Publicatieblad
van de Europese Unie

NL
L-serie

2025/1944

30.9.2025

UITVOERINGSVERORDENING (EU) 2025/1944 VAN DE COMMISSIE

van 29 september 2025

tot vaststelling van uitvoeringsbepalingen voor Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad inzake referentienormen voor processen voor het verzenden en ontvangen van gegevens in gekwalificeerde elektronische aangetekende bezorging en inzake de interoperabiliteit van die diensten

DE EUROPESE COMMISSIE,

Gezien het verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG ([1]), en met name artikel 44, lid 2, en artikel 44, lid 2, punt b),

Overwegende hetgeen volgt:

(1) Gekwalificeerde diensten voor elektronisch aangetekende bezorging bieden een veilig kanaal voor de verzending van documenten, met inbegrip van het bewijs van verzending en ontvangst van de gegevens. Zij zijn bedoeld om zekerheid te bieden bij de identificatie van de geadresseerde en een hoog niveau van vertrouwen in de identificatie van de afzender te waarborgen.

(2) Het in artikel 44, lid 1 bis, van Verordening (EU) nr. 910/2014 vastgestelde vermoeden van overeenstemming mag alleen van toepassing zijn wanneer gekwalificeerde vertrouwensdiensten voor de levering van gekwalificeerde diensten voor elektronisch aangetekende bezorging voldoen aan de in deze verordening vastgestelde normen. Deze normen moeten vaste praktijken weerspiegelen en in de betrokken sectoren algemeen erkend worden. Deze normen moeten worden aangepast om er aanvullende controles in op te nemen die de veiligheid en betrouwbaarheid van de gekwalificeerde vertrouwensdienst waarborgen.

(3) Indien een verlener van vertrouwensdiensten voldoet aan de in de bijlage bij deze verordening vastgestelde vereisten, moeten toezichtinstanties veronderstellen dat hij voldoet aan de desbetreffende vereisten van Verordening (EU) nr. 910/2014 en deze veronderstelling naar behoren in aanmerking nemen voor de toekenning of bevestiging van de gekwalificeerde status van de vertrouwensdienst. Een gekwalificeerde verlener van vertrouwensdiensten kan echter nog steeds vertrouwen op andere praktijken om de naleving met de vereisten van Verordening (EU) nr. 910/2014 aan te tonen.

(4) Krachtens artikel 44, lid 2, punt a), van Verordening (EU) nr. 910/2014, wanneer gekwalificeerde verleners van vertrouwensdiensten ermee instemmen om hun diensten uitwisselbaar te maken, is het belangrijk dat ze de gepaste normen en specificaties opvolgen die zijn uiteengezet in bijlage II bij deze uitvoeringsverordening teneinde de overdracht van elektronisch aangetekende gegevens tussen twee of meer gekwalificeerde verleners van vertrouwensdiensten te bespoedigen en eerlijke praktijken op de interne markt te bevorderen.

(5) De Commissie voert regelmatig beoordelingen van nieuwe technologieën, praktijken, normen of technische specificaties uit. Overeenkomstig overweging 75 van Verordening (EU) 2024/1183 van het Europees Parlement en de Raad ([2]) moet de Commissie deze verordening indien nodig evalueren en actualiseren om deze in overeenstemming te houden met de mondiale ontwikkelingen, de nieuwe technologieën, de normen of de technische specificaties en om de beste praktijken op de interne markt te volgen.

([1]) PB L 257 van 28.8.2014, blz. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Verordening (EU) 2024/1183 van het Europees Parlement en de Raad van 11 april 2024 tot wijziging van Verordening (EU) nr. 910/2014, wat betreft de vaststelling van het Europees kader voor digitale identiteit (PB L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(6) Verordening (EU) 2016/679 van het Europees Parlement en de Raad ([3]), en, in voorkomend geval, Richtlijn 2002/58/EG van het Europees Parlement en de Raad ([4]) zijn van toepassing op alle activiteiten betreffende de verwerking van alle persoonsgegevens uit hoofde van deze verordening.

(7) De Europese Toezichthouder voor gegevensbescherming is overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([5]) geraadpleegd en heeft op 6 juni 2025 een advies uitgebracht.

(8) De in deze verordening vervatte maatregelen zijn in overeenstemming met het advies van het bij artikel 48 van Verordening (EU) nr. 910/2014 ingestelde comité,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Referentienormen en specificaties voor gekwalificeerde diensten voor elektronisch aangetekende bezorging

De in artikel 44, lid 2, van Verordening (EU) nr. 910/2014 genoemde referentienormen en specificaties zijn vastgesteld in bijlage I bij deze verordening.

