Dziennik Urzędowy
Unii Europejskiej

PL
Seria L

2025/1929

30.9.2025

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2025/1929

z dnia 29 września 2025 r.

ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do powiązania daty i czasu z danymi oraz określenia dokładności źródeł czasu do celów zapewniania kwalifikowanych elektronicznych znaczników czasu

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. 42 ust. 2,

a także mając na uwadze, co następuje:

(1) Kwalifikowane elektroniczne znaczniki czasu odgrywają kluczową rolę w środowisku cyfrowym poprzez wspieranie przejścia od tradycyjnych procesów opartych na dokumentacji papierowej do ich elektronicznych odpowiedników. Dzięki powiązaniu informacji o dacie i czasie z danymi elektronicznymi kwalifikowane elektroniczne znaczniki czasu pomagają zapewnić dokładność wskazanej daty i godziny oraz integralność dokumentów cyfrowych, z którymi dana data i godzina są powiązane.

(2) Domniemanie zgodności określone w art. 42 ust. 1a rozporządzenia (UE) nr 910/2014 powinno mieć zastosowanie wyłącznie w przypadku, gdy kwalifikowane usługi zaufania w zakresie wydawania kwalifikowanych znaczników czasu są zgodne z normami określonymi w niniejszym rozporządzeniu. Przedmiotowe normy powinny odzwierciedlać utrwalone praktyki i być powszechnie uznawane w odpowiednich sektorach. Normy te należy dostosować w taki sposób, aby obejmowały dodatkowe kontrole zapewniające bezpieczeństwo i wiarygodność kwalifikowanej usługi zaufania oraz powiązania daty i czasu z danymi, a także dokładność źródeł czasu.

(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 poddawać przeglądowi i w razie potrzeby aktualizować niniejsze rozporządzenie wykonawcze, aby zachować jego 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) nr 910/2014,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Normy referencyjne i specyfikacje, o których mowa w art. 42 ust. 2 rozporządzenia (UE) nr 910/2014, określono w załączniku do niniejszego rozporządzenia.

Artykuł 2

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

Wykaz norm referencyjnych i specyfikacji dotyczących kwalifikowanych usług znacznika czasu

Normy ETSI EN 319 421 V1.3.1 ([1]) („ETSI EN 319 421") oraz ETSI EN 319 422 V1.1.1 ([2]) („ETSI EN 319 422") stosuje się z zastrzeżeniem następujących dostosowań:

1. W przypadku ETSI EN 319 421

1) 2.1 Odniesienia normatywne:

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

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

— [5] ETSI EN 319 422 V1.1.1 (2016-03) „Podpisy elektroniczne i infrastruktura elektroniczna (ESI); Protokół znakowania czasem oraz profile tokenu znacznika czasu",

— [6] nieważny,

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

— [10] Rozporządzenie wykonawcze Komisji (UE) 2024/482 ([4]) 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"),

— [11] Rozporządzenie wykonawcze Komisji (UE) 2024/3144 ([5]) 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.

2) 3.1 Warunki

— okres ważności certyfikatu: przedział czasu od notBefore do notAfter włącznie, w którym urząd certyfikacji gwarantuje, że będzie utrzymywał informacje o statusie certyfikatu.

3) 3.3 Skróty

— EUCC – europejski program certyfikacji cyberbezpieczeństwa oparty na wspólnych kryteriach.

4) 6.2 Oświadczenie dotyczące praktyk w zakresie usług zaufania

— OVR-6.2-03 W swoim oświadczeniu o ujawnianiu informacji TSA zamieszcza oświadczenia o dostępności swojej usługi znacznika czasu.

5) 7.3 Bezpieczeństwo personelu

— OVR-7.3-02 Personel TSA 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-7.3-03 Zgodność z pkt OVR-7.3-02 obejmuje regularne aktualizacje (co najmniej raz na 12 miesięcy) dotyczące nowych zagrożeń i obecnych praktyk w zakresie bezpieczeństwa.

([1]) EN 319 421 – Podpisy elektroniczne i infrastruktura (ESI) – Wymagania polityki i bezpieczeństwa dla dostawców usług zaufania wydających znaczniki czasu, V1.3.1.
([2]) EN 319 422 – Podpisy elektroniczne i infrastruktura (ESI) – Protokół znakowania czasem oraz profile tokenu znacznika czasu, V1.1.1 (2016-03). https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf.
([3]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([4]) Dz.U. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([5]) Dz.U. L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

6) 7.6.2 Generowanie kluczy TSU

— TIS-7.6.2-03 Generowanie klucza(-y) TSU odbywa się w ramach bezpiecznego urządzenia kryptograficznego, które jest wiarygodnym systemem certyfikowanym zgodnie z:

a) wspólnymi kryteriami oceny bezpieczeństwa technologii informacyjnych, określonymi w normie ISO/IEC 15408 [3] 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 [10][11] i certyfikowany zgodnie z EAL na poziomie 4 lub wyższym; lub

c) do 31.12.2030 r. FIPS PUB 140-3 [7] 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 [10][11], urządzenie to musi być skonfigurowane i używane zgodnie z tą certyfikacją.

