Euroopan unionin
virallinen lehti

FI
L-sarja

2025/1929

30.9.2025

KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2025/1929,

annettu 29 päivänä syyskuuta 2025,

Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 soveltamissäännöistä siltä osin kuin on kyse päivän ja ajankohdan sitomisesta tietoihin ja aikalähteiden virheettömyyden vahvistamisesta hyväksyttyjen sähköisten aikaleimojen myöntämistä varten

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 42 artiklan 2 kohdan,

sekä katsoo seuraavaa:

(1) Hyväksytyillä sähköisillä aikaleimoilla on keskeinen rooli digitaalisessa ympäristössä, sillä ne edistävät siirtymistä perinteisistä paperipohjaisista prosesseista vastaaviin sähköisiin prosesseihin. Hyväksytyt sähköiset aikaleimat sitovat päivää ja ajankohtaa koskevat tiedot sähköisiin tietoihin ja auttavat siten varmistamaan niiden osoittamien päivän ja ajankohdan virheettömyyden ja niiden digitaalisten asiakirjojen eheyden, joihin päivä ja ajankohta on sidottu.

(2) Asetuksen (EU) N:o 910/2014 42 artiklan 1 a kohdassa säädettyä vaatimustenmukaisuusolettamaa olisi sovellettava ainoastaan, jos hyväksyttyjä aikaleimoja myöntävät hyväksytyt luottamuspalvelut ovat tässä asetuksessa vahvistettujen standardien mukaisia. Näiden standardien olisi heijastettava vakiintuneita käytäntöjä, ja niiden olisi oltava laajasti tunnustettuja kyseessä olevilla aloilla. Näitä standardeja olisi mukautettava siten, että niihin sisällytetään lisätarkastuksia, joilla varmistetaan hyväksytyn luottamuspalvelun sekä päivän ja ajankohdan tietoihin sitomisen turvallisuus ja luotettavuus sekä aikalähteen virheettömyys.

(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.

(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]).

([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).

([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).

(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

Asetuksen (EY) N:o 910/2014 42 artiklan 2 kohdassa tarkoitetut viitestandardit ja eritelmät esitetään tämän asetuksen liitteessä.

2 artikla

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

([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 hyväksyttyjä aikaleimoja myöntävien palvelujen viitestandardeista ja eritelmistä

Standardeja ETSI EN 319 421 V1.3.1 ([1]) ('ETSI EN 319 421') ja ETSI EN 319 422 V1.1.1 ([2]) ('ETSI EN 319 422') sovelletaan seuraavin mukautuksin:

1. ETSI EN 319 421

1) 2.1 Velvoittavat viittaukset

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

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

— [5] ETSI EN 319 422 V1.1.1 (2016–03) "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".

— [6] Tyhjä.

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

— [10] Komission täytäntöönpanoasetus (EU) 2024/482 ([4]), 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.

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

2) 3.1 Käsitteet

— varmenteen voimassaoloaika: aikaväli, joka alkaa hetkestä notBefore ja päättyy hetkeen notAfter ja jonka aikana varmenneviranomainen (CA) takaa, että se säilyttää tiedot varmenteen tilasta.

3) 3.3 Lyhenteet

— EUCC Yhteisiin kriteereihin perustuva eurooppalainen kyberturvallisuuden sertifiointijärjestelmä

4) 6.2 Luottamuspalvelun käytäntöselostus

— OVR-6.2–03 Aikaleiman myöntävän viranomaisen (TSA) on sisällytettävä TSA:n tiedonantoilmoitukseensa tiedot aikaleimapalvelunsa saatavuudesta.

5) 7.3 Henkilöstön luotettavuus

— OVR-7.3–02 TSA: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.

— OVR-7.3–03 Kohdan OVR-7.3–02 noudattamiseen on sisällyttävä säännöllisesti (vähintään 12 kuukauden välein) tehtäviä päivityksiä uusista uhkista ja nykyisistä turvakäytännöistä.

