Euroopan unionin
virallinen lehti

FI
L-sarja

2025/2531

17.12.2025

KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2025/2531,

annettu 16 päivänä joulukuuta 2025,

Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 soveltamissäännöistä hyväksyttyjä sähköisiä tilikirjoja koskevien viitestandardien ja eritelmien osalta

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 45 l artiklan 3 kohdan,

sekä katsoo seuraavaa:

(1) Euroopan parlamentin ja neuvoston asetuksella (EU) 2024/1183 ([2]) asetukseen (EU) N:o 910/2014 lisättiin luettelo uusista luottamuspalveluista ja hyväksytyistä luottamuspalveluista, mukaan lukien sähköisten tietojen tallentaminen hyväksyttyyn sähköiseen tilikirjaan. Komission on määrä laatia luettelo tällaisia palveluja koskevista viitestandardeista ja tarvittaessa niitä koskevat eritelmät.

(2) Sähköisellä tilikirjalla tarkoitetaan sähköisten tietueiden sarjaa, jolla varmistetaan kyseisten tietueiden eheys ja kyseisten tietueiden kronologisen järjestyksen oikeellisuus. Sen varmistamiseksi, että tietojen tallentaminen hyväksyttyyn sähköiseen tilikirjaan tapahtuu kronologisessa järjestyksessä, johdonmukaisesti ja luotettavasti, on tarpeen vahvistaa yhteiset eritelmät sähköisten tietojen tallentamiselle hyväksyttyyn sähköiseen tilikirjaan.

(3) Asetuksen (EU) N:o 910/2014 45 l artiklan 2 kohdassa säädettyä vaatimustenmukaisuusolettamaa olisi sovellettava ainoastaan, jos sähköisten tietojen tallentamista hyväksyttyyn sähköiseen tilikirjaan koskevat 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.

(4) 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.

(5) Komissio arvioi säännöllisesti uusia teknologioita, käytäntöjä, standardeja tai teknisiä eritelmiä. Asetuksen (EU) 2024/1183 johdanto-osan 75 kappaleen mukaan komission olisi tarkasteltava uudelleen ja tarvittaessa päivitettävä tätä asetusta sen pitämiseksi maailmanlaajuisen kehityksen ja uusien teknologioiden, käytäntöjen, 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) 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]), ottaen huomioon myös Euroopan tietosuojaneuvoston ohjeet 02/2025 henkilötietojen käsittelystä lohkoketjuteknologian avulla ([5]).

(7) Euroopan tietosuojavaltuutettua on kuultu Euroopan parlamentin ja neuvoston asetuksen (EU) 2018/1725 ([6]) 42 artiklan 1 kohdan mukaisesti, ja hän antoi lausuntonsa 21 päivänä lokakuuta 2025 ([7]).

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

ON HYVÄKSYNYT TÄMÄN ASETUKSEN:

1 artikla

Viitestandardit ja eritelmät

Asetuksen (EU) N:o 910/2014 45 l artiklan 3 kohdassa tarkoitetut hyväksyttyjä sähköisiä tilikirjoja koskevat viitestandardit ja eritelmät esitetään tämän asetuksen liitteessä.

2 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 16 päivänä joulukuuta 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]) edpb_guidelines_202502_blockchain_en.pdf.

([6]) 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).

([7]) EDPS Formal comments on the draft Implementing Regulation laying down rules for the application of Regulation (EU) No 910/2014 as regards reference standards and specifications for qualified electronic ledgers.

LIITE

Luettelo hyväksyttyjen hajautettujen sähköisten tilikirjojen teknisistä eritelmistä ja viitestandardeista

1. Tässä asetuksessa tarkoitetaan:

   a) 'lopullisuudella' sähköisen tilikirjan tietueen tilaa, jossa siitä on tullut peruuttamaton eikä sitä voida muuttaa tai poistaa;

   b) 'hajautetulla sähköisellä tilikirjalla' sähköistä tilikirjaa, joka jaetaan joukolle hajautetun sähköisen tilikirjan solmuja ja joka synkronoidaan hajautetun sähköisen tilikirjan solmujen välillä konsensusmekanismia käyttäen;

   c) 'hajautetun sähköisen tilikirjan solmulla' laitetta tai prosessia, joka on osa hajautetun sähköisen tilikirjan verkkoa ja joka tallentaa täydellisen tai osittaisen kopion sähköisen tilikirjan tietueista;

   d) 'hajautetun sähköisen tilikirjan verkolla' hajautetun sähköisen tilikirjan solmujen verkostoa, joka muodostaa hajautetun sähköisen tilikirjan järjestelmän;

   e) 'hajautetun sähköisen tilikirjan järjestelmällä' järjestelmää, joka toteuttaa hajautetun sähköisen tilikirjan;

