Euroopan unionin
virallinen lehti

FI
L-sarja

2025/1944

30.9.2025

KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2025/1944,

annettu 29 päivänä syyskuuta 2025,

Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 soveltamissäännöistä siltä osin kuin on kyse tietojen lähettämis- ja vastaanottamisprosesseihin hyväksytyissä sähköisissä rekisteröidyissä jakelupalveluissa sovellettavista viitestandardeista ja näiden palvelujen yhteentoimivuudesta

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen,

ottaa huomioon sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta 23 päivänä heinäkuuta 2014 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 ([1]) ja erityisesti sen 44 artiklan 2 kohdan ja 44 artiklan 2 b kohdan,

sekä katsoo seuraavaa:

(1) Hyväksytyt sähköiset rekisteröidyt jakelupalvelut tarjoavat suojatun kanavan asiakirjojen toimittamiseen, myös antamalla vahvistuksen tietojen lähettämisestä ja vastaanottamisesta. Niiden tarkoituksena on tarjota varmuutta vastaanottajan tunnistamisessa ja varmistaa lähettäjän tunnistaminen korkealla varmuustasolla.

(2) Asetuksen (EU) N:o 910/2014 44 artiklan 1 a kohdassa säädettyä vaatimustenmukaisuusolettamaa olisi sovellettava ainoastaan, jos hyväksyttyjä sähköisiä rekisteröityjä jakelupalveluja tarjoavat hyväksytyt luottamuspalvelut ovat tässä asetuksessa vahvistettujen standardien mukaisia. Näiden standardien olisi heijastettava vakiintuneita käytäntöjä, ja niiden olisi oltava laajasti tunnustettuja kyseessä olevilla aloilla. Niitä olisi mukautettava siten, että niihin sisällytetään lisätarkastuksia, joilla varmistetaan hyväksytyn luottamuspalvelun turvallisuus ja luotettavuus.

(3) Jos luottamuspalvelun tarjoaja noudattaa tämän asetuksen liitteessä vahvistettuja vaatimuksia, valvontaelinten olisi oletettava, että asetuksen (EU) N:o 910/2014 asiaankuuluvia vaatimuksia on noudatettu, ja otettava tällainen olettamus asianmukaisesti huomioon luottamuspalvelun hyväksytyn aseman myöntämiseksi tai vahvistamiseksi. Hyväksytty luottamuspalvelun tarjoaja voi kuitenkin edelleen tukeutua muihin käytäntöihin osoittaakseen, että asetuksen (EU) N:o 910/2014 vaatimuksia noudatetaan.

(4) Jos hyväksytyt luottamuspalvelun tarjoajat sopivat palvelujensa yhteentoimivuudesta asetuksen (EU) N:o 910/2014 44 artiklan 2 a kohdan mukaisesti, on tärkeää, että ne noudattavat tämän täytäntöönpanoasetuksen liitteessä II vahvistettuja asianmukaisia standardeja ja eritelmiä, jotta sähköisesti rekisteröityjä tietoja voidaan helposti siirtää kahden tai useamman hyväksytyn luottamuspalvelun tarjoajan välillä ja voidaan edistää oikeudenmukaisia käytäntöjä sisämarkkinoilla.

(5) Komissio arvioi säännöllisesti uusia teknologioita, käytäntöjä, standardeja tai teknisiä eritelmiä. Euroopan parlamentin ja neuvoston asetuksen (EU) 2024/1183 ([2]) johdanto-osan 75 kappaleen mukaan komission olisi tarkasteltava uudelleen ja tarvittaessa päivitettävä tätä asetusta sen pitämiseksi maailmanlaajuisen kehityksen ja uusien teknologioiden, standardien tai teknisten eritelmien mukaisena sekä sisämarkkinoiden parhaiden käytäntöjen noudattamiseksi.

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

([2]) Euroopan parlamentin ja neuvoston asetus (EU) 2024/1183, annettu 11 päivänä huhtikuuta 2024, asetuksen (EU) N:o 910/2014 muuttamisesta eurooppalaisen digitaalisen identiteetin kehyksen vahvistamisen osalta (EUVL L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(6) Kaikkiin tämän asetuksen mukaisiin henkilötietojen käsittelytoimiin sovelletaan Euroopan parlamentin ja neuvoston asetusta (EU) 2016/679 ([3]) ja tarvittaessa Euroopan parlamentin ja neuvoston direktiiviä 2002/58/EY ([4]).

(7) Euroopan tietosuojavaltuutettua on kuultu Euroopan parlamentin ja neuvoston asetuksen (EU) 2018/1725 ([5]) 42 artiklan 1 kohdan mukaisesti, ja hän antoi lausuntonsa 6 päivänä kesäkuuta 2025.

