ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2025/1944

z dnia 29 września 2025 r.

ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do norm referencyjnych dotyczących procesów wysyłania i otrzymywania danych w ramach kwalifikowanych usług rejestrowanego doręczenia elektronicznego oraz dotyczących interoperacyjności tych usług

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. 44 ust. 2 i 2b,

a także mając na uwadze, co następuje:

(1) Kwalifikowane usługi rejestrowanego doręczenia elektronicznego zapewniają bezpieczny kanał przekazywania dokumentów, w tym dowodów wysłania i otrzymania danych. Służą one zapewnieniu pewności w identyfikacji adresata i utrzymaniu wysokiego poziomu zaufania do identyfikacji nadawcy.

(2) Domniemanie zgodności określone w art. 44 ust. 1a rozporządzenia (UE) nr 910/2014 powinno mieć zastosowanie wyłącznie w przypadku, gdy kwalifikowane usługi zaufania w zakresie świadczenia kwalifikowanych usług rejestrowanego doręczenia elektronicznego 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.

(3) Jeżeli dostawca usług zaufania spełnia wymogi określone w załączniku I 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 kwalifikowanego statusu 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) Zgodnie z art. 44 ust. 2a rozporządzenia (UE) nr 910/2014, w przypadku gdy kwalifikowani dostawcy usług zaufania zgadzają się na zapewnienie interoperacyjności swoich usług, ważne jest, aby przestrzegali oni odpowiednich norm i specyfikacji określonych w załączniku II do niniejszego rozporządzenia wykonawczego w celu łatwego przekazywania zarejestrowanych danych elektronicznych między co najmniej dwoma kwalifikowanymi dostawcami usług zaufania oraz w celu promowania uczciwych praktyk na rynku wewnętrznym.

(5) 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).

(6) 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.

(7) 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.

(8) 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 dotyczące kwalifikowanych usług rejestrowanego doręczenia elektronicznego

Normy referencyjne i specyfikacje, o których mowa w art. 44 ust. 2 rozporządzenia (UE) nr 910/2014, określono w załączniku I do niniejszego rozporządzenia.

Artykuł 2

Normy referencyjne i specyfikacje dotyczące interoperacyjności między kwalifikowanymi usługami rejestrowanego doręczenia elektronicznego

Normy referencyjne i specyfikacje, o których mowa w art. 44 ust. 2b rozporządzenia (UE) nr 910/2014, określono w załączniku II do niniejszego rozporządzenia.

Artykuł 3

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 I

Wykaz norm referencyjnych, o których mowa w art. 1

Norma ETSI EN 319 521 V1.1.1 (2019-02) („ETSI EN 319 521") ma zastosowanie z następującymi dostosowaniami:

1. W przypadku ETSI EN 319 521

   1) 2.1 Odniesienia normatywne:

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

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

   — [3] ETSI EN 319 522-1 V1.2.1 (2024-01) „Podpisy elektroniczne i infrastruktura (ESI); Usługi rejestrowanego doręczenia elektronicznego; Część 1: Zasady ogólne i architektura",

   — [4] ETSI EN 319 522-2 V1.2.1 (2024-01) „Podpisy elektroniczne i infrastruktura (ESI); Usługi rejestrowanego doręczenia elektronicznego; Część 2: Zawartość semantyczna",

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

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

   — [7] 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),

   — [8] 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,

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

   2) 3.1 Terminy

   — zaawansowana pieczęć elektroniczna: Zgodnie z definicją w rozporządzeniu (UE) nr 910/2014 [i.1],

   — zaawansowany podpis elektroniczny: Zgodnie z definicją w rozporządzeniu (UE) nr 910/2014 [i.1],

   — kwalifikowana pieczęć elektroniczna: Zgodnie z definicją w rozporządzeniu (UE) nr 910/2014 [i.1],

   — kwalifikowany podpis elektroniczny: Zgodnie z definicją w rozporządzeniu (UE) nr 910/2014 [i.1],

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

([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.