([1]) EN 319 421 – Electronic Signatures and Infrastructures (ESI) – Policy and Security Requirements for Trust Service Providers issuing Time Stamps, V1.3.1.
([2]) EN 319 422 – Electronic Signatures and Infrastructures (ESI) – Time-stamping protocol and time-stamp token profiles, V1.1.1 (2016–03), https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf.
([3]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([4]) EUVL L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([5]) EUVL L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

6) 7.6.2 Aikaleimayksikön (TSU) avaimen luominen

— TIS-7.6.2–03 TSU:n avaimen (avainten) luominen on suoritettava suojatulla salauslaitteella, joka on seuraavien mukaisesti sertifioitu luotettava järjestelmä:

a) tietoteknologian turvallisuuden arviointia koskevat yhteiset kriteerit, sellaisina kuin ne on esitetty standardissa ISO/IEC 15408 [3] 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 [10][11], ja sertifioitu vähintään tasolle EAL 4; tai

c) 31.12.2030 saakka FIPS PUB 140–3 [7] 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 [10][11]-sertifiointi, laite on konfiguroitava ja sitä on käytettävä kyseisen sertifioinnin mukaisesti.

— TIS-7.6.2–04 Tyhjä.

— HUOMAUTUS 3 Tyhjä.

— TIS-7.6.2–05A TSU:n avaimen luontialgoritmin, tuloksena saatavan allekirjoitusavaimen pituuden ja allekirjoitusalgoritmin, joita käytetään aikaleimojen allekirjoittamiseen ja TSU:n julkisen avaimen varmenteiden allekirjoittamiseen, on oltava Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [9] mukaisia.

— HUOMAUTUS 4 Tyhjä.

— TIS-7.6.2–06 TSU:n allekirjoitusavaimen saa viedä ja tuoda toiseen suojattuun salauslaitteeseen ainoastaan, jos kyseinen vienti ja tuonti toteutetaan turvallisesti ja kyseisten laitteiden sertifioinnin mukaisesti.

7) 7.6.3 TSU:n yksityisen avaimen suojaaminen

— TIS-7.6.3–02 TSU:n yksityistä avainta 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 [3] 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) [10][11], joka on sertifioitu vähintään tasolle EAL 4; tai

c) 31.12.2030 saakka FIPS PUB 140–3 [7] 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 [10][11]-sertifiointi, laite on konfiguroitava ja sitä on käytettävä kyseisen sertifioinnin mukaisesti.

— TIS-7.6.3–03 Tyhjä.

— HUOMAUTUS 2 Tyhjä.

8) 7.6.7 TSU:n avaimen elinkaaren päättyminen

— TIS-7.6.7–03A TSU:n yksityisten avainten voimassaolon päättymispäivän on oltava sovittujen salausmekanismien [9] mukainen.

— HUOMAUTUS 1 Tyhjä.

9) 7.10 Verkkoturvallisuus

— OVR-7.10–05 Standardin ETSI EN 319 401 [1] kohdassa REQ-7.8–13 edellytetty haavoittuvuuskartoitus on tehtävä vähintään neljännesvuosittain.

— OVR-7.10–06 Standardin ETSI EN 319 401 [1] kohdassa REQ-7.8–17X edellytetty tunkeutumistesti on tehtävä vähintään neljännesvuosittain.

— OVR-7.10–07 Palomuurit on konfiguroitava siten, että estetään kaikki protokollat ja liittymät, joita ei tarvita TSA:n toiminnassa.

10) 7.14 TSA:n toiminnan lopettaminen ja lopettamissuunnitelmat

— OVR-7.14–01A TSP:n toiminnan lopettamissuunnitelman on oltava asetuksen (EU) N:o 910/2014 [i.4] 24 artiklan 5 kohdan nojalla hyväksytyissä täytäntöönpanosäädöksissä vahvistettujen vaatimusten mukainen.