(8) Tässä asetuksessa säädetyt toimenpiteet ovat asetuksen (EU) N:o 910/2014 48 artiklalla perustetun komitean lausunnon mukaiset,

ON HYVÄKSYNYT TÄMÄN ASETUKSEN:

1 artikla

Hyväksyttyjä sähköisiä rekisteröityjä jakelupalveluja koskevat viitestandardit ja eritelmät

Asetuksen (EU) N:o 910/2014 44 artiklan 2 kohdassa tarkoitetut viitestandardit ja eritelmät esitetään tämän asetuksen liitteessä I.

2 artikla

Hyväksyttyjen sähköisten rekisteröityjen jakelupalvelujen yhteentoimivuutta koskevat viitestandardit ja eritelmät

Asetuksen (Eu) N:o 910/2014 44 artiklan 2 b kohdassa tarkoitetut viitestandardit ja eritelmät esitetään tämän asetuksen liitteessä II.

3 artikla

Voimaantulo

Tämä asetus tulee voimaan kahdentenakymmenentenä päivänä sen jälkeen, kun se on julkaistu *Euroopan unionin virallisessa lehdessä*.

Tämä asetus on kaikilta osiltaan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa.

Tehty Brysselissä 29 päivänä syyskuuta 2025.

Komission puolesta
Puheenjohtaja
Ursula VON DER LEYEN

([3]) Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (EUVL L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi) (EYVL L 201, 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) Euroopan parlamentin ja neuvoston asetus (EU) 2018/1725, annettu 23 päivänä lokakuuta 2018, luonnollisten henkilöiden suojelusta unionin toimielinten, elinten ja laitosten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta sekä asetuksen (EY) N:o 45/2001 ja päätöksen N:o 1247/2002/EY kumoamisesta (EUVL L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

LIITE I

Luettelo 1 artiklassa tarkoitetuista viitestandardeista ja eritelmistä

Standardia ETSI EN 319 521 V1.1.1 (2019-02) (’ETSI EN 319 521’) sovelletaan seuraavin mukautuksin:

1. ETSI EN 319 521

1) 2.1 Velvoittavat viittaukset

— [1] ETSI EN 319 401 V3.1.1 (2024-06) ”Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers”.

— [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”.

— [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”.

— [4] ETSI EN 319 522-2 V1.2.1 (2024-01) ”Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic content”.

— [5] Euroopan kyberturvallisuuden sertifiointiryhmä, Salausta käsittelevä alaryhmä: Euroopan kyberturvallisuusviraston (ENISA) julkaisema asiakirja ”Agreed Cryptographic Mechanisms” ([1]).

— [6] ISO/IEC 15408-1:2022 – Information security, cybersecurity and privacy protection – Evaluation criteria for IT security.

— [7] Komission täytäntöönpanoasetus (EU) 2024/482 ([2]) Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 soveltamissäännöistä siltä osin kuin on kyse yhteisiin kriteereihin perustuvan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän (EUCC) hyväksymisestä.

— [8] Komission täytäntöönpanoasetus (EU) 2024/3144 ([3]) täytäntöönpanoasetuksen (EU)2024/482 muuttamisesta sovellettavien kansainvälisten standardien osalta ja kyseisen täytäntöönpanoasetuksen oikaisemisesta.

— [9] FIPS PUB 140-3 (2019) ”Security Requirements for Cryptographic Modules”.

2) 3.1 Käsitteet

— kehittynyt sähköinen leima: siten kuin se on määritelty asetuksessa (EU) N:o 910/2014 [i.1].

— kehittynyt sähköinen allekirjoitus: siten kuin se on määritelty asetuksessa (EU) N:o 910/2014 [i.1].

— hyväksytty sähköinen leima: siten kuin se on määritelty asetuksessa (EU) N:o 910/2014 [i.1].

— hyväksytty sähköinen allekirjoitus: siten kuin se on määritelty asetuksessa (EU) N:o 910/2014 [i.1].

— suojattu salauslaite: laite, jossa pidetään käyttäjän yksityistä avainta ja joka suojaa tätä avainta vaarantumiselta ja suorittaa allekirjoitus- tai salauksenpurkutoimintoja käyttäjän puolesta.

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

3) 5.1.1 Yhteiset säännökset

— REQ-ERDS-5.1.1-01 Sähköisen rekisteröidyn jakelupalvelun (ERDS) on varmistettava, että käyttäjäsisällön saatavuus, eheys ja luottamuksellisuus taataan asianmukaisesti niin kauan kuin sitä käsitellään ERDS:ssä, ja valittava sopivia eheyttä ja luottamuksellisuutta tukevia salaustekniikoita, jotka ovat Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [5] mukaisia.

