Euroopan unionin
virallinen lehti

FI
L-sarja

2025/1943

30.9.2025

KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2025/1943,

annettu 29 päivänä syyskuuta 2025,

Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 soveltamissäännöistä sähköisten allekirjoitusten hyväksyttyjen varmenteiden ja sähköisten leimojen hyväksyttyjen varmenteiden viitestandardien 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 28 artiklan 6 kohdan ja 38 artiklan 6 kohdan,

sekä katsoo seuraavaa:

(1) Sähköisten allekirjoitusten hyväksytyillä varmenteilla ja sähköisten leimojen hyväksytyillä varmenteilla on keskeinen rooli digitaalisessa liiketoimintaympäristössä, sillä ne edistävät siirtymistä perinteisistä paperipohjaisista prosesseista vastaaviin sähköisiin prosesseihin. Hyväksytyt varmenteet yhdistävät sähköisen allekirjoituksen validointitiedot tai sähköisen leiman validointitiedot luonnolliseen henkilöön tai oikeushenkilöön ja vahvistavat kyseisen henkilön nimen ja lisäävät siten varmuutta allekirjoittajan ja leiman luojan henkilöllisyydestä.

(2) Asetuksen (EU) N:o 910/2014 28 artiklan 6 kohdassa ja 38 artiklan 6 kohdassa säädettyä vaatimustenmukaisuusolettamaa olisi sovellettava ainoastaan, jos sähköisten allekirjoitusten hyväksyttyjen varmenteiden myöntämiseen käytettävät hyväksytyt luottamuspalvelut ja sähköisten leimojen hyväksyttyjen varmenteiden myöntämiseen käytettävät 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 hyväksyttyjen luottamuspalvelujen ja hyväksyttyjen varmenteiden sisällön 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) 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

Sähköisten allekirjoitusten ja sähköisten leimojen hyväksyttyjen varmenteiden viitestandardit ja eritelmät

1. Asetuksen (EU) N:o 910/2014 28 artiklan 6 kohdassa tarkoitetut viitestandardit ja eritelmät esitetään tämän asetuksen liitteessä I.

2. Asetuksen (EU) N:o 910/2014 38 artiklan 6 kohdassa tarkoitetut viitestandardit ja eritelmät esitetään tämän asetuksen liitteessä II.

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

([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 sähköisten allekirjoitusten hyväksyttyjen varmenteiden viitestandardeista ja eritelmistä

Standardeja ETSI EN 319 411-2 V2.6.1 ('ETSI EN 319 411-2'), ETSI EN 319 412-1 V1.6.1 ('ETSI EN 319 412-1'), ETSI EN 319 412-2 V2.4.1 ('ETSI EN 319 412-2') ja ETSI EN 319 412-5 V2.5.1 ('ETSI EN 319 412-5') sovelletaan seuraavin mukautuksin:

1. ETSI EN 319 411-2

1) 2.1 Velvoittavat viittaukset

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

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 1: General requirements", seuraavin mukautuksin:

Muutetaan standardin ETSI EN 319 411-1 V1.5.1 lauseke 2.1 Velvoittavat viittaukset seuraavasti:

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

— [10] ETSI EN 319 412-2 V2.4.1 "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons".

— [14] ETSI EN 319 412-1 V1.6.1 "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".

— [3] ETSI EN 319 412-5 V2.5.1 "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".

— [5] ETSI EN 319 412-1 V1.6.1 "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".

— [6] CEN/TS 419261:2015 "Security requirements for trustworthy systems managing certificates and time-stamps".

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

— [8] 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.

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

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

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

([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.

2) 5.2 Varmennuskäytäntöä koskevat vaatimukset

— OVR-5.2-02 Luottamuspalvelun tarjoajan (TSP) asiakirjoissa yksilöidyssä varmennepolitiikassa(-politiikoissa) (CP) on täsmennettävä käytettäviä varmenneprofiileja koskevat vaatimukset.

3) 5.3 Varmennepolitiikan nimi ja tunnistetiedot

— OVR-5.3-01 Jos lausekkeessa 4.2.2 kuvattuun CP:hen tehdään muutoksia, jotka vaikuttavat sen sovellettavuuteen, politiikan tunnistetta on muutettava.

4) 6.1 Julkaisemista ja tallentamista koskevat velvollisuudet

— OVR-6.1-02 Standardin ETSI EN 319 411-1 [2] kohdassa DIS-6.1-04 mainittujen tietojen on oltava julkisesti ja kansainvälisesti saatavilla.

5) 6.2.2 Henkilöllisyyden ensimmäinen vahvistaminen

— REG-6.2.2-01A Käyttäjän henkilöllisyyttä koskevien attribuuttien ja todisteiden kerääminen ja validointi on tehtävä asetuksen (EU) N:o 910/2014 [i.1] 24 artiklan 1 c kohdan nojalla hyväksyttyjen täytäntöönpanosäädösten mukaisesti.

