2025/1944

2025.9.30.

A BIZOTTSÁG (EU) 2025/1944 VÉGREHAJTÁSI RENDELETE

(2025. szeptember 29.)

a 910/2014/EU európai parlamenti és tanácsi rendeletnek a minősített ajánlott elektronikus kézbesítési szolgáltatások keretében történő adatküldés és adatfogadás folyamatára vonatkozó referenciaszabványok tekintetében, valamint az említett szolgáltatások interoperabilitása tekintetében történő alkalmazására vonatkozó szabályok megállapításáról

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről szóló, 2014. július 23-i 910/2014/EU európai parlamenti és tanácsi rendeletre ([1]) és különösen annak 44. cikke (2) bekezdésére és 44. cikke (2b) bekezdésére,

mivel:

(1) A minősített ajánlott elektronikus kézbesítési szolgáltatások biztonságos csatornát jelentenek a dokumentumok továbbítására, beleértve az adatok küldésének és fogadásának igazolását is. Céljuk, hogy bizonyosságot nyújtsanak a fogadó fél azonosításához, és lehetővé tegyék azt, hogy nagy biztonsággal lehessen azonosítani a küldő felet.

(2) A 910/2014/EU rendelet 44. cikkének (1a) bekezdésében meghatározott megfelelési vélelem csak akkor alkalmazandó, ha a minősített ajánlott elektronikus kézbesítési szolgáltatások nyújtására vonatkozó minősített bizalmi szolgáltatások megfelelnek az e rendeletben meghatározott szabványoknak. E szabványoknak tükrözniük kell a bevett gyakorlatokat, és széles körben elismertnek kell lenniük az érintett ágazatokban. A szóban forgó szabványokat ki kell igazítani oly módon, hogy magukban foglaljanak a minősített bizalmi szolgáltatás biztonságát és megbízhatóságát garantáló további ellenőrzéseket.

(3) Ha a bizalmi szolgáltató megfelel az e rendelet I. mellékletében meghatározott követelményeknek, a felügyeleti szerveknek vélelmezniük kell a 910/2014/EU rendelet vonatkozó követelményeinek való megfelelést, és ezt a vélelmet kellőképpen figyelembe kell venniük a bizalmi szolgáltatás minősített státuszának megadása vagy megerősítése során. A minősített bizalmi szolgáltatók azonban továbbra is alkalmazhatnak más gyakorlatot a 910/2014/EU rendelet követelményeinek való megfelelés igazolásához.

(4) A 910/2014/EU rendelet 44. cikkének (2a) bekezdése értelmében, amennyiben a minősített bizalmi szolgáltatók megállapodnak abban, hogy szolgáltatásaikat interoperábilissá teszik, fontos, hogy megfeleljenek az e végrehajtási rendelet II. mellékletében meghatározott megfelelő szabványoknak és specifikációknak annak érdekében, hogy az elektronikusan nyilvántartott adatokat könnyen továbbíthassák két vagy több minősített bizalmi szolgáltató között, és előmozdítsák a belső piaci tisztességes gyakorlatot.

(5) A Bizottság rendszeresen értékel új technológiákat, gyakorlatokat, szabványokat és technikai specifikációkat. Az (EU) 2024/1183 európai parlamenti és tanácsi rendelet ([2]) (75) preambulumbekezdése értelmében a Bizottságnak rendszeresen felül kell vizsgálnia, és szükség esetén aktualizálnia kell ezt a rendeletet, hogy az folyamatosan megfeleljen a globális fejleményeknek, az új technológiáknak, a szabványoknak és a technikai specifikációknak, illetve igazodjon a belső piaci bevált gyakorlatokhoz.

([1]) HL L 257., 2014.8.28., 73. o., ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Az Európai Parlament és a Tanács (EU) 2024/1183 rendelete (2024. április 11.) a 910/2014/EU rendeletnek az európai digitális személyazonossági keret létrehozása tekintetében történő módosításáról (HL L, 2024/1183, 2024.4.30., ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(6) Az (EU) 2016/679 európai parlamenti és tanácsi rendelet ([3]) és adott esetben a 2002/58/EK európai parlamenti és tanácsi irányelv ([4]) az e rendelet szerinti valamennyi személyesadat-kezelési tevékenységre alkalmazandó.

(7) Az (EU) 2018/1725 európai parlamenti és tanácsi rendelet ([5]) 42. cikkének (1) bekezdésével összhangban konzultációra került sor az európai adatvédelmi biztossal, aki 2025. június 6-án véleményt nyilvánított.