4) 5.2.1.1 Yleistä

— REQ-QERDS-5.2.1.1-01 Hyväksytyn sähköisen rekisteröidyn jakelupalvelun tarjoajan (QERDSP) on tarkastettava vastaanottajan henkilöllisyys erittäin korkealla luottamustasolla joko suoraan tai kolmannen osapuolen avulla ja käyttäen tarpeen mukaan jotakin seuraavista menetelmistä tai niiden yhdistelmää:

a) luonnollisen henkilön tai oikeushenkilön valtuutetun edustajan fyysisellä läsnäololla, käyttäen asianmukaisia todisteita ja menettelyjä kansallisen lainsäädännön mukaisesti;

b) etänä käyttäen sähköisen tunnistamisen menetelmää, joka täyttää asetuksen (EU) N:o 910/2014 [i.1] 8 artiklassa säädetyt korkeaa varmuustasoa koskevat vaatimukset, tai eurooppalaisen digitaalisen identiteetin lompakon avulla;

c) käyttäen hyväksytyn sähköisen allekirjoituksen tai hyväksytyn sähköisen leiman varmennetta;

d) käyttäen muita tunnistamismenetelmiä, joilla varmistetaan, että luonnollinen henkilö tai oikeushenkilön valtuutettu edustaja voidaan tunnistaa erittäin korkealla luottamustasolla. Vaatimustenmukaisuuden arviointilaitoksen on vahvistettava, että tämä tunnistaminen tapahtuu erittäin korkealla luottamustasolla.

— REQ-QERDS-5.2.1.1-01A QERDSP:n on tarkastettava lähettäjän henkilöllisyys asianmukaisin keinoin joko suoraan tai kolmannen osapuolen avulla käyttäen jotakin seuraavista menetelmistä tai niiden yhdistelmää:

a) luonnollisen henkilön tai oikeushenkilön valtuutetun edustajan fyysisellä läsnäololla, käyttäen asianmukaisia todisteita ja menettelyjä kansallisen lainsäädännön mukaisesti;

b) etänä käyttäen eurooppalaista digitaalisen identiteetin lompakkoa tai ilmoitettua sähköisen tunnistamisen menetelmää, joka täyttää asetuksen (EU) N:o 910/2014 [i.1] 8 artiklassa säädetyt korotettua varmuustasoa koskevat vaatimukset edellyttäen, että se on myönnetty luonnollisen henkilön tai oikeushenkilön valtuutetun edustajan aiemman fyysisen läsnäolon perusteella;

c) käyttäen kehittyneen sähköisen allekirjoituksen tai kehittyneen sähköisen leiman varmennetta edellyttäen, että varmenne on myönnetty luonnolliselle henkilölle tai oikeushenkilön valtuutetulle edustajalle standardissa ETSI EN 319 411-1 [2] määritellyn normalisoidun varmennepolitiikan (NCP) mukaisesti; tai

d) käyttäen muita tunnistamismenetelmiä, joilla varmistetaan, että luonnollinen henkilö tai oikeushenkilön valtuutettu edustaja voidaan tunnistaa erittäin korkealla luottamustasolla. Vaatimustenmukaisuuden arviointilaitoksen on vahvistettava, että tämä tunnistaminen tapahtuu erittäin korkealla luottamustasolla.

— HUOMAUTUS Lähettäjän ja vastaanottajan henkilöllisyyden tarkastava kolmas osapuoli voi olla toinen QERDSP, jos lähettäjä ja vastaanottaja ovat tilaajina eri QERDSP:ssä.

5) 5.2.1.2 Vastaanottajan tunnistaminen ja käyttäjäsisällön luovuttaminen

— REQ-QERDS-5.2.1.2-03 Jos vastaanottajan tunnistaminen perustuu QERDS:n sisäiseen prosessiin, QERDSP:n on suoritettava koko prosessi suojatussa ja valvotussa ympäristössä.