   f) 'konsensuksella' hajautetun sähköisen tilikirjan solmujen välistä yhteisymmärrystä transaktioiden pätevyydestä ja johdonmukaisen ja järjestetyn validoitujen transaktioiden sarjan ylläpitämisestä hajautetun sähköisen tilikirjan järjestelmässä;

   g) 'konsensusmekanismilla' sääntöjä ja menettelyjä, joiden avulla saavutetaan yhteisymmärrys;

   h) 'hallintosäännöillä' protokollia, politiikkoja ja mekanismeja, jotka määräävät, miten hajautetun sähköisen tilikirjan järjestelmä toimii, miten tiedot validoidaan ja lisätään sähköiseen tilikirjaan ja miten osallistujat ovat vuorovaikutuksessa;

   i) 'transaktiolla' sähköisen tilikirjan työprosessin pienintä yksikköä;

   j) 'työprosessilla' yhtä tai useampaa toimintosarjaa, joka tarvitaan sähköisen tilikirjan hallintosääntöjen mukaisen lopputuloksen aikaansaamiseksi;

   k) 'validoidulla transaktiolla' transaktiota, jonka osalta vaadittu eheys, aitous ja protokollakohtaiset ehdot on tarkastettu hajautetun sähköisen tilikirjan järjestelmän hallintosääntöjen mukaisesti;

   l) 'salauslinkillä' viittausta tietoihin, jotka on luotu sopivilla salaustekniikoilla viitattujen tietojen eheyden, aitouden tai jäljitettävyyden sekä tietueiden oikean järjestyksen varmistamiseksi;

   m) 'tilikirjaraportilla' sähköisen tilikirjan tietueista poimittujen todennettavissa olevien tietojen jäsenneltyä esitystä, jossa annetaan tietoja tietyistä toimista, tiloista tai ennalta määriteltyjen sääntöjen noudattamisesta;

   n) 'hyväksytyn sähköisen tilikirjan tarjoajalla' hyväksyttyä luottamuspalvelun tarjoajaa, joka tarjoaa hyväksyttyä luottamuspalvelua, joka koostuu tietojen tallentamisesta hyväksyttyyn sähköiseen tilikirjaan;

   o) 'hyväksytyllä hajautetulla sähköisellä tilikirjalla' hajautettua sähköistä tilikirjaa, joka täyttää hyväksytyn sähköisen tilikirjan vaatimukset.

2. Jos hyväksytyn luottamuspalvelun tarjoajan on laadittava tilikirjaraportti, se on laadittava automaattisesti.

3. Hyväksyttyjen sähköisten tilikirjojen tarjoajien on luotava hyväksytty sähköinen tilikirjaa, tallennettava siihen sähköisiä tietoja ja päivitettävä ja ylläpidettävä sitä seuraavissa vahvistettujen eritelmien mukaisesti:

   a) Kaikkien hyväksyttyjen sähköisten tilikirjojen tarjoajien osalta standardi ETSI EN 319 401 v3.1.1 (2024–06) seuraavin mukautuksin:

      — 2.1 Velvoittavat viittaukset

        [1] Euroopan kyberturvallisuuden sertifiointiryhmä, Salausta käsittelevä alaryhmä: Euroopan verkko- ja tietoturvaviraston (ENISA) julkaisema asiakirja "Agreed Cryptographic Mechanisms".

[2] IETF RFC 7515 (May 2015): ”JSON Web Signature (JWS)”.

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

[4] Komission täytäntöönpanoasetus (EU) 2024/482, annettu 31 päivänä tammikuuta 2024, Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 soveltamissäännöistä siltä osin kuin on kyse yhteisiin kriteereihin perustuvan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän (EUCC) hyväksymisestä.

[5] Komission täytäntöönpanoasetus (EU) 2024/3144, annettu 18 päivänä joulukuuta 2024, täytäntöönpanoasetuksen (EU) 2024/482 muuttamisesta sovellettavien kansainvälisten standardien osalta ja kyseisen täytäntöönpanoasetuksen oikaisemisesta.

[6] ISO/IEC 15408:2022 (osat 1–5): ”Information security, cybersecurity and privacy protection – Evaluation criteria for IT security”.