— TIS-7.6.2-04 nieważny,

— UWAGA 3 nieważna,

— TIS-7.6.2-05 A Algorytm generowania klucza TSU, długość uzyskanego klucza podpisu oraz algorytm podpisu używany odpowiednio do podpisywania znaczników czasu i do podpisywania certyfikatów klucza publicznego TSU muszą być zgodne z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa [9] i opublikowanymi przez ENISA,

— UWAGA 4 nieważna,

— TIS-7.6.2-06 Klucz podpisu TSU 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) 7.6.3 Ochrona klucza prywatnego TSU

— TIS-7.6.3-02 Klucz prywatny podpisu TSU jest przechowywany i używany w bezpiecznym urządzeniu kryptograficznym, które jest wiarygodnym systemem certyfikowanym zgodnie z:

a) wspólnymi kryteriami oceny bezpieczeństwa technologii informacyjnych, określonymi w normie ISO/IEC 15408 [3] 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

b) europejskim programem certyfikacji cyberbezpieczeństwa opartym na wspólnych kryteriach (EUCC) [10][11] i certyfikowanym zgodnie z EAL na poziomie 4 lub wyższym; lub

c) do dnia 31.12.2030 r. FIPS PUB 140-3 [7] 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 [10][11], urządzenie to musi być skonfigurowane i używane zgodnie z tą certyfikacją.

— TIS-7.6.3-03 nieważny,

— UWAGA 2 nieważna.

8) 7.6.7 Zakończenie cyklu życia klucza TSU

— TIS-7.6.7-03 A Data wygaśnięcia kluczy prywatnych TSU musi być zgodna z uzgodnionymi mechanizmami kryptograficznymi [9],

— UWAGA 1 nieważna.

9) 7.10 Bezpieczeństwo sieci

— OVR-7.10-05 Skanowanie podatności wymagane zgodnie z pkt REQ-7.8-13 normy ETSI EN 319 401 [1] przeprowadza się co najmniej raz na kwartał,

— OVR-7.10-06 Wymagany w pkt REQ-7.8-17X normy ETSI EN 319 401 [1] test penetracyjny przeprowadza się co najmniej raz w roku,

— OVR-7.10-07 Zapory sieciowe należy skonfigurować tak, aby uniemożliwić wszelkie protokoły i dostępy, które nie są wymagane do funkcjonowania TSA.

10) 7.14 Zakończenie działalności dostawcy usługi zaufania i plany zakończenia działalności

— OVR-7.14-01 A Plan zakończenia działalności musi spełniać wymogi określone w aktach wykonawczych przyjętych na podstawie art. 24 ust. 5 rozporządzenia (UE) nr 910/2014 [i.4].

2. W przypadku ETSI EN 319 422

1) 2.1 Odniesienia normatywne

— [5] nieważny,

— [6] nieważny,

— [8] Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa, podgrupa ds. kryptografii: „Uzgodnione mechanizmy kryptograficzne”,

— [9] RFC 9110 HTTP Semantics.

2) 4.1.3 Algorytmy skrótu, które należy stosować

— Stosuje się następującą klauzulę:

Algorytmy skrótu stosowane do skrótu informacji, które mają być opatrzone znacznikiem czasu, przewidywany czas trwania znacznika czasu i wybrane funkcje skrótu w stosunku do czasu muszą być zgodne z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA [8],

— UWAGA nieważna.

3) 4.2.3 Algorytmy, które mają być obsługiwane

— Stosuje się następującą klauzulę:

Algorytmy podpisu znacznika czasu, które mają być obsługiwane, muszą być zgodne z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA [8]”,

— UWAGA nieważna.

4) 4.2.4 Długości klucza, które mają być obsługiwane

— Stosuje się następującą klauzulę:

Długości kluczy algorytmu podpisu dla wybranego algorytmu podpisu muszą być zgodne z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA,

— UWAGA nieważna.

5) 5.1.3 Algorytmy, które mają być obsługiwane

— Stosuje się następującą klauzulę:

Algorytmy skrótu dla danych znacznika czasu, które mają być obsługiwane, przewidywany czas trwania znacznika czasu oraz wybrane funkcje skrótu w funkcji czasu muszą być zgodne z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA[8],

— UWAGA nieważna.

6) 5.2.3 Algorytmy, które należy stosować

— Stosuje się następującą klauzulę:

Algorytmy skrótu stosowane do skrótu informacji, które mają być opatrzone znacznikiem czasu i algorytmy podpisu znacznika czasu, muszą być zgodne z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA [8],

— UWAGA nieważna.

7) 6.3 Wymogi dotyczące długości klucza

— Stosuje się następującą klauzulę:

Długość klucza wybranego algorytmu podpisu certyfikatu TSU musi być zgodna z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA [8],

— UWAGA nieważna.

8) 6.5 Wymogi dotyczące algorytmów

— Stosuje się następującą klauzulę:

Klucz publiczny TSU i podpis certyfikatu TSU wykorzystują algorytmy zgodne z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA[8],

— UWAGA nieważna.

9) 7 Profile obsługiwanych protokołów transportowych

— Klient znakowania czasem oraz serwer znakowania czasem powinny obsługiwać protokół znakowania czasem za pośrednictwem HTTPS [9], zgodnie z definicją zawartą w pkt 3.4 dokumentu IETF RFC 3161 [1].

10) 8 Identyfikatory obiektów algorytmów kryptograficznych

— Stosuje się następującą klauzulę:

Klucz publiczny TSU i podpis certyfikatu TSU wykorzystują algorytmy zgodne z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA[8].

11) 9.1 Oświadczenie o zgodności z przepisami

— Jeżeli TSA deklaruje, że token znacznika czasu jest kwalifikowanym elektronicznym znacznikiem czasu zgodnie z rozporządzeniem (UE) nr 910/2014 [i.2], musi on zawierać jeden przypadek rozszerzenia qcStatements w polu rozszerzenia tokena czasu o składni określonej w pkt 3.2.6 dokumentu IETF RFC 3739 [i.3],

— Rozszerzenie qcStatements zawiera jeden przypadek stwierdzenia „esi4-qtstStatement-1” zgodnie z definicją w załączniku B,

— Rozszerzenia qcStatements nie należy oznaczyć jako krytyczne.