Artikel 2

Referentienormen en specificaties voor de interoperabiliteit tussen gekwalificeerde diensten voor elektronisch aangetekende bezorging

De in artikel 44, lid 2, punt b), van Verordening (EU) nr. 910/2014 genoemde referentienormen en specificaties zijn vastgesteld in bijlage II bij deze verordening.

Artikel 3

Inwerkingtreding

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 29 september 2025.

Voor de Commissie
De voorzitter
Ursula VON DER LEYEN

([3]) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB L 201 van 31.7.2002, blz. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

BIJLAGE I

Lijst van de in artikel 1 bedoelde referentienormen en specificaties

De norm ETSI EN 319 521 V1.1.1 (2019-02) ("ETSI EN 319 521") is van toepassing met de volgende aanpassingen:

1. Voor ETSI EN 319.521

(1) 2.1 Normatieve referenties:

— [1] ETSI EN 319 401 V3.1.1 (2024-06) "Elektronische handtekeningen en infrastructuren (ESI); Algemene beleidseisen voor verleners van vertrouwensdiensten".

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) "Elektronische handtekeningen en infrastructuren (ESI); Beleids- en beveiligingseisen voor verleners van vertrouwensdiensten die certificaten afgeven; Deel 1: Algemene eisen".

— [3] ETSI EN 319 522-1 V1.2.1 (2024-01) "Elektronische handtekeningen en infrastructuren (ESI); Diensten voor elektronisch aangetekende bezorging; Deel 1: Kader en architectuur".

— [4] ETSI EN 319 522-2 V1.2.1 (2024-01) "Elektronische handtekeningen en infrastructuren (ESI); Diensten voor elektronisch aangetekende bezorging; Deel 2: Semantische inhoud".

— [5] Europese Groep voor cyberbeveiligingscertificering, subgroep inzake cryptografie: "Agreed Cryptographic Mechanisms", gepubliceerd door het Agentschap van de Europese Unie voor cyberbeveiliging ("Enisa") ([1]).

— [6] ISO/IEC 15408-1:2022 "Informatiebeveiliging, cyberbeveiliging en privacybescherming — Evaluatiecriteria voor IT-beveiliging".

— [7] Uitvoeringsverordening (EU) 2024/482 van de Commissie ([2]) houdende uitvoeringsbepalingen van Verordening (EU) 2019/881 van het Europees Parlement en de Raad wat betreft de vaststelling van de Europese op gemeenschappelijke criteria gebaseerde cyberbeveiligingscertificeringsregeling (EUCC).

— [8] Uitvoeringsverordening (EU) 2024/3144 van de Commissie ([3]) tot wijziging van Uitvoeringsverordening (EU) 2024/482 wat betreft toepasselijke internationale normen en tot rectificatie van die uitvoeringsverordening.

— [9] FIPS PUB 140-3 (2019) "Beveiligingseisen voor cryptografische modules".

(2) 3.1 Definities

— geavanceerd elektronisch zegel: zoals gedefinieerd in Verordening (EU) nr. 910/2014 [i.1].

— geavanceerde elektronische handtekening: zoals gedefinieerd in Verordening (EU) nr. 910/2014 [i.1].

— gekwalificeerd elektronisch zegel: zoals gedefinieerd in Verordening (EU) nr. 910/2014 [i.1].

— gekwalificeerde elektronische handtekening: zoals gedefinieerd in Verordening (EU) nr. 910/2014 [i.1].

— beveiligd cryptografisch apparaat: apparaat dat de privésleutel van de gebruiker bevat, deze sleutel tegen inbreuk beschermt en namens de gebruiker ondertekening of ontcijferingsfuncties uitvoert.

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

(3) 5.1.1 Algemene bepalingen

— REQ-ERDS-5.1.1-01 De dienst voor elektronisch aangetekende bezorging zorgt ervoor dat de beschikbaarheid, integriteit en vertrouwelijkheid van de gebruikersinhoud op adequate wijze worden gewaarborgd tijdens de verwerking ervan door de dienst voor elektronisch aangetekende bezorging, door geschikte cryptografische technieken voor integriteit en vertrouwelijkheid te selecteren die overeenstemmen met de door de Europese Groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa [5] gepubliceerde Agreed Cryptographic Mechanisms.