— 6.1 Luottamuspalvelun käytäntöselostus:

  — REQ-6.1–12 Sähköisen tilikirjan käytäntöselostukseen on sisällyttävä vähintään seuraavat tiedot:

    — sähköisen tilikirjan alustan toiminnalliset ja tekniset valmiudet ja sen käyttö koko sen ajan, kun tietojen tallentamista hyväksyttyyn sähköiseen tilikirjaan tarjotaan hyväksyttynä luottamuspalveluna;

    — palvelun tarjoamisen yhteydessä käytetyt erityiset tietojen alkuperän todentamismekanismit;

    — palvelun tarjoamisen yhteydessä käytetyt erityiset kronologiseen järjestykseen asettamisen mekanismit;

    — tarvittaessa tietueiden järjestyksen varmistamiseen käytetty salauslinkki;

    — tarvittaessa konsensusmekanismi, jolla varmistetaan tilikirjaan tallennettujen tietueiden ja transaktioiden lopullisuus ja eheys, mukaan lukien mahdollinen varoaika, kunnes lopullisuus ja eheys on saavutettu;

    — palvelun tarjoamisen yhteydessä käytetyt erityiset tietojen eheyden varmistusmekanismit.

  — 6.2 Ehdot:

    — REQ-6.2–03 Luottamuspalvelua käyttäville tilaajille ja osapuolille on ennen sopimussuhteen solmimista ilmoitettava täsmälliset ehdot selkeästi, kattavasti ja helposti saatavilla olevalla tavalla sekä julkisesti että yksilöllisesti.

  — 6.3 Tietoturvapolitiikka:

    — REQ-6.3–04X Luottamuspalvelun tarjoajan (TSP) on vahvistettava menettelyt, joilla valvontaelimelle ilmoitetaan kaikista muutoksista luottamuspalvelun tarjoamisessa, liiketoimintavaatimusten ja asiaankuuluvien lakien ja asetusten mukaisesti. TSP:n on ilmoitettava valvontaelimelle vähintään

      — kuukautta ennen muutoksen toteuttamista;

      — kolme kuukautta ennen luottamuspalvelun tarjoamisen suunniteltua lopettamista.

  — 7.2 Henkilöresurssit:

    — REQ-7.2–04X TSP: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-7.2–05X Tähän on sisällyttävä säännöllisesti (vähintään 12 kuukauden välein) tehtäviä päivityksiä uusista uhkista ja nykyisistä turvakäytännöistä.

— 7.5 Salaustekniikka koskevat tarkastukset:

— REQ-7.5–01X Salausavaimien, salausalgoritmien ja salauslaitteiden hallintaa varten on oltava käytössä asianmukaisia turvatarkastuksia niiden koko elinkaaren ajan, tarvittaessa kryptoketteryyteen perustuvaa lähestymistapaa noudattaen.

— REQ-7.5–02 TSP:n on valittava ja käytettävä luottamuspalvelujensa tarjoamista varten sopivia salaustekniikoita, jotka ovat Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [1] mukaisia.

Erityisesti:

— REQ-7.5–03 Hyväksyttyjen sähköisten tilikirjojen tarjoajien on vahvistettava sähköiseen tilikirjaan tallennettujen tietueiden alkuperä. Tässä yhteydessä niiden on käytettävä palvelun käyttäjien luomiin hyväksyttyihin varmenteisiin perustuvia kehittyneitä sähköisiä allekirjoituksia tai hyväksyttyihin varmenteisiin perustuvia kehittyneitä sähköisiä leimoja seuraavien standardien ja eritelmien mukaisesti:

a) ETSI EN 319 122–1 V1.3.1 (2023–06). ”Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures”

b) ETSI EN 319 132–1 V1.3.1 (2024–07). ”Electronic Signatures and Trust Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures”

c) ETSI TS 119 182–1 V1.2.1 (2024–07). ”Electronic Signatures and Trust Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures”, seuraavin mukautuksin:

— 5.1.8 x5c-otsikkoparametri (X.509 Varmenneketju)

— JAdES-allekirjoituksessa on oltava IETF RFC 7515:n [2] lausekkeessa 4.1.6 määritelty x5c-otsikkoparametri joko allekirjoitettuna tai allekirjoittamattomana otsikkoparametrina.

— x5c-otsikkoparametrilla on oltava IETF RFC 7515:n [2] lausekkeen 4.1.6 mukainen semantiikka.

— x5c-otsikkoparametrilla on oltava IETF RFC 7515:n [2] lausekkeen 4.1.6 mukainen syntaksi.

— REQ-7.5–04 Hyväksyttyjen sähköisten tilikirjojen tarjoajien on varmistettava sähköiseen tilikirjaan tallennettujen tietueiden yksilöllinen peräkkäinen kronologinen järjestys. Tässä yhteydessä niiden on käytettävä salauslinkkejä, jotka perustuvat hash-luetteloihin tai -puihin, käyttäen kryptografisia tiivistefunktioita seuraavien eritelmien ja standardien mukaisesti:

a) ulostulon tiivistekoko SHA-256 tai suurempi Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [1] mukaisesti;

b) ulostulon tiivistekoko SHA3-256 tai suurempi Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [1] mukaisesti.

Vaihtoehtoisesti hyväksyttyjen sähköisten tilikirjojen tarjoajien on käytettävä hyväksyttyjä aikaleimoja, kun ne käyttävät ajantallennusta varmistaakseen sähköisen tilikirjan tietueiden yksilöllisen peräkkäisen kronologisen järjestyksen.

