVR-7.5-02 [WARUNKOWO] W przypadku podpisania sprawozdań z walidacji certyfikat podpisu publicznego SVSP odpowiadający kluczowi podpisu prywatnego SVSP jest wydawany przez wiarygodny urząd certyfikacji zgodnie z polityką certyfikacji NCP+ określoną w normie ETSI EN 319 411-1 [12]. Certyfikat należy wydawać zgodnie z odpowiednią polityką certyfikacji określoną w normie ETSI EN 319 411-2 [i.17],

— OVR-7.5-03 [WARUNKOWO] Po podpisaniu sprawozdań z walidacji klucz prywatnego podpisu SVSP jest przechowywany i wykorzystywany w bezpiecznym urządzeniu kryptograficznym, które jest wiarygodnym systemem certyfikowanym zgodnie z:

a) wspólnymi kryteriami oceny bezpieczeństwa technologii informacyjnych, określonymi w normie ISO/IEC 15408 [4] 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 poświadczonych zgodnie z EAL na poziomie 4 lub wyższym; lub

b) EUCC [7][11] i certyfikowany zgodnie z EAL na poziomie 4 lub wyższym; lub

c) do dnia 31.12.2030 r. FIPS PUB 140-3 [6] 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 [7][11], urządzenie to musi być skonfigurowane i używane zgodnie z tą certyfikacją.

— OVR-7.5-04 nieważny,

— OVR-7.5-06 Prywatny klucz podpisu SVSP jest eksportowany i importowany do innego bezpiecznego urządzenia kryptograficznego wtedy, gdy ten eksport i import są realizowane w sposób bezpieczny i zgodnie z certyfikacją tych urządzeń.

9) 7.7 Bezpieczeństwo operacji

— OVR-7.7-02 Aby zapewnić, by systemy, w których opracowano aplikację, stosowały odpowiednie środki bezpieczeństwa i dostosowywały się do określonych środowisk aplikacji, SVA korzysta ze środowiska aplikacji, które jest utrzymywane za pomocą aktualnych poprawek zabezpieczeń,

— OVR-7.7-03 Do SVA stosuje się następujące wymagania określone w ETSI TS 119 101 [1], pkt 5.2: GSM 1.3.

10) 7.8 Bezpieczeństwo sieci

— OVR-7.8-02 Jeżeli dozwolony jest zdalny dostęp do systemów przechowywania lub przetwarzania danych poufnych, należy przyjąć formalną politykę i opisać ją jako część elementów wymaganych zgodnie z pkt OVR-6.3-02,

— OVR-7.8-04 Wymagany w pkt REQ-7.8-13 ETSI EN 319 401 [1] skan podatności przeprowadza się co najmniej raz na kwartał,

— OVR-7.8-05 Wymagany w pkt REQ-7.8-17X normy ETSI EN 319 401 [1] test penetracyjny przeprowadza się co najmniej raz w roku,

— OVR-7.8-06 Zapory sieciowe należy skonfigurować tak, aby uniemożliwić wszelkie protokoły i dostępy, które nie są wymagane do funkcjonowania SVSP.

11) 7.12 Usługi walidacji podpisów obejmujące zakończenie działalności i plany zakończenia działalności

— OVR-7.12-02 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.1].

12) 7.14 Łańcuch dostaw

— OVR-7.14-01 Stosuje się wymagania określone w normie ETSI EN 319 401 [2], pkt 7.14.

13) 8.1 Proces walidacji podpisu

— VPR-8.1-07 Aplikacja do walidacji (SVA) musi spełniać wymogi określone w normie ETSI TS 119 101 [1], pkt 7.4, SIA 1–SIA 4,

— VPR-8.1-11 [WARUNKOWO] Jeżeli celem SVS (usługa walidacji podpisów) jest walidacja kwalifikowanych podpisów elektronicznych lub kwalifikowanych pieczęci elektronicznych zgodnie z art. 32 ust. 1 (lub odpowiednio art. 40) rozporządzenia (UE) nr 910/2014 [i.1], proces walidacji musi być zgodny z wymogami normy ETSI TS 119 172-4 [8].

14) 8.2 Protokół walidacji podpisu

— SVP-8.2-03 Odpowiedź na walidację podpisu musi być opatrzona identyfikatorem obiektu polityki SVS.

15) 8.4 Sprawozdanie z walidacji podpisu

— SVR-8.4-02 Sprawozdanie z walidacji musi być zgodne z normą ETSI TS 119 102-2 [9],

— SVR-8.4-07 [WARUNKOWO] Jeżeli polityka walidacji podpisów nie jest w pełni przetwarzana przez SVS, sprawozdanie zawiera, oprócz sprawozdawczości na temat walidowanych ograniczeń, informacje o ograniczeniach, które zignorowano lub zniesiono,

— SVR-8.4-15 W sprawozdaniu z walidacji wyraźnie wskazuje się pochodzenie każdego PoE (od podpisu, od klienta, z serwera),

— SVR-8.4-16 Sprawozdanie z walidacji musi być opatrzone podpisem sprawozdania z walidacji, którym jest podpis cyfrowy SVSP,

— SVR-8.4-17 [WARUNKOWO] W przypadku podpisania sprawozdań z walidacji format i cel podpisu muszą być zgodne z normą ETSI TS 119 102-2 [9].