3) 5.1.1 Przepisy wspólne

— REQ-ERDS-5.1.1-01 ERDS zapewnia odpowiednie zagwarantowanie dostępności, integralności i poufności treści użytkowników podczas ich obsługi przez ERDS, wybierając odpowiednie techniki kryptograficzne w zakresie integralności i poufności zgodne z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA [5].

4) 5.2.1.1 Informacje ogólne

— REQ-QERDS-5.2.1.1-01 QERDSP (dostawca kwalifikowanych usług rejestrowanego doręczania elektronicznego) weryfikuje z bardzo wysokim poziomem ufności tożsamość odbiorcy bezpośrednio albo poprzez poleganie na osobie trzeciej, przy użyciu jednego z następujących środków lub ich kombinacji, stosownie do potrzeb:

a) poprzez fizyczną obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej, za pomocą odpowiednich dowodów oraz procedur, zgodnie z prawem krajowym;

b) zdalnie, przy użyciu środka identyfikacji elektronicznej, który spełnia wymogi określone w art. 8 rozporządzenia (UE) nr 910/2014 [i.1] w odniesieniu do „wysokiego" poziomu bezpieczeństwa, lub za pomocą europejskiego portfela tożsamości cyfrowej;

c) za pomocą certyfikatu kwalifikowanego podpisu elektronicznego lub kwalifikowanej pieczęci elektronicznej;

d) poprzez zastosowanie innych metod identyfikacji, które zapewniają, że osoba fizyczna lub upoważniony przedstawiciel osoby prawnej mogą zostać zidentyfikowani z bardzo wysokim poziomem pewności. Jednostka oceniająca zgodność potwierdza, że taka identyfikacja odbywa się z bardzo wysokim poziomem ufności,

— REQ-QERDS-5.2.1.1-01A QERDSP weryfikuje tożsamość nadawcy za pomocą odpowiednich środków, bezpośrednio lub poprzez poleganie na stronie trzeciej, na podstawie jednej z następujących metod lub ich połączenia:

a) poprzez fizyczną obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej, za pomocą odpowiednich dowodów oraz procedur, zgodnie z prawem krajowym;

b) zdalnie za pomocą europejskiego portfela tożsamości cyfrowej lub notyfikowanego środka identyfikacji elektronicznej, który spełnia wymogi określone w art. 8 rozporządzenia (UE) nr 910/2014 [i.1] w odniesieniu do „średniego" poziomu bezpieczeństwa, pod warunkiem że został on wydany na podstawie uprzedniej fizycznej obecności osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej;

c) za pomocą certyfikatu zaawansowanego podpisu elektronicznego lub zaawansowanej pieczęci elektronicznej, pod warunkiem że certyfikat został wydany osobie fizycznej lub upoważnionemu przedstawicielowi osoby prawnej w ramach znormalizowanej polityki certyfikacji (zasady NCP) określonej w normie ETSI EN 319 411-1 [2]; lub

d) poprzez zastosowanie innych metod identyfikacji, które zapewniają, że osoba fizyczna lub upoważniony przedstawiciel osoby prawnej mogą zostać zidentyfikowani z bardzo wysokim poziomem pewności. Jednostka oceniająca zgodność potwierdza, że identyfikacja ta jest przeprowadzana z wysokim poziomem ufności,

— UWAGA Stroną trzecią weryfikującą tożsamość nadawcy i odbiorcy może być inny QERDSP, jeżeli nadawca i odbiorca są abonentami różnych QERDSP.

5) 5.2.1.2 Identyfikacja odbiorcy i przekazywanie treści użytkownika

— REQ-QERDS-5.2.1.2-03 Jeżeli identyfikacja odbiorcy opiera się na procesie wewnętrznym QERDS (kwalifikowanej usługi rejestrowanego doręczania elektronicznego), QERDSP przeprowadza cały proces w bezpiecznym i kontrolowanym środowisku.