(4) 5.2.1.1 Algemeen

— REQ-QERDS-5.2.1.1-01 De gekwalificeerde dienst voor elektronisch aangetekende bezorging verifieert met een zeer hoog betrouwbaarheidsniveau de identiteit van de ontvanger, hetzij rechtstreeks, hetzij door gebruik te maken van een derde partij, en indien nodig met behulp van een van de volgende middelen of een combinatie daarvan:

(a) door de fysieke aanwezigheid van de natuurlijke persoon of van een gemachtigde vertegenwoordiger van de rechtspersoon, volgens passende bewijzen en procedures, overeenkomstig nationaal recht;

(b) extern, door gebruik van elektronische identificatiemiddelen die voldoen aan de vereisten van artikel 8 van Verordening (EU) nr. 910/2014 [i.1] wat betreft het betrouwbaarheidsniveau “hoog” of door middel van de Europese portemonnee voor digitale identiteit;

(c) door middel van een certificaat van een gekwalificeerde elektronische handtekening of van een gekwalificeerd elektronisch zegel;

(d) door middel van andere identificatiemethoden die ervoor zorgen dat de natuurlijke persoon of de gemachtigde vertegenwoordiger van de rechtspersoon met een zeer hoge mate van betrouwbaarheid kan worden geïdentificeerd. De garantie dat deze identificatie met een zeer hoge mate van betrouwbaarheid wordt uitgevoerd, wordt bevestigd door een conformiteitsbeoordelingsinstantie.

— REQ-QERDS-5.2.1.1-01A De gekwalificeerde dienst voor elektronisch aangetekende bezorging verifieert de identiteit van de afzender met behulp van passende middelen, hetzij rechtstreeks, hetzij door gebruik te maken van een derde partij, op basis van een van de volgende methoden of een combinatie daarvan:

(a) door de fysieke aanwezigheid van de natuurlijke persoon of van een gemachtigde vertegenwoordiger van de rechtspersoon, volgens passende bewijzen en procedures, overeenkomstig nationaal recht;

(b) op afstand, door middel van de Europese portemonnee voor digitale identiteit of een aangemeld elektronisch identificatiemiddel dat voldoet aan de vereisten van artikel 8 van Verordening (EU) nr. 910/2014 [i.1] met betrekking tot het betrouwbaarheidsniveau “substantieel”, mits het is afgegeven op basis van de voorafgaande fysieke aanwezigheid van de natuurlijke persoon of van een gemachtigde vertegenwoordiger van de rechtspersoon;

(c) door middel van een certificaat van een geavanceerde elektronische handtekening of een geavanceerd elektronisch zegel, op voorwaarde dat het certificaat werd afgegeven aan een natuurlijk persoon of een gemachtigde vertegenwoordiger van de rechtspersoon in het kader van de normalised certificate policy (NCP) van ETSI EN 319 411-1 [2]; of

(d) door middel van andere identificatiemethoden die ervoor zorgen dat de natuurlijke persoon of de gemachtigde vertegenwoordiger van de rechtspersoon met een zeer hoge mate van betrouwbaarheid kan worden geïdentificeerd. De garantie dat deze identificatie met een hoge mate van betrouwbaarheid wordt uitgevoerd, wordt bevestigd door een conformiteitsbeoordelingsinstantie.

— OPMERKING De derde partij die de identiteit van de afzender en de ontvanger verifieert, kan een andere gekwalificeerde dienst voor elektronisch aangetekende bezorging zijn indien de afzender en de ontvanger op verschillende gekwalificeerde diensten voor elektronisch aangetekende bezorging zijn geabonneerd.

(5) 5.2.1.2 Identificatie van ontvanger en overdracht van gebruikersinhoud

— REQ-QERDS-5.2.1.2-03 Indien de identificatie van de ontvanger is gebaseerd op een intern proces van de gekwalificeerde dienst voor elektronisch aangetekende bezorging, voert de gekwalificeerde dienst voor elektronisch aangetekende bezorging het hele proces uit in een beveiligde en gecontroleerde omgeving.

(6) 5.2.2 Bepalingen voor authenticatie door een gekwalificeerde EU-dienst voor elektronisch aangetekende bezorging

— REQ-QERDS-5.2.2-03 [VOORWAARDELIJK] Wanneer de gekwalificeerde dienst voor elektronisch aangetekende bezorging authenticatiemiddelen koppelt aan de identiteit van een afzender die is geverifieerd overeenkomstig clausule 5.2.1, moet het een van de volgende zijn:

(a) tweefactorenauthenticatiemechanismen;

(b) de Europese portemonnee voor digitale identiteit of een aangemeld elektronisch identificatiemiddel dat voldoet aan de vereisten van artikel 8 van Verordening (EU) nr. 910/2014 [i.1] wat betreft het betrouwbaarheidsniveau “hoog” of “substantieel”;

(c) een wederzijdse TLS-authenticatie die een certificaat omvat dat in het kader van het NCP van ETSI EN 319 411-1 [2] aan de afzender is afgegeven;

