Euroopan unionin
virallinen lehti

FI
L-sarja

2025/1946

30.9.2025

KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2025/1946,

annettu 29 päivänä syyskuuta 2025,

Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 soveltamissäännöistä hyväksyttyjen sähköisten allekirjoitusten ja hyväksyttyjen sähköisten leimojen hyväksyttyjen säilyttämispalvelujen 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 34 artiklan 2 kohdan ja 40 artiklan,

sekä katsoo seuraavaa:

(1) Hyväksyttyjen sähköisten allekirjoitusten ja hyväksyttyjen sähköisten leimojen hyväksytyillä säilyttämispalveluilla varmistetaan kyseisten sähköisten allekirjoitusten ja sähköisten leimojen säilyttämistodisteiden pitkän aikavälin eheys, aitous, olemassaolon todistaminen ja käytettävyys. Tämä mahdollistaa niiden oikeudellisen pätevyyden osoittamisen pitkällä aikavälillä ja takaa, että ne voidaan validoida tulevista teknologisista muutoksista riippumatta. Näitä palveluja tarjotaan itsenäisesti tai osana toista hyväksyttyä luottamuspalvelua, kuten hyväksyttyä sähköistä arkistointipalvelua.

(2) Asetuksen (EU) N:o 910/2014 34 artiklan 1 a kohdassa ja 40 artiklassa säädettyä vaatimustenmukaisuusolettamaa olisi sovellettava ainoastaan, jos hyväksyttyjen sähköisten allekirjoitusten ja hyväksyttyjen sähköisten leimojen hyväksytyt säilyttämispalvelut 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 sekä mahdollisuus tarkistaa allekirjoitusten ja leimojen hyväksytty asema ja tekninen pätevyys ajan mittaan.

(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) 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).

(5) 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]).

(6) 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.

(7) 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 (EY) N:o 910/2014 34 artiklan 2 kohdassa ja 40 artiklassa tarkoitetut 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 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

Luettelo 2 artiklassa tarkoitetuista viitestandardeista ja eritelmistä

Standardeja ETSI TS 119 511 V1.1.1 (2019-06) ('ETSI TS 119 511') ja ETSI TS 119 172-4 V1.1.1 (2021-05) ('ETSI TS 119 172-4') sovelletaan seuraavin mukautuksin:

1. ETSI TS 119 511

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 TS 119 612 (V2.3.1) "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

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

— [6] Komission täytäntöönpanoasetus (EU) 2024/482 ([1]) Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 soveltamissäännöistä siltä osin kuin on kyse yhteisiin kriteereihin perustuvan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän (EUCC) hyväksymisestä.

— [7] Komission täytäntöönpanoasetus (EU) 2024/3144 ([2]) täytäntöönpanoasetuksen (EU) 2024/482 muuttamisesta sovellettavien kansainvälisten standardien osalta ja kyseisen täytäntöönpanoasetuksen oikaisemisesta.

— [8] Euroopan kyberturvallisuuden sertifiointiryhmä, Salausta käsittelevä alaryhmä: Euroopan kyberturvallisuusviraston (ENISA) julkaisema asiakirja "Agreed Cryptographic Mechanisms" ([3]).

— [9] ETSI TS 119 172-4 V1.1.1 (2021-05) "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists".

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

2) 3.1 Käsitteet

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

3) 6.4 Säilyttämisprofiilit

— OVR-6.4-08A [WTS][WOS] Todisteiden odotetun keston on oltava Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [8] mukainen.

— HUOMAUTUS 3 Tyhjä.

4) 6.5 Säilyttämistodistepolitiikka

— OVR-6.5-04A Käytettyjen salausalgoritmien on oltava Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [8] mukaisia.

— HUOMAUTUS 1 Tyhjä.

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

5) 7.2 Henkilöresurssit

— OVR-7.2-02 Säilyttämispalvelun tarjoajan (PSP) 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.

— OVR-7.2-03 Kohdan OVR-7.2-02 noudattamiseen on sisällyttävä säännöllisesti (vähintään 12 kuukauden välein) tehtäviä päivityksiä uusista uhkista ja nykyisistä turvakäytännöistä.

6) 7.5 Salaustekniikka koskevat tarkastukset

— OVR-7.5-05 [EHDOLLINEN] Kun PSP allekirjoittaa säilyttämistodisteen (tai sen osan), PSP: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 [10] 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) EUCC [6][7], ja sertifioitu vähintään tasolle EAL 4; tai

c) 31.12.2030 saakka FIPS PUB 140-3 [5] 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 [6][7]-sertifiointi, laite on konfiguroitava ja sitä on käytettävä kyseisen sertifioinnin mukaisesti.

— OVR-7.5-06 [EHDOLLINEN] Tyhjä.

— OVR-7.5-07 [EHDOLLINEN] Kun PSP allekirjoittaa säilyttämistodisteen (tai sen osan), kaikki PSP:n yksityisten allekirjoitusavainten varmuuskopiot on suojattava suojatulla salauslaitteella niiden eheyden ja luottamuksellisuuden varmistamiseksi ennen niiden tallentamista kyseisen laitteen ulkopuolelle.

— OVR-7.5-08 PSP:n yksityisen allekirjoitusavaimen saa viedä ja tuoda toiseen suojattuun salauslaitteeseen ainoastaan, jos kyseinen vienti ja tuonti toteutetaan turvallisesti ja kyseisten laitteiden sertifioinnin mukaisesti.

7) 7.8 Verkkoturvallisuus

— OVR-7.8-03 Standardin ETSI EN 319 401 [1] kohdassa REQ-7.8-13 edellytetty haavoittuvuus-kartoitus on tehtävä vähintään neljännesvuosittain.

