Úradný vestník
Európskej únie

SK
Séria L

2025/1944

30.9.2025

VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2025/1944

z 29. septembra 2025,

ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o referenčné normy pre procesy odosielania a doručovania údajov v kvalifikovaných elektronických doručovacích službách pre registrované zásielky a pokiaľ ide o interoperabilitu týchto služieb

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES ([1]), a najmä na jeho článok 44 ods. 2 a článok 44 ods. 2b,

keďže:

(1) Kvalifikované elektronické doručovacie služby pre registrované zásielky poskytujú bezpečný kanál na prenos dokumentov vrátane potvrdenia o odoslaní a doručení údajov. Ich cieľom je poskytnúť istotu pri identifikácii adresáta a zabezpečiť vysokú úroveň spoľahlivosti pri identifikácii odosielateľa.

(2) Domnienka súladu s požiadavkami stanovená v článku 44 ods. 1a nariadenia (EÚ) č. 910/2014 by sa mala uplatňovať len vtedy, ak kvalifikované dôveryhodné služby na poskytovanie kvalifikovaných elektronických doručovacích služieb pre registrované zásielky spĺňajú normy stanovené v tomto nariadení. Tieto normy by mali odrážať zavedené postupy a mali by byť všeobecne uznávané v príslušných odvetviach. Mali by sa upraviť tak, aby zahŕňali dodatočné kontroly, ktoré zaistia bezpečnosť a dôveryhodnosť kvalifikovanej dôveryhodnej služby.

(3) Ak poskytovateľ dôveryhodných služieb dodržiava požiadavky stanovené v prílohe I k tomuto nariadeniu, orgány dohľadu by mali predpokladať súlad s príslušnými požiadavkami nariadenia (EÚ) č. 910/2014 a náležite zvážiť takúto domnienku pri udeľovaní alebo potvrdzovaní kvalifikovaného štatútu dôveryhodnej služby. Kvalifikovaný poskytovateľ dôveryhodnej služby však môže pri preukazovaní súladu s požiadavkami nariadenia (EÚ) č. 910/2014 stále využívať aj iné postupy.

(4) Podľa článku 44 ods. 2a nariadenia (EÚ) č. 910/2014, ak sa kvalifikovaní poskytovatelia dôveryhodných služieb dohodnú, že ich služby budú interoperabilné, je dôležité, aby dodržiavali príslušné normy a špecifikácie stanovené v prílohe II k tomuto vykonávaciemu nariadeniu s cieľom ľahko prenášať elektronické registrované údaje medzi dvoma alebo viacerými kvalifikovanými poskytovateľmi dôveryhodných služieb a podporovať spravodlivé postupy na vnútornom trhu.

(5) Komisia pravidelne posudzuje nové technológie, postupy, normy alebo technické špecifikácie. V súlade s odôvodnením 75 nariadenia Európskeho parlamentu a Rady (EÚ) 2024/1183 ([2]) by Komisia mala toto nariadenie podľa potreby preskúmať a aktualizovať, aby bolo v súlade s globálnym vývojom, novými technológiami, normami alebo technickými špecifikáciami a aby sa na vnútornom trhu dodržiavali najlepšie postupy.

([1]) Ú. v. EÚ L 257, 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1183 z 11. apríla 2024, ktorým sa mení nariadenie (EÚ) č. 910/2014, pokiaľ ide o zriadenie európskeho rámca digitálnej identity (Ú. v. EÚ L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(6) Na všetky činnosti spracúvania osobných údajov podľa tohto nariadenia sa vzťahuje nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 ([3]) a v relevantných prípadoch smernica Európskeho parlamentu a Rady 2002/58/ES ([4]).

(7) V súlade s článkom 42 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725 ([5]) sa konzultovalo s európskym dozorným úradníkom pre ochranu údajov, ktorý vydal 6. júna 2025 svoje stanovisko.

(8) Opatrenia stanovené v tomto nariadení sú v súlade so stanoviskom výboru uvedeného v článku 48 nariadenia (EÚ) č. 910/2014,

PRIJALA TOTO NARIADENIE:

Článok 1

Referenčné normy a špecifikácie pre kvalifikované elektronické doručovacie služby pre registrované zásielky

Referenčné normy a špecifikácie uvedené v článku 44 ods. 2 nariadenia (EÚ) č. 910/2014 sú stanovené v prílohe I k tomuto nariadeniu.