(8) Az e rendeletben előírt intézkedések összhangban vannak a 910/2014/EU rendelet 48. cikkével létrehozott bizottság véleményével,

ELFOGADTA EZT A RENDELETET:

1. cikk

A minősített ajánlott elektronikus kézbesítési szolgáltatásokra vonatkozó referenciaszabványok és specifikációk

A 910/2014/EU rendelet 44. cikkének (2) bekezdésében említett referenciaszabványokat és specifikációkat e rendelet I. melléklete tartalmazza.

2. cikk

A minősített ajánlott elektronikus kézbesítési szolgáltatások közötti interoperabilitásra vonatkozó referenciaszabványok és specifikációk

A 910/2014/EU rendelet 44. cikkének (2b) bekezdésében említett referenciaszabványokat és specifikációkat e rendelet II. melléklete tartalmazza.

3. cikk

Hatálybalépés

Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.

Kelt Brüsszelben, 2025. szeptember 29-én.

a Bizottság részéről
az elnök
Ursula VON DER LEYEN

([3]) Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o., ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv) (HL L 201., 2002.7.31., 37. o., ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről (HL L 295., 2018.11.21., 39. o., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

I. MELLÉKLET

Az 1. cikkben említett referenciaszabványok és specifikációk jegyzéke

Az ETSI EN 319 521 V1.1.1 (2019-02) (a továbbiakban: ETSI EN 319 521) szabvány alkalmazandó, a következő kiigazításokkal:

1. Az ETSI EN 319 521 esetében

1. 2.1. Normatív hivatkozások:

— [1] ETSI EN 319 401 V3.1.1 (2024-06) „Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers" (Elektronikus aláírások és infrastruktúrák (ESI). Bizalmi szolgáltatókra vonatkozó általános szabályzati rend követelményei)

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements" (Elektronikus aláírások és bizalmi infrastruktúrák (ESI). Tanúsítványokat kibocsátó bizalmi szolgáltatókra vonatkozó szabályzati rend és biztonsági követelmények. 1. rész: Általános követelmények)

— [3] ETSI EN 319 522-1 V1.2.1 (2024-01) „Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture" (Elektronikus aláírások és infrastruktúrák (ESI). Ajánlott elektronikus kézbesítési szolgáltatások. 1. rész: Keretrendszer és architektúra)

— [4] ETSI EN 319 522-2 V1.2.1 (2024-01) „Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic content" (Elektronikus aláírások és infrastruktúrák (ESI). Ajánlott elektronikus kézbesítési szolgáltatások. 2. rész: Szemantikus tartalmak)

— [5] Európai kiberbiztonsági tanúsítási csoport, kriptográfiai alcsoport: „Agreed Cryptographic Mechanisms" (elfogadott kriptográfiai mechanizmusok), az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) kiadványa ([1])

— [6] ISO/IEC 15408-1:2022 – „Information security, cybersecurity and privacy protection – Evaluation criteria for IT security" (Információbiztonság, kiberbiztonság és a magánélet védelme. Az informatikai biztonságértékelés kritériumai)

— [7] A Bizottság (EU) 2024/482 végrehajtási rendelete ([2]) a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC) elfogadása tekintetében az (EU) 2019/881 európai parlamenti és tanácsi rendelet alkalmazására vonatkozó szabályok megállapításáról ([3])

— [8] A Bizottság (EU) 2024/3144 végrehajtási rendelete az (EU) 2024/482 végrehajtási rendeletnek az alkalmazandó nemzetközi szabványok tekintetében történő módosításáról és az említett végrehajtási rendelet helyesbítéséről

— [9] FIPS PUB 140-3 (2019) „Security Requirements for Cryptographic Modules" (Kriptográfiai modulok biztonsági követelményei)

2. 3.1. Fogalommeghatározások

— fokozott biztonságú elektronikus bélyegző: a 910/2014/EU rendelet [i.1] meghatározásának megfelelően

— fokozott biztonságú elektronikus aláírás: a 910/2014/EU rendelet [i.1] meghatározásának megfelelően

— minősített elektronikus bélyegző: a 910/2014/EU rendelet [i.1] meghatározásának megfelelően

— minősített elektronikus aláírás: a 910/2014/EU rendelet [i.1] meghatározásának megfelelően

— biztonságos kriptográfiai eszköz: a felhasználó személyes kulcsát tároló eszköz, amely megvédi az említett kulcsot a sérüléstől, és a felhasználó nevében aláírási vagy dekódolási funkciókat lát el

([1]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([2]) HL L, 2024/3144, 2024.12.19., ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.
([3]) HL L, 2024/482, 2024.2.7., ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.

