Euroopan unionin
virallinen lehti

FI
L-sarja

2025/2532

17.12.2025

KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2025/2532,

annettu 16 päivänä joulukuuta 2025,

Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 soveltamissäännöistä hyväksyttyjä sähköisiä arkistointipalveluja 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 j artiklan 2 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 hyväksytty sähköinen arkistointipalvelu. Komission on määrä laatia luettelo tällaisia palveluja koskevista viitestandardeista ja tarvittaessa niitä koskevat eritelmät.

2) Sähköisellä arkistoinnilla tarkoitetaan palvelua, jossa vastaanotetaan, tallennetaan, haetaan ja poistetaan sähköisiä tietoja ja sähköisiä asiakirjoja, jotta voidaan varmistaa niiden pysyvyys ja luettavuus sekä säilyttää niiden eheys ja luottamuksellisuus ja todistus alkuperästä koko säilytysajan. Hyväksytyillä sähköisillä arkistointipalveluilla on keskeinen rooli digitaalisessa liiketoimintaympäristössä, sillä ne edistävät siirtymistä perinteisistä paperipohjaisista prosesseista vastaaviin sähköisiin prosesseihin. Sen varmistamiseksi, että olettamus sähköisten tietojen ja sähköisten asiakirjojen eheydestä ja alkuperästä säilyy koko sen ajan, jonka hyväksytty luottamuspalvelun tarjoaja säilyttää niitä, ja jotta voidaan saavuttaa korkea läpinäkyvyyden ja luottamuksen taso kaikkien tietojen elinkaaren osallistuvien osapuolten keskuudessa, on tarpeen vahvistaa hyväksyttyjä sähköisiä arkistointipalveluja koskevat yhteiset eritelmät.

3) Hyväksyttyjen sähköisten arkistointipalvelujen todistusarvon, turvallisuuden ja luotettavuuden lisäämiseksi olisi käytettävä hyväksyttyjä luottamuspalveluja, jos sähköisiä allekirjoituksia, sähköisiä leimoja tai sähköisiä aikaleimoja käytetään esimerkiksi arkistointitodisteiden, todisterekisterien, tapahtumarekisterien, menettelyjen moitteetonta toteuttamista koskevien tietojen tai arkistoinnin vahvistusraporttien luomiseen, allekirjoittamiseen, leimaamiseen tai päivämäärän ja kellonajan todistamiseen.

4) Asetuksen (EU) N:o 910/2014 45 j artiklan 2 kohdassa säädettyä vaatimustenmukaisuusolettamaa olisi sovellettava ainoastaan, jos hyväksytyt sähköiset arkistointipalvelut ovat tässä asetuksessa vahvistettujen vaatimusten mukaisia. Hyväksyttyjä sähköisiä arkistointipalveluja koskevien viitestandardien olisi heijastettava vakiintuneita käytäntöjä, ja niiden olisi oltava laajasti tunnustettuja kyseessä olevilla aloilla. Niitä olisi mukautettava siten, että niihin sisällytetään lisätarkastuksia, joilla varmistetaan hyväksyttyjen sähköisten arkistointipalvelujen turvallisuus ja luotettavuus.

5) Jos luottamuspalvelun tarjoaja noudattaa tässä asetuksessa 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.

6) Jotta voidaan säilyttää yhden tai useamman hyväksytyn sähköisen allekirjoituksen tai leiman sisältävien sähköisten tietojen ja sähköisten asiakirjojen eheys ja todistus niiden alkuperästä, hyväksyttyjen sähköisten arkistointipalvelujen olisi käytettävä menettelyjä ja teknologioita, joilla näiden sähköisten allekirjoitusten ja leimojen luotettavuutta voidaan jatkaa teknologisen luotettavuusajan jälkeen ainakin koko säilytysajan.

([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).

7) 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.

8) 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]).

9) Euroopan tietosuojavaltuutettua on kuultu Euroopan parlamentin ja neuvoston asetuksen (EU) 2018/1725 ([5]) 42 artiklan 1 kohdan mukaisesti, ja hän antoi lausuntonsa 21 päivänä lokakuuta 2025 ([6]).