— OVR-7.8-04 Standardin ETSI EN 319 401 [1] kohdassa REQ-7.8-17X edellytetty tunkeutumistesti on tehtävä vähintään neljännesvuosittain.

— OVR-7.8-05 Palomuurit on konfiguroitava siten, että estetään kaikki protokollat ja liittymät, joita ei tarvita PSP:n toiminnassa.

8) 7.14 Salaustekniikkaa koskeva seuranta

— OVR-7.14-03A Kohdissa OVR-7.14.01 ja OVR-7.14.02 tarkoitettu salausalgoritmien arviointi on toteutettava Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [8] mukaisesti.

— HUOMAUTUS Tyhjä.

9) 7.12 TSP:n toiminnan lopettaminen ja lopettamissuunnitelmat

— OVR-7.12-01A TSP:n toiminnan lopettamissuunnitelman on oltava asetuksen (EU) N:o 910/2014 [i.2] 24 artiklan 5 kohdan nojalla hyväksytyissä täytäntöönpanosäädöksissä vahvistettujen vaatimusten mukainen.

10) 7.17 Toimitusketju

— OVR-7.17-01 Sovelletaan standardin ETSI EN 319 401 [1] lausekkeessa 7.14 määriteltyjä vaatimuksia.

11) Liite A (velvoittava): Asetuksen (EU) N:o 910/2014 34 artiklassa määritelty QES:n hyväksytty säilyttämispalvelu

— OVR-A-02 [PDS][PDS+PGD]

a) säilyttämispalvelun on säilytettävä kaikki sähköisen allekirjoituksen tai leiman hyväksytyn tilan tarkistamiseen tarvittavat tiedot, jotka eivät olisi julkisesti saatavilla, säilytysajan päättymiseen saakka;

b) säilyttämispalvelun on varmistettava, että säilytetyt tiedot ovat milloin tahansa säilytysajan aikana sellaiset, että kun ne annetaan syöttötietoina standardin ETSI 119 172-4 [9] lausekkeessa 4.4 määriteltyyn prosessiin, prosessin tulos määrittää selkeästi, oliko digitaalinen allekirjoitus tai leima sen säilyttämishetkellä teknisesti soveltuva toteuttamaan EU:n hyväksytyn sähköisen allekirjoituksen tai EU:n hyväksytyn sähköisen leiman.

— OVR-A-03 [PDS][PDS+PGD] Säilyttämistodisteissa käytettyjen aikaleimojen on oltava asetuksen (EU) N:o 910/2014 [i.2] mukaisia hyväksyttyjä aikaleimoja.

2. ETSI TS 119 172-4

1) 2.1 Velvoittavat viittaukset

— [1] ETSI EN 319 102-1 V1.4.1 (2024-06) "Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

— Kaikkia viittauksia standardiin "ETSI TS 119 102-1 [1]" pidetään viittauksina standardiin "ETSI EN 319 102-1 [1]".

— [2] ETSI TS 119 612 (V2.3.1) "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

— [13] ETSI TS 119 101 V1.1.1 (2016-03) "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation".

2) 4.2 Validointirajoitukset ja validointimenettelyt, vaatimus REQ-4.2-03, kohta "X.509 Validointirajoitukset", c alakohta:

— i) Jos loppukäyttäjän varmenne muodostaa luottamusankkurin, rajoitusta "RevocationChecking-Constraints" ei käytetä.

— ii) Jos loppukäyttäjän varmenne ei muodosta luottamusankkuria, rajoituksen "RevocationChecking-Constraints" arvoksi asetetaan "eitherCheck", siten kuin määritellään standardin ETSI TS 119 172-1 [3] lausekkeessa A.4.2.1 olevan taulukon A.2 riveillä (m)2.1.

— iii) Jos loppukäyttäjän varmenne muodostaa luottamusankkurin, standardin ETSI TS 119 172-1 [3] lausekkeessa A.4.2.1 olevan taulukon A.2 riveillä (m)2.2 määriteltyä rajoitusta "RevocationFreshness-Constraints" ei käytetä.

— iv) Jos loppukäyttäjän varmenne ei muodosta luottamusankkuria, standardin ETS TS 119 172-1 [3] lausekkeessa A.4.2.1 olevan taulukon A.2 riveillä (m)2.2 määriteltyä rajoitusta ”RevocationFreshness-Constraints” käytetään allekirjoitusvarmenteen osalta enimmäisarvolla 0 varmistaen, että peruutustiedot hyväksytään vain, jos ne on annettu parhaan allekirjoitusajan jälkeen. Rajoitukselle ”RevocationFreshnessConstraints” ei aseteta arvoa muille varmenteille kuin allekirjoitusvarmenteelle, aikaleimaa tukevat varmenteet mukaan luettuina.

3) 4.3 Allekirjoitusten validointia ja sovellettavuutta koskevien sääntöjen tarkastuskäytäntöjä koskevat vaatimukset

— REQ-4.3-02 Allekirjoituksen validointisovellusten on oltava standardin ETSI TS 119 101 [13] mukaisia.

4) 4.4 Teknisen sovellettavuuden (sääntöjen) tarkastusprosessi

— REQ-4.4.2-03 Jos jokin kohdassa REQ-4.4.2–01 määritellyistä tarkastuksista epäonnistuu,

— prosessi pysähtyy;

— allekirjoitus määritellään teknisesti määrittelemättömäksi eli ei EU:n hyväksytyksi sähköiseksi allekirjoitukseksi eikä EU:n hyväksytyksi sähköiseksi leimaksi;

— edellä esitetty tulos ja kaikkien väliprosessien tulokset on otettava huomioon allekirjoituksen sovellettavuussääntöjä koskevassa tarkastusraportissa.