Článok 2

Referenčné normy a špecifikácie pre interoperabilitu medzi kvalifikovanými elektronickými doručovacími službami pre registrované zásielky

Referenčné normy a špecifikácie uvedené v článku 44 ods. 2b nariadenia (EÚ) č. 910/2014 sú stanovené v prílohe II k tomuto nariadeniu.

Článok 3

Nadobudnutie účinnosti

Toto nariadenie nadobúda účinnosť dvadsiatym dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 29. septembra 2025

Za Komisiu
predsedníčka
Ursula VON DER LEYEN

([3]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

PRÍLOHA I

Zoznam referenčných noriem a špecifikácií uvedených v článku 1

Uplatňuje sa norma ETSI EN 319 521 V1.1.1 (2019-02) (ďalej len „ETSI EN 319 521“) s týmito úpravami:

1. Pokiaľ ide o normu ETSI EN 319 521:

    1. 2.1. Normatívne odkazy:

        — [1] ETSI EN 319 401 V3.1.1 (2024-06) „Elektronické podpisy a infraštruktúry (ESI); všeobecné požiadavky týkajúce sa politiky pre poskytovateľov dôveryhodných služieb“,

        — [2] ETSI EN 319 411-1 V1.5.1 (2025-04) „Elektronické podpisy a infraštruktúry (ESI); požiadavky týkajúce sa politiky a bezpečnosti pre poskytovateľov dôveryhodných služieb vydávajúcich certifikáty; časť 1: všeobecné požiadavky“,

        — [3] ETSI EN 319 522-1 V1.2.1 (2024-01) „Elektronické podpisy a infraštruktúry (ESI); elektronické doručovacie služby pre registrované zásielky; časť 1: rámec a architektúra“,

        — [4] ETSI EN 319 522-2 V1.2.1 (2024-01) „Elektronické podpisy a infraštruktúry (ESI); elektronické doručovacie služby pre registrované zásielky; časť 2: sémantický obsah“,

        — [5] európska skupina pre certifikáciu kybernetickej bezpečnosti, podskupina pre kryptografiu: *Agreed Cryptographic Mechanisms* (Dohodnuté kryptografické mechanizmy), uverejnené Agentúrou Európskej únie pre kybernetickú bezpečnosť (ENISA) ([1]),

        — [6] ISO/IEC 15408-1:2022 – Bezpečnosť informácií, kybernetická bezpečnosť a ochrana súkromia – kritériá na hodnotenie bezpečnosti IT,

        — [7] vykonávacie nariadenie Komisie (EÚ) 2024/482 ([2]), ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881, pokiaľ ide o prijatie európskej schémy certifikácie kybernetickej bezpečnosti založenej na spoločných kritériách (EUCC),

        — [8] vykonávacie nariadenie Komisie (EÚ) 2024/3144 ([3]), ktorým sa mení vykonávacie nariadenie (EÚ) 2024/482, pokiaľ ide o uplatniteľné medzinárodné normy, a ktorým sa opravuje uvedené vykonávacie nariadenie,

        — [9] FIPS PUB 140-3 (2019) „Bezpečnostné požiadavky na kryptografické moduly“.

    2. 3.1. Termíny

        — zdokonalená elektronická pečať: v zmysle nariadenia (EÚ) č. 910/2014 [i.1],

        — zdokonalený elektronický podpis: v zmysle nariadenia (EÚ) č. 910/2014 [i.1],

        — kvalifikovaná elektronická pečať: v zmysle nariadenia (EÚ) č. 910/2014 [i.1],

        — kvalifikovaný elektronický podpis: v zmysle nariadenia (EÚ) č. 910/2014 [i.1],

        — zabezpečené kryptografické zariadenie: zariadenie, v ktorom sa uchováva súkromný kľúč používateľa, ktoré tento kľúč chráni pred kompromitáciou a ktoré vykonáva funkcie podpisovania alebo dešifrovania v mene používateľa.

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

3. 5.1.1. Spoločné ustanovenia

— REQ-ERDS-5.1.1-01 Elektronická doručovacia služba pre registrované zásielky (ďalej len „ERDS“) zabezpečuje, aby boli dostupnosť, integrita a dôvernosť používateľského obsahu primerane zaručené v čase, keď s ním ERDS nakladá, pričom sú zvolené vhodné kryptografické techniky na zachovanie integrity a dôvernosti, ktoré sú v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [5].