— REQ-7.5–05 Hyväksyttyjen sähköisten tilikirjojen tarjoajien on varmistettava sähköiseen tilikirjaan tallennettujen tietueiden eheys. Tässä yhteydessä niiden on käytettävä hyväksyttyihin varmenteisiin perustuvia kehittyneitä sähköisiä allekirjoituksia tai hyväksyttyihin varmenteisiin perustuvia kehittyneitä sähköisiä leimoja seuraavien standardien ja eritelmien mukaisesti:

  a) kaikki allekirjoitus- tai leimamuodot, jotka ovat Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [1] mukaisia;

  b) ulostulon tiivistekoko SHA-256 tai suurempi Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [1] mukaisesti;

  c) ulostulon tiivistekoko SHA3-256 tai suurempi Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [1] mukaisesti.

  d) Hyväksyttyjen sähköisten tilikirjojen tarjoajien on varmistettava, että hyväksyttyyn sähköiseen tilikirjaan tallennettujen tietueiden mahdollinen myöhempi muuttaminen voidaan havaita välittömästi.

— REQ-7.5–06 Kun käytetään digitaalisia allekirjoitusmekanismeja, hyväksytyn sähköisen tilikirjan tarjoajan 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 ([1]) [6] tai asiakirjassa ”Common Criteria for Information Technology Security Evaluation”, versio CC:2022, 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) ([2]) ([3]), [4][5], joka on sertifioitu vähintään tasolle EAL 4; tai

  c) 31.12.2030 saakka FIPS PUB 140–3 ([4]) [3] 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-sertifiointi [4][5], laite on konfiguroitava ja sitä on käytettävä kyseisen sertifioinnin mukaisesti.

([1]) ISO/IEC 15408:2022 (osat 1–5): ”Information security, cybersecurity and privacy protection – Evaluation criteria for IT security”.

([2]) Komission täytäntöönpanoasetus (EU) 2024/482, annettu 31 päivänä tammikuuta 2024, Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 soveltamissäännöistä siltä osin kuin on kyse yhteisiin kriteereihin perustuvan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän (EUCC) hyväksymisestä (EUVL L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/2025-01-08).

([3]) Komission täytäntöönpanoasetus (EU) 2024/3144, annettu 18 päivänä joulukuuta 2024, täytäntöönpanoasetuksen (EU) 2024/482 muuttamisesta sovellettavien kansainvälisten standardien osalta ja kyseisen täytäntöönpanoasetuksen oikaisemisesta (EUVL 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

([4]) FIPS PUB 140–3 (2019): ”Security Requirements for Cryptographic Modules”.

— 7.8 Verkkoturvallisuus:

— REQ-7.8–14X Kohdassa REQ-7.8–13 edellytetty haavoittuvuuskartoitus on tehtävä vähintään neljännesvuosittain.

— REQ-7.8–18X Kohdassa REQ-7.8–17X edellytetty tunkeutumistesti on tehtävä vähintään neljännesvuosittain.

— REQ-7.8–21X Palomuurit on myös konfiguroitava siten, että estetään kaikki protokollat ja liittymät, joita ei tarvita TSP:n toiminnassa.

— 7.9.1 Seuranta ja kirjaaminen:

— REQ-7.9.1–02X Seurantatoimissa on otettava huomioon kerättyjen tai analysoitujen tietojen arkaluonteisuus.

— 7.12 TSP:n toiminnan lopettaminen ja lopettamissuunnitelmat

— REQ-7.12–02A TSP:n toiminnan lopettamissuunnitelman on oltava asetuksen (EU) N:o 910/2014 [i.1] 24 artiklan 5 kohdan nojalla hyväksytyissä täytäntöönpanosäädöksissä vahvistettujen vaatimusten mukainen.

b) Lisäksi kaikkien hajautetun sähköisen tilikirjan teknologiaa käyttävien hyväksyttyjen sähköisten tilikirjojen tarjoajien osalta:

1) ISO 23257:2022 ”Blockchain and distributed ledger technologies – Reference architecture”, lauseke 9, jossa esitetään täydellinen kuvaus hajautetun sähköisen tilikirjan teknologiajärjestelmästä, vastaavasta hajautetun sähköisen tilikirjan teknologiaverkosta ja hajautetun sähköisen tilikirjan teknologiasolmuista;

2) ISO 23635:2022 ”Blockchain and distributed ledger technologies – Guidelines for governance”, siltä osin kuin on kyse niiden tarjoaman sähköisen tilikirjan palvelun hallintorakenteeseen liittyvistä kirjallisista ja julkisesti saatavilla olevista politiikoista ja käytännöistä.