6) 5.2.2 EU QERDS:n todentamista koskevat säännökset

— REQ-QERDS-5.2.2-03 [EHDOLLINEN] Kun QERDSP sitoo todentamismenetelmän lausekkeen 5.2.1 mukaisesti varmennettuun lähettäjän henkilöllisyyteen, menetelmän on oltava jokin seuraavista:

a) kaksivaiheinen todentamismekanismi;

b) eurooppalainen digitaalisen identiteetin lompakko tai ilmoitettu sähköisen tunnistamisen menetelmä, joka täyttää asetuksen (EU) N:o 910/2014 [i.1] 8 artiklassa säädetyt korkeaa tai korotettua varmuustasoa koskevat vaatimukset;

c) keskinäinen TLS-todennus, johon sisältyy lähettäjälle standardissa ETSI EN 319 411-1 [2] määritellyn NCP:n mukaisesti myönnetty varmenne;

d) digitaalinen allekirjoitus, jota tukee standardissa ETSI EN 319 411-1 [2] määritellyn NCP:n mukaisesti myönnetty varmenne;

e) muut keinot, joilla varmistetaan tunnistetun lähettäjän todentaminen. Vaatimustenmukaisuuden arviointilaitoksen on vahvistettava, että sitominen on vaatimusten mukainen. Esimerkki: Tähän voi sisältyä jokin edellä a, b ja d alakohdassa tarkoitetuista menetelmistä, joilla rekisteröidään TLS-asiakasvarmenne keskinäisen TLS:n (Transport Layer Security) kautta tapahtuvaa automaattista lähettämistä varten tai rekisteröidään digitaalinen leimavarmenne, jota käytetään väitteiden leimaamiseen niiden todentamiseksi ERDS:ssä. Voidaan soveltaa myös muita mekanismeja, joissa tunnistetut lähettäjät käyttävät delegoituja kolmannen osapuolen palveluja.

— REQ-QERDS-5.2.2-03A [EHDOLLINEN] Kun QERDSP sitoo todentamismenetelmän lausekkeen 5.2.1 mukaisesti varmennettuun vastaanottajan henkilöllisyyteen, menetelmän on oltava jokin seuraavista edellyttäen, että menetelmä tai mikä tahansa menetelmien yhdistelmä varmistaa erittäin korkean luottamustason todennetun vastaanottajan henkilöllisyyden suhteen:

a) kaksivaiheinen todentamismekanismi;

b) eurooppalainen digitaalisen identiteetin lompakko tai ilmoitettu sähköisen tunnistamisen menetelmä, joka täyttää asetuksen (EU) N:o 910/2014 [i.1] 8 artiklassa säädetyt korkeaa tai korotettua varmuustasoa koskevat vaatimukset;

c) hyväksytyn sähköisen allekirjoituksen tai hyväksytyn sähköisen leiman varmenne;

d) muut keinot, joilla varmistetaan tunnistetun vastaanottajan todentaminen. Vaatimustenmukaisuuden arviointilaitoksen on vahvistettava, että sitominen on vaatimusten mukainen. Esimerkki: Tähän voi sisältyä jokin edellä a–c alakohdassa tarkoitetuista menetelmistä, joilla rekisteröidään TLS-asiakasvarmenne keskinäisen TLS:n kautta tapahtuvaa automaattista lähettämistä varten tai rekisteröidään digitaalinen leimavarmenne, jota käytetään väitteiden leimaamiseen niiden todentamiseksi ERDS:ssä. Voidaan soveltaa myös muita mekanismeja, joissa tunnistetut lähettäjät käyttävät delegoituja kolmannen osapuolen palveluja.

— REQ-QERDS-5.2.2-04 [EHDOLLINEN] Jos lähettäjä on yhteydessä QERDS:ään suojatulla yhteydellä, joka edellyttää standardissa ETSI EN 319 411-1 [2] määritellyn NCP:n mukaisesti myönnettyihin varmenteisiin perustuvaa laitteiden välistä vastavuoroista todentamista lähettäjän laitteen ja QERDS:n palvelimen välillä, tämän suojatun yhteyden muodostamisen jälkeen lähettäjän todentamisen toista vaihetta varten voidaan ottaa käyttöön yhden tekijän todentamismekanismeja, jos käyttöön otetuilla organisatorisilla menettelyillä ja turvatoimenpiteillä varmistetaan luottamus lähettäjän todentamiseen.

7) 5.4.1 Yhteiset säännökset

— REQ-ERDS-5.4.1-06 ERDS:n on tuotettava ja asetettava oikeutettujen asianomaisten osapuolten saataville ERD-tapahtumia koskevat ERDS-todisteet, siten kuin ne on määritelty standardin ETSI EN 319 522-1 [3] lausekkeessa 6.

— REQ-ERDS-5.4.1-07 ERDSP:n on arkistoitava todisteet ja/tai todistetiivistelmä kustakin antamastaan todisteesta.

— REQ-ERDS-5.4.1-08 ERDS:n tuottamien ERDS-todisteiden on oltava standardin ETSI EN 319 522-2 [4] lausekkeessa 8 määritellyn todistesemantiikan mukaisia.