(d) een digitale handtekening die door een in het kader van het NCP van ETSI EN 319 411-1 [2] certificaat wordt gestaafd;

(e) andere middelen die de authenticatie van de geïdentificeerde afzender garanderen. De overeenstemming daarvan wordt bevestigd door een conformiteitsbeoordelingsinstantie. Voorbeeld: Dit kan het gebruik omvatten van een van de bovenstaande middelen van letter a), b) en d) om een clientcertificaat voor beveiliging van de transportlaag (TLS) te registreren voor geautomatiseerde bezorging via wederzijdse TLS, of om een digitaal zegelcertificaat te registreren dat kan worden gebruikt om een digitaal zegelcertificaat te registreren dat wordt gebruikt om beweringen te zegelen voor authenticatie bij de dienst voor elektronisch aangetekende bezorging. Andere mechanismen kunnen ook van toepassing zijn wanneer de geïdentificeerde afzenders gebruikmaken van gedelegeerde diensten van derden.

— REQ-QERDS-5.2.2-03A [VOORWAARDELIJK] Wanneer de gekwalificeerde dienst voor elektronisch aangetekende bezorging authenticatiemiddelen koppelt aan de identiteit van een geverifieerde ontvanger conform clausule 5.2.1, moet het één van de volgende zijn, op voorwaarde dat de middelen, of een combinatie van middelen, een zeer hoge mate van betrouwbaarheid met betrekking tot de identiteit van de geverifieerde ontvanger garanderen:

(a) een multifactorauthenticatiemechanisme

(b) de Europese portemonnee voor digitale identiteit of een aangemeld elektronisch identificatiemiddel dat voldoet aan de vereisten van artikel 8 van Verordening (EU) nr. 910/2014 [i.1] wat betreft het betrouwbaarheidsniveau “hoog” of “substantieel”;

(c) een certificaat van een gekwalificeerde elektronische handtekening of van een gekwalificeerd elektronisch zegel;

(d) andere middelen die de authenticatie van de geïdentificeerde ontvanger garanderen. De overeenstemming daarvan wordt bevestigd door een conformiteitsbeoordelingsinstantie. Voorbeeld: Dit kan het gebruik omvatten van een van de bovenstaande middelen van letter a) tot en met c) om een clientcertificaat voor beveiliging van de transportlaag (TLS) te registreren voor geautomatiseerde bezorging via wederzijdse TLS, of om een digitaal zegelcertificaat te registreren dat kan worden gebruikt om een digitaal zegelcertificaat te registreren dat wordt gebruikt om beweringen te zegelen voor authenticatie bij de dienst voor elektronisch aangetekende bezorging. Andere mechanismen kunnen ook van toepassing zijn wanneer de geïdentificeerde afzenders gebruikmaken van gedelegeerde diensten van derden.

— REQ-QERDS-5.2.2-04 [VOORWAARDELIJK] Indien de afzender verbinding maakt met de gekwalificeerde dienst voor elektronisch aangetekende bezorging via een beveiligde verbinding die wederzijdse authenticatie van machine naar machine vereist tussen de machine van de afzender en de server van de gekwalificeerde dienst voor elektronisch aangetekende bezorging op basis van certificaten die zijn afgegeven overeenkomstig het NCP als bedoeld in ETSI EN 319 411-1 [2], dan kunnen nadat deze beveiligde verbinding is opgezet mechanismen voor enkelvoudige authenticatie worden ingesteld voor een tweede authenticatiefase van de afzender, als de ingevoerde organisatorische procedures en beveiligingsmaatregelen betrouwbaarheid van de authenticatie van de afzender garanderen.

(7) 5.4.1 Algemene bepalingen

— REQ-ERDS-5.4.1-06 De dienst voor elektronisch aangetekende bezorging moet genereert gebeurtenissen zoals gedefinieerd in clausule 6 van ETSI EN 319 522-1 [3] en stelt deze beschikbaar aan legitieme belanghebbenden.

— REQ-ERDS-5.4.1-07 De dienst voor elektronisch aangetekende bezorging archiveert het bewijs en/of de samenvatting van het bewijs voor elk bewijs dat het heeft afgegeven.

— REQ-ERDS-5.4.1-08 Het bewijs van de dienst voor elektronisch aangetekende bezorging dat wordt gegenereerd door de dienst voor elektronisch aangetekende bezorging is in overeenstemming met semantisch gedefinieerd bewijs als bedoeld in ETSI EN 319 522-2 [4], clausule 8.