4. 5.2.1.1. Všeobecné

— REQ-QERDS-5.2.1.1-01 Poskytovateľ kvalifikovaných elektronických doručovacích služieb pre registrované zásielky (ďalej len „QERDSP“) overí s veľmi vysokou úrovňou spoľahlivosti totožnosť príjemcu, a to buď priamo, alebo s využitím tretej strany, pričom podľa potreby používa jeden z týchto prostriedkov alebo ich kombináciu:

a) fyzická prítomnosť fyzickej osoby alebo splnomocneného zástupcu právnickej osoby prostredníctvom vhodnej evidencie a postupov v súlade s vnútroštátnym právom;

b) na diaľku použitím prostriedku elektronickej identifikácie, ktorý spĺňa požiadavky stanovené v článku 8 nariadenia (EÚ) č. 910/2014 [i.1], pokiaľ ide o úroveň zabezpečenia „vysoká“, alebo s použitím európskej peňaženky digitálnej identity;

c) certifikát kvalifikovaného elektronického podpisu alebo kvalifikovanej elektronickej pečate;

d) iné metódy identifikácie, ktorými sa zabezpečuje, že fyzickú osobu alebo splnomocneného zástupcu právnickej osoby možno identifikovať s veľmi vysokou úrovňou spoľahlivosti. Zabezpečenie, že táto identifikácia sa vykonáva s veľmi vysokou úrovňou spoľahlivosti, potvrdí orgán posudzovania zhody.

— REQ-QERDS-5.2.1.1-01A QERDSP overí totožnosť odosielateľa vhodnými prostriedkami, a to buď priamo, alebo s využitím tretej strany, a to na základe jednej z týchto metód alebo ich kombinácie:

a) fyzická prítomnosť fyzickej osoby alebo splnomocneného zástupcu právnickej osoby prostredníctvom vhodnej evidencie a postupov v súlade s vnútroštátnym právom;

b) na diaľku s použitím európskej peňaženky digitálnej identity alebo oznámeného prostriedku elektronickej identifikácie, ktorý spĺňa požiadavky stanovené v článku 8 nariadenia (EÚ) č. 910/2014 [i.1], pokiaľ ide o úroveň zabezpečenia „pokročilá“, za predpokladu, že boli vydané na základe predchádzajúcej fyzickej prítomnosti fyzickej osoby alebo splnomocneného zástupcu právnickej osoby;

c) certifikát zdokonaleného elektronického podpisu alebo zdokonalenej elektronickej pečate za predpokladu, že certifikát bol vydaný fyzickej osobe alebo splnomocnenému zástupcovi právnickej osoby podľa normalizovanej politiky v oblasti certifikátov (ďalej len „NCP“) v zmysle normy ETSI EN 319 411-1 [2], alebo

d) iné metódy identifikácie, ktorými sa zabezpečuje, že fyzickú osobu alebo splnomocneného zástupcu právnickej osoby možno identifikovať s veľmi vysokou úrovňou spoľahlivosti. Zabezpečenie, že táto identifikácia sa vykonáva s vysokou úrovňou spoľahlivosti, potvrdí orgán posudzovania zhody.

— POZNÁMKA: Tretia strana overujúca totožnosť odosielateľa a príjemcu môže byť ďalší QERDSP, ak sú odosielateľ a príjemca účastníkmi u odlišných QERDSP.

5. 5.2.1.2. Identifikácia príjemcu a odovzdanie používateľského obsahu

— REQ-QERDS-5.2.1.2-03 Ak je identifikácia príjemcu založená na internom procese kvalifikovanej elektronickej doručovacej služby pre registrované zásielky (ďalej len „QERDS“), QERDSP vykoná celý proces v zabezpečenom a kontrolovanom prostredí.

6. 5.2.2. Ustanovenia o autentifikácii QERDS EÚ

— REQ-QERDS-5.2.2-03 [PODMIENEČNÉ] Ak QERDSP viaže prostriedky autentifikácie na totožnosť odosielateľa overenú podľa bodu 5.2.1, ide o jeden z týchto prostriedkov:

a) mechanizmy dvojfaktorovej autentifikácie;

b) európska peňaženka digitálnej identity alebo oznámený prostriedok elektronickej identifikácie, ktorý spĺňa požiadavky stanovené v článku 8 nariadenia (EÚ) č. 910/2014 [i.1], pokiaľ ide o úroveň zabezpečenia „vysoká“ alebo „pokročilá“;

c) vzájomná autentifikácia prostredníctvom protokolu Transport Layer Security (TLS), ktorá zahŕňa certifikát vydaný odosielateľovi podľa NCP v zmysle normy ETSI EN 319 411-1 [2];

d) digitálny podpis podporovaný certifikátom vydaným podľa NCP v zmysle normy ETSI EN 319 411-1 [2];