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

ON HYVÄKSYNYT TÄMÄN ASETUKSEN:

1 artikla

Hyväksytyllä sähköisellä allekirjoituksella tai hyväksytyllä sähköisellä leimalla varustettujen asiakirjojen sähköinen arkistointi

1. Kun arkistoidaan sähköisiä tietoja tai sähköisiä asiakirjoja, jotka sisältävät hyväksyttyjä sähköisiä allekirjoituksia tai hyväksyttyjä sähköisiä leimoja, hyväksyttyjen sähköisten arkistointipalvelujen tarjoajien on varmistettava, että kyseisten hyväksyttyjen sähköisten allekirjoitusten tai hyväksyttyjen sähköisten leimojen luotettavuus säilytetään, myös niiden teknologisen luotettavuusajan jälkeen, ja että hyväksyttyjen sähköisten allekirjoitusten ja leimojen eheys ja niiden alkuperän virheettömyys säilytetään ainakin koko lakisääteisen tai sopimusperusteisen säilytysajan päättymiseen saakka.

2. Edellä olevan 1 kohdan soveltamiseksi hyväksyttyjen sähköisten arkistopalvelujen tarjoajat voivat käyttää hyväksyttyjen sähköisten allekirjoitusten hyväksyttyä säilyttämispalvelua tai hyväksyttyjen sähköisten leimojen hyväksyttyä säilyttämispalvelua.

2 artikla

Viitestandardit ja eritelmät hyväksyttyjen sähköisten arkistointipalvelujen tarjoamista varten

Asetuksen (EU) N:o 910/2014 45 j artiklan 2 kohdassa tarkoitetut viitestandardit ja eritelmät esitetään tämän asetuksen liitteessä.

([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).

([6]) 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 archiving services.

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 16 päivänä joulukuuta 2025.

Komission puolesta
Puheenjohtaja
Ursula VON DER LEYEN

LIITE

Luettelo hyväksyttyjen sähköisten arkistointipalvelujen viitestandardeista ja eritelmistä

Standardia CEN/TS 18170:2025 (’CEN/TS 18170’) sovelletaan seuraavin mukautuksin:

a) Velvoittavat viittaukset (lauseke 2)

— ETSI EN 319 401 V3.1.1 (2024–06), Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers

— ETSI EN 319 421 V1.3.1 (2025–07), Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

— ISO 14721:2025, Space Data System Practices – Reference model for an open archival information system (OAIS)

— ACM-ECCG, Euroopan kyberturvallisuuden sertifiointiryhmä, Salausta käsittelevä alaryhmä: Euroopan kyberturvallisuusviraston (ENISA) julkaisema asiakirja ”Agreed Cryptographic Mechanisms”

— CIR (EU) 2024/482, Komission täytäntöönpanoasetus (EU) 2024/482 ([1]).

— CIR (EU) 2024/3144, Komission täytäntöönpanoasetus (EU) 2024/3144 ([2]).

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

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

b) Politiikka ja käytäntöselostus (lauseke 6.1)

— Sovelletaan standardin CEN/TS 18170 lausekkeen 6.1 vaatimuksia.

— Sovelletaan standardin ETSI EN 319 401 lausekkeen 5 vaatimuksia.

— Sähköisen arkistoinnin luottamuspalvelun tarjoajan (EATSP) on vahvistettava menettelyt, joilla valvontaelimelle ilmoitetaan kaikista muutoksista sähköisen arkistoinnin luottamuspalvelun tarjoamisessa ja aikomuksesta lopettaa kyseinen toiminta, liiketoimintavaatimusten ja asiaankuuluvien lakien ja asetusten mukaisesti, myös asetuksen (EU) N:o 910/2014 [i.2] 24 artiklan 5 kohdan nojalla hyväksyttyjen täytäntöönpanosäädösten vaatimusten mukaisesti.

— EATSP:n on ilmoitettava toimivaltaiselle valvontaelimelle vähintään

  — kuukautta ennen muutoksen toteuttamista;

  — kolme kuukautta ennen luottamuspalvelun tarjoamisen suunniteltua lopettamista.

c) Ehdot (lauseke 6.2)

— Sovelletaan standardin CEN/TS 18170 lausekkeen 6.2 vaatimuksia.

— Sähköisen arkistoinnin luottamuspalvelua käyttäville tilaajille ja osapuolille on ennen sopimussuhteen solmimista ilmoitettava täsmälliset ehdot selkeästi, kattavasti ja helposti saatavilla olevalla tavalla sekä julkisesti että yksilöllisesti.

([1]) 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/oj).

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

d) Henkilöresurssit (lauseke 7.3)

— Sovelletaan standardin CEN/TS 18170 lausekkeen 7.3 vaatimuksia.