8) 7.2.1 Yhteiset säännökset

— REQ-ERDS-7.2.1-02 ERDSP:n luotetuissa rooleissa olevan henkilöstön on pystyttävä täyttämään vaatimus, joka koskee ”asiantuntemusta, kokemusta ja pätevyyttä”, joka on osoitettu virallisen koulutuksen ja suositusten, työkokemuksen tai näiden yhdistelmän kautta.

— REQ-ERDS-7.2.1-03 Kohdan REQ-ERDS-7.2.1-02 noudattamiseen on sisällyttävä säännöllisesti (vähintään 12 kuukauden välein) tehtäviä päivityksiä uusista uhkista ja nykyisistä turvakäytännöistä.

9) 7.3.2 Tallennusvälineiden käsittely

— REQ-ERDS-7.3.1-02 Sovelletaan kaikkia standardin ETSI EN 319 401 [1] lausekkeessa 7.3.3 määriteltyjä vaatimuksia.

10) 7.5 Salaustekniikka koskevat tarkastukset

— REQ-ERDS-7.5-01A ERDS:n on valittava ja käytettävä sopivia salaustekniikoita, jotka ovat Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [5] mukaisia.

— REQ-ERDSP-7.5-03 ERDS:n yksityistä allekirjoitusavainta on säilytettävä ja käytettävä suojatussa salauslaitteessa, joka on seuraavien mukaisesti sertifioitu luotettava järjestelmä:

a) tietoteknologian turvallisuuden arviointia koskevat yhteiset kriteerit, sellaisina kuin ne on esitetty standardissa ISO/IEC 15408 [6] tai asiakirjassa ”Common Criteria for Information Technology Security Evaluation”, versio CC:2002, osat 1–5, jotka yhteisten kriteerien mukaisten sertifikaattien tunnustamista tietotekniikan turvallisuuden alalla koskevan järjestelyn (Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security) osallistujat ovat julkaisseet ja jotka on sertifioitu vähintään tasolle EAL 4; tai

b) yhteisiin kriteereihin perustuva eurooppalainen kyberturvallisuuden sertifiointijärjestelmä (EUCC) [7][8], joka on sertifioitu vähintään tasolle EAL 4; tai

c) 31.12.2030 saakka FIPS PUB 140-3 [9] taso 3.

Sertifioinnin on koskettava turvatavoitetta tai suojausprofiilia tai moduulin suunnittelua ja turva-asiakirjoja, jotka täyttävät tämän asiakirjan vaatimukset, riskianalyysin perusteella ja ottaen huomioon fyysiset ja muut ei-tekniset turvatoimenpiteet.

Jos suojatulla salauslaitteella on EUCC [7][8]-sertifiointi, laite on konfiguroitava ja sitä on käytettävä kyseisen sertifioinnin mukaisesti.

11) 7.8 Verkkoturvallisuus

— REQ-ERDSP-7.8-04 ERDSP:n on käytettävä viimeisintä kehitystä edustavia protokollia ja algoritmeja kuljetuskerroksen tasolla tapahtuvassa salauksessa Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [5] mukaisesti.

— REQ-ERDSP-7.8-06 Standardin ETSI EN 319 401 [1] kohdassa REQ-7.8-13 edellytetty haavoittuvuuskartoitus on tehtävä vähintään neljännesvuosittain.

— REQ-ERDSP-7.8-07 Standardin ETSI EN 319 401 [1] kohdassa REQ-7.8-17X edellytetty tunkeutumistesti on tehtävä vähintään neljännesvuosittain.

— REQ-ERDSP-7.8-08 Palomuurit on konfiguroitava siten, että estetään kaikki protokollat ja liittymät, joita ei tarvita TSP:n toiminnassa.

12) 7.12 ERDSP:n toiminnan lopettaminen ja lopettamissuunnitelmat

— REQ-ERDS-7.12-03 ERDSP:n toiminnan lopettamissuunnitelman on oltava asetuksen (EU) N:o 910/2014 [i.1] 24 artiklan 5 kohdan nojalla hyväksytyissä täytäntöönpanosäädöksissä vahvistettujen vaatimusten mukainen.

13) 7.14 Toimitusketju

— REQ-ERDS-7.14-01 Sovelletaan standardin ETSI EN 319 401 [1] lausekkeessa 7.14 määriteltyjä vaatimuksia.

LIITE II

Luettelo 2 artiklassa tarkoitetuista viitestandardeista ja eritelmistä

Sovelletaan standardeja 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') ja ETSI EN 319 522-4-3 V1.1.1 (2018-09) ('ETSI EN 319 522-4-3').