Dziennik Urzędowy
Unii Europejskiej

PL
Seria L

2025/2531

17.12.2025

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2025/2531

z dnia 16 grudnia 2025 r.

ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do norm referencyjnych i specyfikacji dotyczących kwalifikowanych rejestrów 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. 45l ust. 3,

a także mając na uwadze, co następuje:

(1) Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2024/1183 ([2]) do rozporządzenia (UE) nr 910/2014 wprowadzono wykaz nowych usług zaufania i kwalifikowanych usług zaufania, w tym rejestrowania danych elektronicznych w kwalifikowanym rejestrze elektronicznym. Komisja ma ustanowić wykaz norm referencyjnych i, w razie potrzeby, ustanowić specyfikacje dotyczące takich usług.

(2) Rejestr elektroniczny to sekwencja elektronicznych wpisów danych, która ma zapewnić integralność tych wpisów danych i prawidłowość ich chronologicznego uporządkowania. W celu zapewnienia, aby rejestrowanie danych w kwalifikowanym rejestrze elektronicznym było uporządkowane chronologicznie, spójne i wiarygodne, konieczne jest ustanowienie wspólnego zestawu specyfikacji dotyczących rejestrowania danych elektronicznych w kwalifikowanym rejestrze elektronicznym.

(3) Domniemanie zgodności określone w art. 45l ust. 2 rozporządzenia (UE) nr 910/2014 powinno mieć zastosowanie wyłącznie w przypadku, gdy kwalifikowane usługi zaufania w zakresie rejestrowania danych elektronicznych w kwalifikowanym rejestrze elektronicznym 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 kwalifikowanej usługi zaufania.

(4) 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.

(5) Komisja regularnie przeprowadza ocenę nowych technologii, praktyk, norm lub specyfikacji technicznych. Zgodnie z motywem 75 rozporządzenia (UE) 2024/1183 Komisja powinna, w razie potrzeby, poddawać niniejsze rozporządzenie przeglądowi i aktualizacji, aby zachować jego aktualność względem globalnych zmian, nowych technologii, praktyk, 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).

(6) Do czynności przetwarzania danych osobowych na podstawie niniejszego rozporządzenia mają zastosowanie rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 ([3]) oraz – w stosownych przypadkach – dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady ([4]), z uwzględnieniem również wytycznych Europejskiej Rady Ochrony Danych nr 02/2025 dotyczących przetwarzania danych osobowych z wykorzystaniem technologii blockchain ([5]).

(7) 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 21 października 2025 r. ([7]).

(8) 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

Normy referencyjne i specyfikacje

Normy referencyjne i specyfikacje, o których mowa w art. 45l ust. 3 rozporządzenia (UE) nr 910/2014, dotyczące kwalifikowanych rejestrów elektronicznych, 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 16 grudnia 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]) edpb_guidelines_202502_blockchain_en.pdf.

([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 Implementing Regulation laying down rules for the application of Regulation (EU) No 910/2014 as regards reference standards and specifications for qualified electronic ledgers [Formalne uwagi EIOD do projektu rozporządzenia wykonawczego ustanawiającego zasady stosowania rozporządzenia (UE) nr 910/2014 w odniesieniu do norm referencyjnych i specyfikacji dotyczących kwalifikowanych rejestrów elektronicznych].

ZAŁĄCZNIK

Wykaz specyfikacji technicznych i norm referencyjnych dotyczących kwalifikowanych rozproszonych rejestrów elektronicznych

1. Do celów niniejszego rozporządzenia stosuje się następujące definicje:

   a) „ostateczność” oznacza stan wpisu danych w rejestrze elektronicznym, który stał się nieodwracalny i nie może zostać zmieniony ani usunięty;

   b) „rozproszony rejestr elektroniczny” oznacza rejestr elektroniczny, który jest współdzielony przez zbiór węzłów rozproszonego rejestru elektronicznego i który jest synchronizowany między węzłami rozproszonego rejestru elektronicznego przy użyciu mechanizmu konsensusu;

   c) „węzeł rozproszonego rejestru elektronicznego” oznacza urządzenie lub proces będący częścią sieci rozproszonego rejestru elektronicznego przechowujący pełną lub częściową kopię wpisów danych rejestru elektronicznego;