6) 5.2.2 Przepisy dotyczące uwierzytelniania QERDS w UE

— REQ-QERDS-5.2.2-03 [WARUNKOWO] Jeżeli QERDSP wiąże środki uwierzytelnienia z tożsamością nadawcy zweryfikowaną zgodnie z pkt 5.2.1, powinien to być jeden z następujących elementów:

a) dwuskładnikowe mechanizmy uwierzytelniania;

b) europejski portfel tożsamości cyfrowej lub notyfikowany środek identyfikacji elektronicznej, który spełnia wymogi określone w art. 8 rozporządzenia (UE) nr 910/2014 [i.1] w odniesieniu do „wysokiego" lub „średniego" poziomu bezpieczeństwa;

c) wzajemne uwierzytelnianie TLS obejmujące certyfikat wydany nadawcy w ramach polityki NCP określonej w normie ETSI EN 319 411-1 [2];

d) podpis cyfrowy poparty certyfikatem wydanym w ramach polityki NCP określonej w normie ETSI EN 319 411-1 [2];

e) inne środki zapewniające uwierzytelnienie zidentyfikowanego nadawcy. Zgodność powiązania jest potwierdzana przez jednostkę oceniającą zgodność. Przykład: Może to obejmować wykorzystanie jednego z powyższych środków z lit. a), b) i d) w celu zarejestrowania certyfikatu klienta TLS (bezpieczeństwo warstwy transportowej) do automatycznego wysyłania za pośrednictwem systemu TLS lub do zarejestrowania certyfikatu pieczęci cyfrowej wykorzystywanego do pieczętowania twierdzeń w celu uwierzytelnienia w ERDS. Zastosowanie mogą mieć również inne mechanizmy, w ramach których zidentyfikowani nadawcy korzystają z delegowanych usług stron trzecich,

— REQ-QERDS-5.2.2-03A [WARUNKOWO] Jeżeli QERDSP wiąże środki uwierzytelnienia z tożsamością odbiorcy zweryfikowaną zgodnie z pkt 5.2.1, musi to być jeden z następujących środków lub ich kombinacja, pod warunkiem że środki te lub dowolna ich kombinacja zapewniają bardzo wysoki poziom pewności co do tożsamości uwierzytelnionego odbiorcy:

a) mechanizm uwierzytelniania wieloskładnikowego

b) europejski portfel tożsamości cyfrowej lub notyfikowany środek identyfikacji elektronicznej, który spełnia wymogi określone w art. 8 rozporządzenia (UE) nr 910/2014 [i.1] w odniesieniu do poziomu bezpieczeństwa „wysokiego" lub „średniego";

c) certyfikat kwalifikowanego podpisu elektronicznego lub kwalifikowanej pieczęci elektronicznej;

d) inne środki zapewniające uwierzytelnienie zidentyfikowanego odbiorcy. Zgodność powiązania jest potwierdzana przez jednostkę oceniającą zgodność. Przykład: Może to obejmować wykorzystanie jednego z powyższych środków z lit. a)–c) w celu zarejestrowania certyfikatu klienta TLS (bezpieczeństwo warstwy transportowej) do automatycznego wysyłania za pośrednictwem systemu TLS lub do zarejestrowania certyfikatu pieczęci cyfrowej wykorzystywanego do opatrywania pieczęcią twierdzeń w celu uwierzytelnienia w ERDS. Zastosowanie mogą mieć również inne mechanizmy, w ramach których zidentyfikowani nadawcy korzystają z delegowanych usług stron trzecich,

— REQ-QERDS-5.2.2-04 [WARUNKOWO] Jeżeli nadawca łączy się z QERDS poprzez bezpieczne łącze wymagające wzajemnego uwierzytelniania maszyna–maszyna między maszyną nadawcy a serwerem QERDS w oparciu o certyfikaty wydane zgodnie z polityką NCP określoną w normie ETSI EN 319 411-1 [2], wówczas po ustanowieniu takiego bezpiecznego łącza można przyjąć mechanizmy uwierzytelniania jednoskładnikowego dla drugiej fazy uwierzytelniania nadawcy, jeżeli wprowadzone procedury organizacyjne i środki bezpieczeństwa zapewniają zaufanie do uwierzytelnienia nadawcy.