e) iné prostriedky, ktoré zabezpečujú autentifikáciu identifikovaného odosielateľa. Zhodu väzby s požiadavkami potvrdí orgán posudzovania zhody. Príklad: Môže to zahŕňať použitie jedného z prostriedkov uvedených v písmenách a), b) a d) na registráciu klientskeho certifikátu protokolu TLS na automatické odosielanie prostredníctvom vzájomného TLS alebo na registráciu certifikátu digitálnej pečate, ktorý sa používa na zapečatenie tvrdení na autentifikáciu v ERDS. Môžu sa uplatňovať aj iné mechanizmy, pri ktorých identifikovaní odosielatelia využívajú delegované služby tretích strán.

— REQ-QERDS-5.2.2-03A [PODMIENEČNÉ] Ak QERDSP viaže prostriedky autentifikácie na totožnosť príjemcu overenú podľa bodu 5.2.1, ide o jeden z týchto prostriedkov za predpokladu, že daný prostriedok alebo akákoľvek kombinácia prostriedkov zabezpečujú veľmi vysokú úroveň spoľahlivosti, pokiaľ ide o totožnosť autentifikovaného príjemcu:

a) mechanizmus viacfaktorovej autentifikácie;

b) európska peňaženka digitálnej identity alebo oznámený prostriedok elektronickej identifikácie, ktorý spĺňa požiadavky stanovené v článku 8 nariadenia (EÚ) č. 910/2014 [i.1], pokiaľ ide o úroveň zabezpečenia „vysoká“ alebo „pokročilá“;

c) certifikát kvalifikovaného elektronického podpisu alebo kvalifikovanej elektronickej pečate;

d) iné prostriedky, ktoré zabezpečujú autentifikáciu identifikovaného príjemcu. Zhodu väzby s požiadavkami potvrdí orgán posudzovania zhody. Príklad: Môže to zahŕňať použitie jedného z prostriedkov uvedených v písmenách a) až c) na registráciu klientskeho certifikátu protokolu TLS na automatické odosielanie prostredníctvom vzájomného TLS alebo na registráciu certifikátu digitálnej pečate, ktorý sa používa na zapečatenie tvrdení na autentifikáciu v ERDS. Môžu sa uplatňovať aj iné mechanizmy, pri ktorých identifikovaní odosielatelia využívajú delegované služby tretích strán.

— REQ-QERDS-5.2.2-04 [PODMIENEČNÉ] Ak sa odosielateľ pripojí ku QERDS prostredníctvom zabezpečeného pripojenia, ktoré si vyžaduje vzájomnú autentifikáciu stroj-stroj medzi strojom odosielateľa a serverom QERDS na základe certifikátov vydaných podľa NCP v zmysle normy ETSI EN 319 411-1 [2], potom sa po vytvorení tohto zabezpečeného pripojenia pre druhú fázu autentifikácie odosielateľa môžu prijať mechanizmy jednofaktorovej autentifikácie, ak zavedené organizačné postupy a bezpečnostné opatrenia zabezpečujú dôveru v autentifikáciu odosielateľa.

7. 5.4.1. Spoločné ustanovenia

— REQ-ERDS-5.4.1-06 ERDS generuje a sprístupňuje oprávneným zainteresovaným stranám evidenciu ERDS o udalostiach elektronického doručovania registrovaných zásielok (ERD) v zmysle bodu 6 normy ETSI EN 319 522-1 [3].

— REQ-ERDS-5.4.1-07 Poskytovateľ elektronických doručovacích služieb pre registrované zásielky (ďalej len „ERDSP“) archivuje evidenciu a/alebo odtlačok evidencie pre každú evidenciu, ktorú vydal.

— REQ-ERDS-5.4.1-08 Evidencia ERDS vygenerovaná ERDS sú v súlade so sémantikou evidencie vymedzenou v bode 8 normy ETSI EN 319 522-2 [4].

8. 7.2.1. Spoločné ustanovenia

— REQ-ERDS-7.2.1-02 Personál ERDSP v dôveryhodných rolách a prípadne jeho subdodávatelia v dôveryhodných rolách sú schopní splniť požiadavku na „odborné znalosti, skúsenosti a kvalifikáciu“ na základe formálnej odbornej prípravy a poverení alebo reálnych skúseností, alebo kombinácie oboch možností.

— REQ-ERDS-7.2.1-03 Splnenie požiadavky REQ-ERDS-7.2.1-02 zahŕňa pravidelné aktuálne informácie (aspoň každých 12 mesiacov) o nových hrozbách a súčasných bezpečnostných postupoch.