   d) „sieć rozproszonego rejestru elektronicznego” oznacza sieć węzłów rozproszonego rejestru elektronicznego, która tworzy system rozproszonego rejestru elektronicznego;

   e) „system rozproszonego rejestru elektronicznego” oznacza system, w którym wdrożono rozproszony rejestr elektroniczny;

   f) „konsensus” oznacza porozumienie między węzłami rozproszonego rejestru elektronicznego w sprawie ważności transakcji oraz utrzymania spójnego i uporządkowanego zestawu zwalidowanych transakcji w całym systemie rozproszonego rejestru elektronicznego;

   g) „mechanizm konsensusu” oznacza zbiór zasad i procedur, za pomocą których osiągany jest konsensus;

   h) „zasady zarządzania” oznaczają zbiór protokołów, polityk i mechanizmów, które określają sposób działania systemu rozproszonego rejestru elektronicznego, sposób walidacji i dodawania danych do rejestru elektronicznego oraz sposób interakcji uczestników;

   i) „transakcja” oznacza najmniejszą jednostkę procesu roboczego w rejestrze elektronicznym;

   j) „proces roboczy” oznacza co najmniej jedną sekwencję działań wymaganych do uzyskania wyniku zgodnego z zasadami zarządzania rejestrem elektronicznym;

   k) „zwalidowana transakcja” oznacza transakcję, w przypadku której sprawdzono wymaganą integralność, autentyczność i warunki specyficzne dla protokołu zgodnie z zasadami zarządzania systemem rozproszonego rejestru elektronicznego;

   l) „połączenie kryptograficzne” oznacza odniesienie do danych ustanowione przy użyciu odpowiednich technik kryptograficznych w celu zapewnienia integralności, autentyczności lub identyfikowalności danych, do których odnosi się odniesienie, oraz prawidłowej sekwencji wpisów danych;

   m) „raport z rejestru” oznacza uporządkowane przedstawienie weryfikowalnych informacji pobranych z wpisów danych rejestru elektronicznego, zapewniające wgląd w konkretne działania, stany lub zgodność z wcześniej określonymi zasadami;

   n) „dostawca kwalifikowanego rejestru elektronicznego” oznacza kwalifikowanego dostawcę usług zaufania, który świadczy kwalifikowaną usługę zaufania polegającą na rejestrowaniu danych w kwalifikowanym rejestrze elektronicznym;

   o) „kwalifikowany rozproszony rejestr elektroniczny” oznacza rozproszony rejestr elektroniczny, który spełnia wymogi kwalifikowanego rejestru elektronicznego.

2. W przypadku gdy kwalifikowany dostawca usług zaufania musi sporządzić raport z rejestru, sporządza się go w sposób zautomatyzowany.

3. Dostawcy kwalifikowanych rejestrów elektronicznych tworzą, aktualizują i utrzymują kwalifikowany rejestr elektroniczny oraz rejestrują w nim dane elektroniczne zgodnie ze specyfikacjami ustanowionymi w:

   a) w odniesieniu do wszystkich dostawców kwalifikowanych rejestrów elektronicznych, normie ETSI EN 319 401 v3.1.1 (2024-06) z następującymi dostosowaniami:

      — 2.1 Odniesienia normatywne:

        [1] Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa, podgrupa ds. kryptografii: „Uzgodnione mechanizmy kryptograficzne” opublikowane przez Agencję Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji („ENISA”).

[2] IETF RFC 7515 (maj 2015 r.): „Podpis internetowy JSON (JWS)".

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

[4] 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).

[5] 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.

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

— 6.1 Oświadczenie dotyczące praktyk w zakresie usług zaufania:

  — REQ-6.1-12 Oświadczenie na temat praktyk dotyczących rejestrów elektronicznych zawiera co najmniej informacje na temat:

    — możliwości funkcjonalnych i technicznych platformy rejestru elektronicznego i jej wykorzystania przez cały okres świadczenia usługi rejestrowania danych w kwalifikowanym rejestrze elektronicznym jako kwalifikowanej usługi zaufania,

    — konkretnych mechanizmów uwierzytelniania pochodzenia danych stosowanych podczas świadczenia usługi,

    — konkretnych mechanizmów sekwencyjnego porządkowania chronologicznego stosowanych podczas świadczenia usługi,

    — w stosownych przypadkach, połączenia kryptograficznego wykorzystywanego do zapewnienia sekwencji wpisów danych,

    — w stosownych przypadkach mechanizmu konsensusu zapewniającego ostateczność i integralność wpisów danych oraz transakcji przechowywanych w rejestrze, z uwzględnieniem ewentualnego czasu ostrożności potrzebnego do osiągnięcia ostateczności i integralności,

    — konkretnych mechanizmów zapewniania integralności danych stosowanych podczas świadczenia usługi.