7) 5.4.1 Przepisy wspólne

— REQ-ERDS-5.4.1-06 ERDS generuje i udostępnia uzasadnionym zainteresowanym stronom dowody ERDS dotyczące zdarzeń związanych z ERD (rejestrowanym doręczeniem elektronicznym), jak określono w pkt 6 normy ETSI EN 319 522-1 [3],

— REQ-ERDS-5.4.1-07 ERDSP archiwizuje dowody lub skróty dowodów dla każdego wydanego dowodu,

— REQ-ERDS-5.4.1-08 Dowody ERDS wygenerowane przez ERDS muszą być zgodne z semantyką dowodów określoną w pkt 8 normy ETSI EN 319 522-2 [4].

8) 7.2.1 Przepisy wspólne

— REQ-ERDS-7.2.1-02 Personel ERDSP 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-ERDS-7.2.1-03 Zgodność z REQ-ERDS-7.2.1-02 obejmuje regularne aktualizacje (co najmniej raz na 12 miesięcy) dotyczące nowych zagrożeń i obecnych praktyk w zakresie bezpieczeństwa.

9) 7.3.2 Obsługa mediów

— REQ-ERDS-7.3.1-02 Stosuje się wszystkie wymogi ETSI EN 319 401 [1], pkt 7.3.3.

10) 7.5 Kontrole kryptograficzne

— REQ-ERDS-7.5-01A ERDS wybiera i stosuje odpowiednie techniki kryptograficzne spełniające wymogi określone w uzgodnionych mechanizmach kryptograficznych zatwierdzonych przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanych przez ENISA [5],

— REQ-ERDSP-7.5-03 Klucz prywatny podpisu ERDS 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 [6] 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) [7][8] i certyfikowanym zgodnie z EAL na poziomie 4 lub wyższym; lub

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

11) 7.8 Bezpieczeństwo sieci

— REQ-ERDSP-7.8-04 ERDSP stosuje najnowocześniejsze protokoły i algorytmy szyfrowania na poziomie warstwy transportowej zgodnie z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA [5],

— REQ-ERDSP-7.8-06 Wymagany w pkt REQ-7.8-13 ETSI EN 319 401 [1] skan podatności przeprowadza się co najmniej raz na kwartał,

— REQ-ERDSP-7.8-07 Wymagany w pkt REQ-7.8-17X ETSI EN 319 401 [1] test penetracyjny przeprowadza się co najmniej raz w roku,

— REQ-ERDSP-7.8-08 Zapory sieciowe należy skonfigurować tak, aby uniemożliwić wszelkie protokoły i dostępy, które nie są wymagane do funkcjonowania dostawcy usług zaufania.

12) 7.12 Zakończenie działalności ERDSP i plany zakończenia ERDS

— REQ-ERDS-7.12-03 Plan zakończenia działalności ERDSP musi spełniać wymogi określone w aktach wykonawczych przyjętych na podstawie art. 24 ust. 5 rozporządzenia (UE) nr 910/2014 [i.1].

13) 7.14 Łańcuch dostaw

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

ZAŁĄCZNIK II

Wykaz norm referencyjnych, o których mowa w art. 2

Zastosowanie mają normy ETSI EN 319 522-1 V1.2.1 (2024-01) („ETSI EN 319 522-1”), ETSI EN 319 522-2 V1.2.1 (2024-01) („ETSI EN 319 522-2”), ETSI EN 319 522-3 V1.2.1 (2024-01) („ETSI EN 319 522-3”), ETSI EN 319 522-4-1 V1.2.1 (2019-01) („ETSI EN 319 522-4-1”), ETSI EN 319 522-4-2 V1.1.1 (2018-09) („ETSI EN 319 522-4-2”) i ETSI EN 319 522-4-3 V1.1.1 (2018-09) („ETSI EN 319 522-4-3”).