16) 9 Ramy określania polityk usług walidacji oparte na polityce usług zaufania określonej w niniejszym dokumencie:

— OVR-9-05 [WARUNKOWO] Przy opracowywaniu polityki SVS w oparciu o politykę usług zaufania określoną w niniejszym dokumencie przeprowadza się ocenę ryzyka w celu oceny wymogów biznesowych i określenia wymogów bezpieczeństwa, które należy uwzględnić w polityce danej społeczności i możliwości zastosowania,

— OVR-9-06 [WARUNKOWO] Przy opracowywaniu polityki SVS w oparciu o politykę usług zaufania określoną w niniejszym dokumencie polityka ta jest zatwierdzana i zmieniana zgodnie z określonym procesem przeglądu, z uwzględnieniem odpowiedzialności za utrzymanie tej polityki,

— OVR-9-07 [WARUNKOWO] Przy opracowywaniu polityki SVS w oparciu o politykę usług zaufania określoną w niniejszym dokumencie stosuje się określony proces przeglądu w celu zapewnienia, aby polityka ta była poparta oświadczeniami dotyczącymi praktyk,

— OVR-9-08 [WARUNKOWO] Przy opracowywaniu polityki SVS w oparciu o politykę usług zaufania określoną w niniejszym dokumencie, dostawca usług zaufania udostępnia społeczności użytkowników politykę wspieraną przez dostawcę usług zaufania,

— OVR-9-09 [WARUNKOWO] Przy opracowywaniu polityki SVS w oparciu o politykę usług zaufania określoną w niniejszym dokumencie należy udostępnić abonentom zmiany polityk obsługiwanych przez dostawcę usług zaufania.

17) Załącznik B (normatywny) Usługa walidacji kwalifikowanego podpisu elektronicznego zdefiniowana w art. 33 rozporządzenia (UE) nr 910/2014:

— VPR-B-02 [WARUNKOWO] Jeżeli SVSP jest QSVSP, wdrożenie musi być zgodne z normą ETSI TS 119 172-4 [8],

— UWAGA 2 nieważna,

— OVR-B-04 [WARUNKOWO] Jeżeli SVSP jest QSVSP, w badaniach OVR-B-03 sprawdza się różne przypadki użycia: pozytywne i negatywne,

— VPR-B-11 [WARUNKOWO] Jeżeli SVSP jest QSVSP, SVSP kontroluje obliczenia skrótu (przeprowadza obliczenia po stronie serwera lub kontroluje klienta, jeżeli jest to dozwolone po stronie klienta),

— UWAGA 5 nieważna,

— UWAGA 6 nieważna,

— VPR-B-15 [WARUNKOWO] Jeżeli SVSP jest QSVSP, aby spełnić wymogi VPR-B-13 do VPR-B-14, sprawozdanie z walidacji musi być zgodne z normą ETSI TS 119 102-2 [9],

— VPR-B-16 [WARUNKOWO] Jeżeli SVSP jest QSVSP, wdrożenie musi być zgodne z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA [10] w celu stosowania odpowiednich technik kryptograficznych przy świadczeniu kwalifikowanych usług walidacji na potrzeby kwalifikowanego podpisu elektronicznego.

18) Załącznik C (informacyjny) Przyporządkowanie wymogów do rozporządzenia (UE) nr 910/2014, sekcja „Zapewnianie walidacji zgodnie z art. 32 ust. 1”, akapit drugi:

— Aby zapewnić weryfikację wszystkich warunków wymaganych na mocy art. 32 ust. 1 i art. 40 rozporządzenia (UE) nr 910/2014 [i.1], potrzebny jest prawidłowy algorytm walidacji. Daje on taki sam wynik deterministyczny w odniesieniu do podpisu lub pieczęci przedłożonych do zatwierdzenia. W tym celu kluczowe są zasady walidacji. Z tą myślą wydano normę ETSI TS 119 172-4 [8], opartą na algorytmie walidacji określonym w normie ETSI EN 319 102-1 [3].

2. W przypadku normy 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 składania i walidacji podpisów cyfrowych AdES; Część 1: Składanie i walidacja”,

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

— [2] ETSI TS 119 612 V2.3.1 (2024-11) „Podpisy elektroniczne i infrastruktura (ESI); Zaufane listy”,

— [13] ETSI TS 119 101 V1.1.1 (2016-03) „Podpisy elektroniczne i infrastruktura (ESI); Wymagania polityki i bezpieczeństwa w odniesieniu do wniosków o składanie i walidację podpisów”.

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

— (i) Jeżeli certyfikat podmiotu końcowego stanowi kotwicę zaufania, nie stosuje się mechanizmu RevocationCheckingConstraints,

— (ii) Jeżeli certyfikat podmiotu końcowego nie stanowi kotwicy zaufania, mechanizm 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 24 godzin dla certyfikatu podpisu. W przypadku certyfikatów innych niż certyfikat podpisu, w tym certyfikatów potwierdzających znaczniki czasu, nie ustala się żadnej wartości dla RevocationFreshnessConstraints.

3) 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:

a) zaprzestaje się procesu;

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

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