  — 6.2 Warunki:

    — REQ-6.2-03 Przed nawiązaniem stosunku umownego abonenci i strony ufające korzystające z usługi zaufania są informowani, w sposób jasny, wyczerpujący i łatwo dostępny, w publicznie dostępnej przestrzeni i indywidualnie, o dokładnych warunkach korzystania z usługi, w tym o kwestiach wymienionych powyżej.

  — 6.3 Polityka bezpieczeństwa informacji:

    — REQ-6.3-04X Dostawca usług zaufania ustanawia procedury powiadamiania organu nadzoru o wszelkich zmianach w świadczeniu usługi zaufania, zgodnie z wymogami biznesowymi oraz odpowiednimi przepisami ustawowymi i wykonawczymi. Dostawca usług zaufania powiadamia organ nadzoru co najmniej:

      — na miesiąc przed wprowadzeniem jakiejkolwiek zmiany,

      — na trzy miesiące przed planowanym zaprzestaniem świadczenia usług zaufania.

  — 7.2 Zasoby ludzkie:

    — REQ-7.2-04X Personel dostawcy usług zaufania pełniący zaufane funkcje musi 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.

— REQ-7.2-05X Obejmuje to regularne (co najmniej raz na 12 miesięcy) aktualizacje dotyczące nowych zagrożeń i obecnych praktyk w zakresie bezpieczeństwa.

— 7.5 Kontrole kryptograficzne:

— REQ-7.5-01X 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-7.5-02 W celu świadczenia usług zaufania dostawca usług zaufania wybiera i stosuje odpowiednie techniki kryptograficzne zgodne z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA [1].

W szczególności:

— REQ-7.5-03 Dostawcy kwalifikowanych rejestrów elektronicznych ustalają pochodzenie wpisów danych w rejestrze elektronicznym. W tym zakresie stosują oni zaawansowane podpisy elektroniczne oparte na kwalifikowanych certyfikatach lub zaawansowane pieczęcie elektroniczne oparte na kwalifikowanych certyfikatach utworzonych przez użytkowników usługi zgodnie z następującymi normami i specyfikacjami:

a) ETSI EN 319 122-1 V1.3.1 (2023-06). Podpisy elektroniczne i infrastruktura (ESI); Podpisy cyfrowe CAdES; Część 1: Elementy składowe i podstawowe profile podpisów CAdES.

b) ETSI EN 319 132-1 V1.3.1 (2024-07). Podpisy elektroniczne i infrastruktury zaufania (ESI); Podpisy cyfrowe XAdES; Część 1: Elementy składowe i podstawowe profile podpisów XAdES.

c) ETSI TS 119 182-1 V1.2.1 (2024-07). Podpisy elektroniczne i infrastruktury zaufania (ESI); Podpisy cyfrowe JAdES; Część 1: Elementy podstawowe i podstawowe profile podpisów JAdES, z następującym dostosowaniem:

— 5.1.8 Parametr nagłówka x5c (łańcuch certyfikatów X.509)

— Parametr nagłówka x5c określony w klauzuli 4.1.6 normy IETF RFC 7515 [2] musi być obecny w podpisie JAdES jako podpisany albo niepodpisany parametr nagłówka.

— Parametr nagłówka x5c musi mieć semantykę określoną w klauzuli 4.1.6 normy IETF RFC 7515 [2].

— Parametr nagłówka x5c musi mieć składnię określoną w klauzuli 4.1.6 normy IETF RFC 7515 [2].

— REQ-7.5-04: Dostawcy kwalifikowanych rejestrów elektronicznych zapewniają niepowtarzalne sekwencyjne uporządkowanie chronologiczne wpisów danych w rejestrze elektronicznym. W tym zakresie wykorzystują połączenia kryptograficzne oparte na listach skrótów lub drzewach skrótów, wykorzystując kryptograficzne funkcje skrótu, zgodnie z następującymi specyfikacjami i normami:

a) rozmiar skrótu wyjściowego SHA-256 lub wyższy, zgodnie z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA [1];

b) rozmiar skrótu wyjściowego SHA3-256 lub wyższy, zgodnie z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA [1].