2. ETSI EN 319 422

1) 2.1 Velvoittavat viittaukset

— [5] Tyhjä.

— [6] Tyhjä.

— [8] Euroopan kyberturvallisuuden sertifiointiryhmä, Salausta käsittelevä alaryhmä: ”Agreed Cryptographic Mechanisms”.

— [9] RFC 9110 HTTP Semantics.

2) 4.1.3 Käytettävät hajautusalgoritmit

— Sovelletaan seuraavaa lauseketta:

Aikaleimattavien tietojen hajauttamiseen käytettävien hajautusalgoritmien, aikaleiman odotetun keston ja valittujen hajautusfunktioiden käyttöajan on oltava Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [8] mukaisia.

— HUOMAUTUS Tyhjä.

3) 4.2.3 Tuettavat algoritmit

— Sovelletaan seuraavaa lauseketta:

Tuettavien aikaleimatokenin allekirjoitusalgoritmien on oltava Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [8] mukaisia.

— HUOMAUTUS Tyhjä.

4) 4.2.4 Tuettavat avainpituudet

— Sovelletaan seuraavaa lauseketta:

Valittujen allekirjoitusalgoritmien avainpituuksien on oltava Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien mukaisia.

— HUOMAUTUS Tyhjä.

5) 5.1.3 Tuettavat algoritmit

— Sovelletaan seuraavaa lauseketta:

Tuettavien aikaleimatietojen hajautusalgoritmien, aikaleiman odotetun keston ja valittujen hajautusfunktioiden käyttöajan on oltava Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [8] mukaisia.

— HUOMAUTUS Tyhjä.

6) 5.2.3 Käytettävät algoritmit

— Sovelletaan seuraavaa lauseketta:

Aikaleimattavien tietojen hajauttamiseen käytettävien hajautusalgoritmien ja aikaleimatokenin allekirjoitusalgoritmien on oltava Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [8] mukaisia.

— HUOMAUTUS Tyhjä.

7) 6.3 Avainpituutta koskevat vaatimukset

— Sovelletaan seuraavaa lauseketta:

TSU-varmenteen valitun allekirjoitusalgoritmin avainpituuden on oltava Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [8] mukainen.

— HUOMAUTUS Tyhjä.

8) 6.5 Algoritmeja koskevat vaatimukset

— Sovelletaan seuraavaa lauseketta:

TSU:n julkisessa avaimessa ja TSU-varmenteen allekirjoituksessa on käytettävä algoritmeja, jotka ovat Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [8] mukaisia.

— HUOMAUTUS Tyhjä.

9) 7 Tuettavat siirtoprotokollien profiilit

— Aikaleima-asiakkaan ja aikaleimapalvelimen on tuettava aikaleimaprotokollaa HTTPS:n [9] kautta, kuten standardin IETF RFC 3161 [1] lausekkeessa 3.4 määritellään.

10) 8 Salausalgoritmien objektitunnisteet

— Sovelletaan seuraavaa lauseketta:

TSU:n julkisessa avaimessa ja TSU-varmenteen allekirjoituksessa on käytettävä algoritmeja, jotka ovat Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [8] mukaisia.

11) 9.1 Sääntöjen noudattamista koskeva vakuutus

— Jos TSA ilmoittaa aikaleimatokenin olevan asetuksen (EU) N:o 910/2014 [i.2] mukainen hyväksytty sähköinen aikaleima, sen on sisällytettävä aikaleimatokenin laajennuskenttään yksi qcStatements-laajennus, joka on standardin IETF RFC 3739 [i.3] lausekkeessa 3.2.6 määritellyn syntaksin mukainen.

— qcStatements-laajennuksen on sisällettävä yksi liitteessä B määritelty lausuma ”esi4-qtstStatement-1”.

— qcStatements-laajennusta ei saa merkitä kriittiseksi.