3. 5.1.1. Közös rendelkezések

— REQ-ERDS-5.1.1-01 Az ajánlott elektronikus kézbesítési szolgáltatás (ERDS) az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusoknak [5] megfelelő, az integritás és a bizalmas jelleg megőrzésére alkalmas kriptográfiai technikákat kiválasztva gondoskodik arról, hogy a felhasználói tartalom rendelkezésre állása, integritása és bizalmas jellege az ERDS általi kezelés során kellően garantált legyen

4. 5.2.1.1. Általános rendelkezések

— REQ-QERDS-5.2.1.1-01 A minősített ajánlott elektronikus kézbesítési szolgáltató (QERDSP) nagyon nagy megbízhatósággal – akár közvetlenül, akár harmadik fél igénybevételével –, szükség szerint az alábbi eszközök egyikének vagy azok kombinációjának alkalmazásával ellenőrzi a fogadó fél személyazonosságát:

a) a természetes személynek vagy a jogi személy meghatalmazott képviselőjének a személyes jelenléte útján, megfelelő bizonyítékok és eljárások révén, a nemzeti joggal összhangban;

b) távolról, olyan elektronikus azonosító eszközzel, amely megfelel a 910/2014/EU rendelet [i.1] 8. cikkében a „magas” biztonsági szint tekintetében meghatározott követelményeknek, vagy az európai digitális személyiadat-tárca révén;

c) minősített elektronikus aláírás vagy minősített elektronikus bélyegző tanúsítványával;

d) olyan egyéb azonosítási módszerek alkalmazásával, amelyek biztosítják, hogy a természetes személy vagy a jogi személy meghatalmazott képviselője nagyon nagy megbízhatósággal azonosítható legyen. Az azonosítás kiemelten magas megbízhatósági szintjét megfelelőségértékelő szervezet igazolja

— REQ-QERDS-5.2.1.1-01 A QERDSP megfelelő eszközökkel – akár közvetlenül, akár harmadik fél igénybevételével –, az alábbi módszerek egyikének vagy azok kombinációjának alapján ellenőrzi a küldő fél személyazonosságát:

a) a természetes személynek vagy a jogi személy meghatalmazott képviselőjének a személyes jelenléte útján, megfelelő bizonyítékok és eljárások révén, a nemzeti joggal összhangban;

b) távolról, az európai digitális személyiadat-tárca segítségével vagy a 910/2014/EU rendelet [i.1] 8. cikkében a „jelentős” biztonsági szint tekintetében meghatározott követelményeknek megfelelő bejelentett elektronikus azonosító eszköz révén, feltéve, hogy azt a természetes személynek vagy a jogi személy meghatalmazott képviselőjének az előzetes fizikai jelenléte alapján bocsátották ki;

c) fokozott biztonságú elektronikus aláírásra vagy fokozott biztonságú elektronikus bélyegzőre vonatkozó tanúsítvány révén, feltéve, hogy a tanúsítványt a természetes személy vagy a jogi személy meghatalmazott képviselője részére az ETSI EN 319 411-1 szabványban [2] meghatározott normalizált hitelesítési rend (NCP) alapján bocsátották ki; vagy

d) olyan egyéb azonosítási módszerek alkalmazásával, amelyek biztosítják, hogy a természetes személy vagy a jogi személy meghatalmazott képviselője nagyon nagy megbízhatósággal azonosítható legyen. Az azonosítás magas megbízhatósági szintjét megfelelőségértékelő szervezet igazolja

— MEGJEGYZÉS A küldő és a fogadó fél személyazonosságát ellenőrző harmadik fél lehet másik QERDSP, ha a küldő és a fogadó fél különböző QERDSP előfizetője

5. 5.2.1.2. A fogadó fél azonosítása és a felhasználói tartalom átadása

— REQ-QERDS-5.2.1.2-03 Ha a fogadó fél azonosítása minősített ajánlott elektronikus kézbesítési szolgáltatás (QERDS) belső folyamatán alapul, a QERDSP a teljes folyamatot biztonságos és ellenőrzött környezetben hajtja végre