— EATSP:n luotetuissa rooleissa olevan henkilöstön ja tarvittaessa luotetuissa rooleissa olevien alihankkijoiden, on pystyttävä täyttämään vaatimus, joka koskee ”asiantuntemusta, kokemusta ja pätevyyttä”, joka on osoitettu virallisen koulutuksen ja suositusten, työkokemuksen tai näiden yhdistelmän kautta. Tähän on sisällyttävä säännöllisesti (vähintään 12 kuukauden välein) tehtäviä päivityksiä uusista uhkista ja nykyisistä turvakäytännöistä.

e) Salaustekniikkaa koskevat tarkastukset ja seuranta (lauseke 7.6)

— Arkistointijärjestelmän on taattava tietojen ja asiakirjojen luottamuksellisuus arkiston koko elinkaaren ajan aineiston tallettamisesta sen poistamiseen saakka.

— Sovelletaan standardin ETSI EN 319 401 lausekkeen 7.5 ”Salaustekniikkaa koskevat tarkastukset” vaatimuksia.

— EATSP:n on vahvistettava sähköiseen arkistointijärjestelmään arkistoitavien tietojen alkuperä. Jos se käyttää tätä varten sähköisiä allekirjoituksia tai sähköisiä leimoja, kyseisten sähköisten allekirjoitustent tai sähköisten leimojen on oltava hyväksyttyjä.

— Kun EATSP allekirjoittaa digitaalisesti digitaalisen esineen tai tiedon (tai sen osan), EATSP:n yksityistä allekirjoitusavainta on säilytettävä ja käytettävä joko hyväksytyssä sähköisen allekirjoituksen tai leiman luontivälineessä tai 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 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 (CIR (EU) 2024/482, CIR (EU) 2024/3144), joka on sertifioitu vähintään tasolle EAL 4; tai

  c) 31.12.2030 saakka FIPS PUB 140–3 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 (CIR (EU) 2024/482, CIR (EU) 2024/3144), laite on konfiguroitava ja sitä on käytettävä kyseisen sertifioinnin mukaisesti.

— EATSP:n on seurattava aiemmin käytetyn ja parhaillaan käytössä olevan salausalgoritmin vahvuutta. Jos jonkin käytetyn algoritmin tai parametrin ei enää katsota olevan soveltuva riskinhallinnassa määritellyllä tavalla, EATSP:n on joko päivitettävä asiaan liittyvät arkistointiperiaatteet tai luotava uusi arkistoprofiili AIP:den käsittelyä varten sekä määriteltävä ja toteutettava asianmukaiset toimenpiteet.

— EATSP:n salausalgoritmien ja niiden käytön arviointi on toteutettava Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien mukaisesti (ACM-ECCG).

— EATS:n teknisten komponenttien on todennettava toisensa salaustekniikoiden perusteella ennen lähettämistä.

f) Verkko (lauseke 7.9)

— Sovelletaan standardin ETSI EN 319 401 lausekkeen 7.8 ”Verkkoturvallisuus” vaatimuksia.

— Standardin ETSI EN 319 401 kohdassa REQ-7.8–13 edellytetty haavoittuvuuskartoitus on tehtävä vähintään neljännesvuosittain.

— Standardin ETSI EN 319 401 kohdassa REQ-7.8–17X edellytetty tunkeutumistesti on tehtävä vähintään neljännesvuosittain.

— Palomuurit on konfiguroitava siten, että estetään kaikki protokollat ja liittymät, joita ei tarvita EATSP:n toiminnassa.

g) Todisteiden kerääminen (lauseke 7.11)

— Standardin ETSI EN 319 401 lausekkeen 7.10 ”Todisteiden kerääminen” vaatimuksia sovelletaan myös kriittisiin ja ei-kriittisiin tapahtumiin (ks. lauseke 13.2).

h) EATSP:n toiminnan lopettaminen ja lopettamissuunnitelma (lauseke 7.13)

— Sovelletaan standardin CEN/TS 18170 lausekkeen 7.13 vaatimuksia.

— EATSP:n toiminnan lopettamissuunnitelman on oltava asetuksen (EU) N:o 910/2014 24 artiklan 5 kohdan nojalla hyväksytyissä täytäntöönpanosäädöksissä vahvistettujen vaatimusten mukainen.

i) Luotettava tapahtuma-aika (lauseke 13.3.1)

— Sovelletaan standardin CEN/TS 18170 lausekkeen 13.3.1 vaatimuksia.

— Kun EATSP käyttää aikaleimoja, sen on käytettävä hyväksyttyä aikaleimaa.