9. 7.3.2. Nakladanie s médiami

— REQ-ERDS-7.3.1-02 Uplatňujú sa všetky požiadavky stanovené v bode 7.3.3 normy ETSI EN 319 401 [1].

10. 7.5. Kryptografické kontroly

— REQ-ERDS-7.5-01A ERDS vyberá a používa vhodné kryptografické techniky v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [5].

— REQ-ERDSP-7.5-03 Podpisový súkromný kľúč ERDS sa uschováva a používa v rámci zabezpečeného kryptografického zariadenia, ktoré je dôveryhodným systémom certifikovaným v súlade:

a) so spoločnými kritériami hodnotenia bezpečnosti informačných technológií, ako sa stanovuje v norme ISO/IEC 15408 [6] alebo v časti 1 až 5 spoločných kritérií hodnotenia bezpečnosti informačných technológií, verzii CC:2002, ktoré uverejnili účastníci dohody o uznávaní certifikátov spoločných kritérií v oblasti hodnotenia bezpečnosti informačných technológií, a certifikovaným na úrovni EAL 4 alebo vyššej alebo

b) s európskou schémou certifikácie kybernetickej bezpečnosti založenou na spoločných kritériách (EUCC) [7][8] a certifikovaným na úrovni EAL 4 alebo vyššej, alebo

c) do 31. 12. 2030 s normou FIPS PUB 140-3 [9] na úrovni 3.

Táto certifikácia zodpovedá bezpečnostnému cieľu alebo profilu ochrany, alebo koncepcii modulu a bezpečnostnej dokumentácii, ktorá spĺňa požiadavky tohto dokumentu, a to na základe analýzy rizík a s prihliadnutím na fyzické a iné netechnické bezpečnostné opatrenia.

Ak má zabezpečené kryptografické zariadenie certifikáciu EUCC [7][8], potom sa toto zariadenie nakonfiguruje a používa v súlade s uvedenou certifikáciou.

11. 7.8. Bezpečnosť siete

— REQ-ERDSP-7.8-04 ERDSP používa najmodernejšie protokoly a algoritmy na šifrovanie na úrovni transportnej vrstvy v súlade s dohodnutými kryptografickými mechanizmami schválenými európskou skupinou pre certifikáciu kybernetickej bezpečnosti a uverejnenými agentúrou ENISA [5].

— REQ-ERDSP-7.8-06 Skenovanie zraniteľnosti požadované v rámci požiadavky REQ-7.8-13 normy ETSI EN 319 401 [1] sa vykonáva aspoň raz za štvrťrok.

— REQ-ERDSP-7.8-07 Penetračný test požadovaný v rámci požiadavky REQ-7.8-17X normy ETSI EN 319 401 [1] sa vykonáva aspoň raz za rok.

— REQ-ERDSP-7.8-08 Firewally sú konfigurované tak, aby sa zabránilo všetkým protokolom a prístupom, ktoré nie sú potrebné na prevádzku poskytovateľa dôveryhodných služieb (TSP).

12. 7.12. Ukončenie činnosti ERDSP a plány ukončenia činnosti ERDS

— REQ-ERDS-7.12-03 Plán ukončenia činnosti ERDSP spĺňa požiadavky stanovené vo vykonávacích aktoch prijatých podľa článku 24 ods. 5 nariadenia (EÚ) č. 910/2014 [i.1].

13. 7.14. Dodávateľský reťazec

— REQ-ERDS-7.14-01 Uplatňujú sa požiadavky stanovené v bode 7.14 normy ETSI EN 319 401 [1].

PRÍLOHA II

Zoznam referenčných noriem a špecifikácií uvedených v článku 2

Uplatňujú sa normy ETSI EN 319 522-1 V1.2.1 (2024-01) (ďalej len „ETSI EN 319 522-1“), ETSI EN 319 522-2 V1.2.1 (2024-01) (ďalej len „ETSI EN 319 522-2“), ETSI EN 319 522-3 V1.2.1 (2024-01) (ďalej len „ETSI EN 319 522-3“), ETSI EN 319 522-4-1 V1.2.1 (2019-01) (ďalej len „ETSI EN 319 522-4-1“), ETSI EN 319 522-4-2 V1.1.1 (2018-09) (ďalej len „ETSI EN 319 522-4-2“) a ETSI EN 319 522-4-3 V1.1.1 (2018-09) (ďalej len „ETSI EN 319 522-4-3“).