6. 5.2.2. Az uniós QERDS hitelesítésére vonatkozó rendelkezések

— REQ-QERDS-5.2.2-03 [FELTÉTELES] Amennyiben a QERDSP a küldő félnek az 5.2.1. szakasz szerint ellenőrzött személyazonosságához hitelesítési eszközt köt, annak a következők egyikének kell lennie:

a) kéttényezős hitelesítési mechanizmus;

b) európai digitális személyiadat-tárca vagy olyan bejelentett elektronikus azonosító eszköz, amely megfelel a 910/2014/EU rendelet [i.1] 8. cikkében a „magas” vagy a „jelentős” biztonsági szint tekintetében meghatározott követelményeknek;

c) kölcsönös TLS-hitelesítés, amely magában foglalja a küldő fél számára az ETSI EN 319 411-1 szabványban [2] meghatározott NCP alapján kibocsátott tanúsítványt;

d) az ETSI EN 319 411-1 szabványban [2] meghatározott NCP alapján kibocsátott tanúsítvánnyal alátámasztott digitális aláírás;

e) egyéb olyan eszköz, amely biztosítja az azonosított küldő fél hitelesítését. A személyazonossághoz kötés megfelelőségét megfelelőségértékelő szervezet igazolja. Például ilyen lehet a fenti a), b) és d) pont szerinti egyik eszköz használata TLS-ügyféltanúsítvány kölcsönös TLS-en keresztül történő automatikus küldéshez való nyilvántartásba vételére vagy az állításoknak az ERDS szolgáltatással való hitelesítéséhez használt digitálisbélyegző-tanúsítvány nyilvántartásba vételére. Más olyan mechanizmusok is alkalmazhatók, amelyek során az azonosított küldő felek megbízott harmadik fél szolgáltatásait veszik igénybe

— REQ-QERDS-5.2.2-03A [FELTÉTELES] Amennyiben a QERDSP a fogadó félnek az 5.2.1. szakasz szerint ellenőrzött személyazonosságához hitelesítési eszközt köt, annak a következők egyikének kell lennie – feltéve, hogy az eszköz vagy az eszközök tetszőleges kombinációja biztosítja a hitelesített fogadó fél nagyon magas megbízhatósági szintű azonosítását:

a) többtényezős hitelesítési mechanizmus;

b) európai digitális személyiadat-tárca vagy olyan bejelentett elektronikus azonosító eszköz, amely megfelel a 910/2014/EU rendelet [i.1] 8. cikkében a „magas” vagy a „jelentős” biztonsági szint tekintetében meghatározott követelményeknek;

c) minősített elektronikus aláírás vagy minősített elektronikus bélyegző tanúsítványa;

d) egyéb olyan eszköz, amely biztosítja az azonosított fogadó fél hitelesítését. A személyazonossághoz kötés megfelelőségét megfelelőségértékelő szervezet igazolja. Például ilyen lehet a fenti a) – c) pont szerinti egyik eszköz használata TLS-ügyféltanúsítvány kölcsönös TLS-en keresztül történő automatikus küldéshez való nyilvántartásba vételére vagy az állításoknak az ERDS szolgáltatással való hitelesítéséhez használt digitálisbélyegző-tanúsítvány nyilvántartásba vételére. Más olyan mechanizmusok is alkalmazhatók, amelyek során az azonosított küldő felek megbízott harmadik fél szolgáltatásait veszik igénybe

— REQ-QERDS-5.2.2-04 [FELTÉTELES] Ha a küldő fél olyan biztonságos kapcsolattal csatlakozik a QERDS szolgáltatáshoz, amely a küldő fél számítógépe és a QERDS szervere közötti, az ETSI EN 319 411-1 szabványban [2] meghatározott NCP szerint kibocsátott tanúsítványokon alapuló, gépek közötti kölcsönös hitelesítést igényel, akkor e biztonságos kapcsolat létrehozása után egytényezős hitelesítési mechanizmusok alkalmazhatók a küldő fél hitelesítésének második szakaszára, amennyiben a bevezetett szervezeti eljárások és biztonsági intézkedések biztosítják a küldő fél hitelesítésének megbízhatóságát

7. 5.4.1. Közös rendelkezések

— REQ-ERDS-5.4.1-06 Az ERDS az EN 319 522-1 szabvány [3] 6. szakaszában meghatározott ajánlott elektronikus kézbesítési (ERD-) eseményekre vonatkozó ERDS-bizonyítékokat állít elő és bocsát az arra jogosult érdekelt felek rendelkezésére

— REQ-ERDS-5.4.1-07 Az ajánlott elektronikus kézbesítési szolgáltató (ERDSP) minden egyes általa kibocsátott bizonyíték esetében archiválja a bizonyítékot és/vagy a bizonyítékkivonatokat

— REQ-ERDS-5.4.1-08 Az ERDS által generált ERDS-bizonyítékok megfelelnek az ETSI EN 319 522-2 szabvány [4] 8. szakaszában meghatározott bizonyítékszemantikának

8. 7.2.1. Közös rendelkezések

— REQ-ERDS-7.2.1-02 Az ERDSP bizalmi szerepet betöltő személyzete képes teljesíteni a formális képzés és bizonyítványok, illetve a tényleges szakmai tapasztalat, vagy pedig a kettő kombinációja révén szerzett szaktudásra, tapasztalatra és képesítésre vonatkozó követelményt