(8) 7.2.1 Algemene bepalingen

— REQ-ERDS-7.2.1-02 Het personeel van de dienst voor elektronisch aangetekende bezorging in vertrouwensrollen is in staat om de eis van "deskundigheid, ervaring en kwalificaties" te vervullen, door middel van formele opleiding en referenties, of feitelijke ervaring, of een combinatie van beide.

— REQ-ERDS- 7.2.1-03 De overeenstemming met REQ-ERDS- 7.2.1-02 gaat gepaard met regelmatig bijgewerkte informatie (ten minste elke twaalf maanden) over nieuwe dreigingen en actuele beveiligingspraktijken.

(9) 7.3.2 Mediabeheer

— REQ-ERDS-7.3.1-02 Alle eisen van ETSI EN 319 401 [1], clausule 7.3.3, zijn van toepassing.

(10) 7.5 Cryptografische beheersmaatregelen

— REQ-ERDS-7.5-01A De dienst voor elektronisch aangetekende bezorging selecteert en gebruikt geschikte cryptografische technieken in overeenstemming met de door de Europese Groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [5].

— REQ-ERDSP-7.5- 03 De privéondertekensleutel van de dienst voor elektronisch aangetekende bezorging wordt bewaard en gebruikt in een beveiligd cryptografisch apparaat: een betrouwbaar systeem dat is gecertificeerd in overeenstemming met:

(a) gemeenschappelijke criteria voor de evaluatie van de beveiliging van informatietechnologie, zoals uiteengezet in ISO/IEC 15408 [6] of in gemeenschappelijke criteria voor de evaluatie van de beveiliging van informatietechnologie, versie CC 2002, delen 1 tot en met 5, gepubliceerd door de deelnemers aan de regeling ter erkenning van certificaten van gemeenschappelijke criteria op het gebied van IT-beveiliging, en gecertificeerd tot EAL 4 of hoger; of

(b) de Europese op gemeenschappelijke criteria gebaseerde cyberbeveiligingscertificeringsregeling (EUCC) [7][8] en gecertificeerd tot EAL 4 of hoger; of

(c) tot 31.12.2030, FIPS PUB 140-3 [9] niveau 3.

Dit certificaat dient voor een beveiligingsdoelstelling of beveiligingsprofiel, of voor een moduleontwerp en beveiligingsdocumentatie, wat voldoet aan de eisen van onderhavig document, op basis van een risicoanalyse en rekening houdend met fysieke en andere niet-technische beveiligingsmaatregelen.

Indien het beveiligd cryptografisch apparaat baat heeft bij een EUCC [7][8]-certificering, dan zal dit apparaat worden geconfigureerd en gebruikt in overeenstemming met dat certificaat.

(11) 7.8 Netwerkbeveiliging

— REQ-ERDSP-7.8-04 De dienst voor elektronisch aangetekende bezorging gebruikt geavanceerde protocollen en algoritmen voor versleuteling op transportlaagniveau die overeenstemmen met de door de Europese Groep voor cyberbeveiligingscertificering goedgekeurde en door Enisa gepubliceerde Agreed Cryptographic Mechanisms [5].

— REQ-ERDSP-7.8-06 De door REQ-7.8-13 van ETSI EN 319.401 [1] aangevraagde kwetsbaarheidsscan wordt ten minste eenmaal per kwartaal uitgevoerd.

— REQ-ERDSP-7.8-07 De door REQ-7.8-17X van ETSI EN 319.401 [1] aangevraagde penetratietest wordt ten minste eenmaal per jaar uitgevoerd.

— REQ-ERDSP-7.8-08 Firewalls worden geconfigureerd om alle protocollen en toegangen die niet vereist zijn voor de bedrijfsvoering van de verlener van vertrouwensdiensten te verwijderen.

(12) 7.12 Beëindiging dienstverlener voor elektronisch aangetekende bezorging en beëindigingsplannen dienst voor elektronisch aangetekende bezorging

— REQ-ERDS-7.12-03 Het beëindigingsplan van de dienstverlener voor elektronisch aangetekende bezorging voldoet aan de eisen van de overeenkomstig artikel 24, lid 5, van Verordening (EU) nr. 910/2014 vastgestelde uitvoeringshandelingen [i.1].

(13) 7.14 Toeleveringsketen

— REQ-ERDS-7.14-01 De in ETSI EN 319 401 [1], clausule 7.14 bedoelde eisen zijn van toepassing.

BIJLAGE II

Lijst van de in artikel 2 bedoelde referentienormen en specificaties

De normen 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") en ETSI EN 319 522-4-3 V1.1.1 (2018-09) ("ETSI EN 319 522-4-3") zijn van toepassing.