Alternatywnie, stosując rejestrację czasu w celu zapewnienia niepowtarzalnego sekwencyjnego uporządkowania chronologicznego wpisów danych w rejestrze elektronicznym, dostawcy kwalifikowanych rejestrów elektronicznych wykorzystują kwalifikowane znaczniki czasu.

— REQ-7.5-05 Dostawcy kwalifikowanych rejestrów elektronicznych zapewniają integralność wpisów danych zapisanych w kwalifikowanym rejestrze elektronicznym. W tym zakresie stosują oni zaawansowane podpisy elektroniczne oparte na kwalifikowanych certyfikatach lub zaawansowane pieczęcie elektroniczne oparte na kwalifikowanych certyfikatach, zgodnie z następującymi normami i specyfikacjami:

  a) wszelkie formaty podpisów lub pieczęci zgodne z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA [1];

  b) rozmiar skrótu wyjściowego SHA-256 lub wyższy, zgodnie z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA [1];

  c) rozmiar skrótu wyjściowego SHA3-256 lub wyższy, zgodnie z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA [1];

  d) dostawcy kwalifikowanych rejestrów elektronicznych zapewniają natychmiastową wykrywalność wszelkich późniejszych zmian w danych zapisanych w kwalifikowanym rejestrze elektronicznym.

— REQ-7.5-06 W przypadku stosowania mechanizmów podpisu cyfrowego prywatne klucze podpisu dostawcy kwalifikowanego rejestru elektronicznego są przechowywane i używane w bezpiecznym urządzeniu kryptograficznym, które jest wiarygodnym systemem certyfikowanym zgodnie z:

  a) wspólnymi kryteriami oceny bezpieczeństwa technologii informacyjnych, określonymi w normie ISO/IEC 15408 ([1]) [6] 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) europejskim programem certyfikacji cyberbezpieczeństwa opartym na wspólnych kryteriach (EUCC) ([2]) ([3]) [4][5] i certyfikowanym zgodnie z EAL na poziomie 4 lub wyższym; lub

  c) do dnia 31.12.2030 r. FIPS PUB 140-3 ([4]) [3] 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 [4][5], urządzenie to musi być skonfigurowane i używane zgodnie z tą certyfikacją.

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

([2]) 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/2024/482/2025-01-08).

([3]) 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).

([4]) FIPS PUB 140-3 (2019): „Wymogi bezpieczeństwa dotyczące modułów kryptograficznych”.

— 7.8 Bezpieczeństwo sieci:

— REQ-7.8-14X Wymagany w pkt REQ-7.8-13 skan podatności przeprowadza się co najmniej raz na kwartał.

— REQ-7.8-18X Wymagany w pkt REQ-7.8-17X test penetracyjny przeprowadza się co najmniej raz w roku.

— REQ-7.8-21X: Zapory sieciowe należy również skonfigurować tak, aby uniemożliwić wszelkie protokoły i dostępy, które nie są wymagane do funkcjonowania dostawcy usług zaufania.

— 7.9.1 Monitorowanie i rejestrowanie:

— REQ-7.9.1-02X Działania monitorujące uwzględniają wrażliwość wszelkich gromadzonych lub analizowanych informacji.

— 7.12 Zakończenie działalności dostawcy usług zaufania i plany zakończenia działalności:

— REQ-7.12-02 A 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].

b) Dodatkowo w przypadku wszystkich dostawców kwalifikowanych rejestrów elektronicznych korzystających z technologii rozproszonego rejestru elektronicznego:

1) norma ISO 23257:2022 Technologie blockchain i rozproszonego rejestru – Architektura referencyjna, klauzula 9, zawierająca pełny opis systemu technologii rozproszonego rejestru elektronicznego, odpowiedniej sieci technologii rozproszonego rejestru elektronicznego i węzłów technologii rozproszonego rejestru elektronicznego;

2) norma ISO/TS 23635:2022. Technologie blockchain i rozproszonego rejestru – Wytyczne dotyczące zarządzania w odniesieniu do pisemnych i publicznie dostępnych polityk i praktyk związanych ze strukturą zarządzania usługą rejestru elektronicznego, którą świadczą.