— REQ-ERDS-7.2.1-03 Az REQ-ERDS-7.2.1-02 követelmény betartása magában foglalja az új fenyegetésekre és a jelenlegi biztonsági gyakorlatokra vonatkozó (legalább 12 havi) rendszeres tájékoztatást

9. 7.3.2. Adathordozók kezelése

— REQ-ERDS-7.3.1-02 Az ETSI EN 319 401 szabvány [1] 7.3.3. szakaszában meghatározott összes követelmény alkalmazandó

10. 7.5. Kriptográfiai ellenőrzések

— REQ-ERDS-7.5-01A Az ERDS az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusokkal [5] összhangban megfelelő kriptográfiai technikákat választ és alkalmaz

— REQ-ERDSP-7.5-03 Az ERDS személyes aláírási kulcsát biztonságos kriptográfiai eszközön belül tárolják és használják, amely az alábbiaknak megfelelően tanúsított, megbízható rendszer:

a) az informatikai biztonságértékelés közös kritériumai az ISO/IEC 15408 szabvány [6] szerint vagy az informatikai biztonságértékelés közös kritériumainak megfelelően, CC:2002 verzió, 1–5. rész, közzétéve az informatikai biztonság területén a közös kritériumokra vonatkozó tanúsítványok elismeréséről szóló megállapodás résztvevői által, EAL 4 vagy magasabb szintű tanúsítással; vagy

b) a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC) [7][8], EAL 4 vagy magasabb szintű tanúsítással; vagy

c) 2030.12.31-ig a FIPS PUB 140-3 szabvány [9] 3. szintje.

A tanúsítás kockázatelemzés alapján, fizikai és egyéb, nem technikai biztonsági intézkedések figyelembevételével történik, olyan biztonsági cél vagy védelmi profil, illetve modulterv- és biztonsági dokumentáció szerint, amely megfelel a jelen dokumentumban szereplő követelményeknek.

Ha a biztonságos kriptográfiai eszköz EUCC [7][8] tanúsítással rendelkezik, akkor ezt az eszközt az említett tanúsításnak megfelelően konfigurálják és használják

11. 7.8. Hálózatbiztonság

— REQ-ERDSP-7.8-04 Az ERDSP a legkorszerűbb protokollokat és algoritmusokat használja a szállítási réteg szintjén történő titkosításhoz, összhangban az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusokkal [5]

— REQ-ERDSP-7.8-06 Az ETSI EN 319 401 szabvány [1] REQ-7.8-13 követelményében előírt sebezhetőségi vizsgálatot negyedévente legalább egyszer elvégzik

— REQ-ERDSP-7.8-07 Az ETSI EN 319 401 szabvány [1] REQ-7.8-17X követelményében előírt behatolási tesztelést évente legalább egyszer elvégzik

— REQ-ERDSP-7.8-08 A tűzfalakat úgy konfigurálják, hogy megakadályozzák a TSP működéséhez nem szükséges protokollok használatát és hozzáférést

12. 7.12. A szolgáltatás ERDSP általi megszüntetése és az ERDS-re vonatkozó szolgáltatásmegszüntetési tervek

— REQ-ERDS-7.12-03 Az ERDSP szolgáltatás megszüntetésére vonatkozó terve megfelel a 910/2014/EU rendelet [i.1] 24. cikkének (5) bekezdése alapján elfogadott végrehajtási jogi aktusokban meghatározott követelményeknek

13. 7.14. Ellátási lánc

— REQ-ERDS-7.14-01 Az ETSI EN 319 401 szabvány [1] 7.14. szakaszában meghatározott követelmények alkalmazandók

II. MELLÉKLET

A 2. cikkben említett referenciaszabványok és specifikációk jegyzéke

Az ETSI EN 319 522-1 V1.2.1 (2024-01) (a továbbiakban: ETSI EN 319 522-1), ETSI EN 319 522-2 V1.2.1 (2024-01) (a továbbiakban: ETSI EN 319 522-2), ETSI EN 319 522-3 V1.2.1 (2024-01) (a továbbiakban: ETSI EN 319 522-3), ETSI EN 319 522-4-1 V1.2.1 (2019-01) (a továbbiakban: ETSI EN 319 522-4-1), ETSI EN 319 522-4-2 V1.1.1 (2018-09) (a továbbiakban: ETSI EN 319 522-4-2) és az ETSI EN 319 522-4-3 V1.1.1 (2018-09) (a továbbiakban: ETSI EN 319 522-4-3) szabvány alkalmazandó.