— REG-6.2.2-02 [QCP-n] ja [QCP-n-qscd] Luonnollisen henkilön henkilöllisyys ja tarvittaessa henkilöön liittyvät erityiset attribuutit on tarkastettava asetuksen (EU) N:o 910/2014 [i.1] 24 artiklan 1 c kohdan nojalla hyväksyttyjen täytäntöönpanosäädösten mukaisesti.

— HUOMAUTUS 1 Tyhjä.

6) 6.3.3 Varmenteen myöntäminen

— GEN-6.3.3-01 Sovelletaan standardin ETSI EN 319 411-1 [2] lausekkeessa 6.3.3 määriteltyjä vaatimuksia GEN-6.3.3-01 – GEN-6.3.3-10.

— GEN-6.3.3-02 [EHDOLLINEN] Jos varmenne myönnetään luonnolliselle henkilölle, joka on tunnistettu yhdessä oikeushenkilön kanssa, varmenteessa mainitun organisaation yksilöivien käyttäjäattribuuttien on edustettava oikeushenkilöä tai kyseisen oikeushenkilön alayksikköä, ja varmenteessa olevan käyttäjätunnisteen on oltava kyseinen luonnollinen henkilö.

— GEN-6.3.3-03 CP-tunnisteen on oltava [VALINNAINEN]:

a) [QCP-n]

— kuten määritellään lausekkeen 5.3 alakohdassa a ja/tai

— objektitunniste (OID), jonka on antanut TSP tai muu asiaankuuluva sidosryhmä tai joka on annettu sellaisen varmennepolitiikkaa koskevan lisästandardoinnin mukaisesti, joka parantaa tässä asiakirjassa määriteltyjä vastaavia sovellettavia politiikkavaatimuksia.

b) [QCP-n-qscd]

— kuten määritellään lausekkeen 5.3 alakohdassa c ja/tai

— objektitunniste (OID), jonka on antanut TSP tai muu asiaankuuluva sidosryhmä tai joka on annettu sellaisen varmennepolitiikkaa koskevan lisästandardoinnin mukaisesti, joka parantaa tässä asiakirjassa määriteltyjä vastaavia sovellettavia politiikkavaatimuksia.

7) 6.3.5 Avainparin ja varmenteen käyttö

— SDP-6.3.5-02A [EHDOLLINEN] Jos TSP hallinnoi hyväksytyn sähköisen allekirjoituksen tai leiman luontivälinettä (QSCD) käyttäjän puolesta, TSP:n on oltava hyväksytty luottamuspalvelun tarjoaja, joka tarjoaa hyväksyttyä luottamuspalvelua hyväksytyn sähköisen allekirjoituksen etäluonti-välineen hallinnointia varten asetuksen (EU) N:o 910/2014 [i.1] mukaisesti.

— SDP-6.3.5-11A Tilaajan velvollisuuksiin (ks. lauseke 6.3.4) kuuluvat, jos tilaaja tai käyttäjä tuottaa käyttäjän avaimet:

a) velvollisuus luoda käyttäjän avaimet käyttäen Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [7] mukaista algoritmia CP:ssä määriteltyjä hyväksytyn avaimen käyttötarkoituksia varten;

b) velvollisuus käyttää Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [7] mukaista avaimen pituutta ja algoritmia CP:ssä määriteltyjä hyväksytyn avaimen käyttötarkoituksia varten varmenteen voimassaoloaikana.

8) 6.3.10 Varmennetilapalvelut

— CSS-6.3.10-08 [EHDOLLINEN] Jos käytettävissä on varmenteiden sulkulistoja (CRL), TSP:n on säilytettävä viimeisen CRL:n eheys ja käytettävyys vähintään varmennuskäytännössä (CPS) määritetyn ajan, kuten kohdassa CSS-6.3.10-12 edellytetään.

9) 6.4.4 Henkilöstön valvonta

— OVR-6.4.4-02 TSP: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-6.4.4-03 Kohdan OVR-6.4.4-02 noudattamiseen on sisällyttävä säännöllisesti (vähintään 12 kuukauden välein) tehtäviä päivityksiä uusista uhkista ja nykyisistä turvakäytännöistä.

— OVR-6.4.4-04 Standardissa ETSI EN 319 401 [1] (lauseke 7.2-15) määriteltyjen luotettujen roolien lisäksi on tuettava standardissa TS 419261 [6] määriteltyjä rekisteröinti- ja peruutusvirkailijoiden luotettuja rooleja. Tapauksissa, joissa hyväksyttyä luottamuspalvelun tarjoajaa (QTSP) hallinnoi suoraan jäsenvaltio tai julkisen sektorin elin tai se toimii jäsenvaltion tai julkisen sektorin elimen puolesta, nämä ylimääräiset luotetut roolit voi hoitaa yksi tai useampi virallinen edustaja, joka toimii paikallis- tai aluehallinnossa toimivien rekisteröinti- ja peruutusvirkailijoiden nimissä ja puolesta.

10) 6.4.9 Varmenneviranomaisen (CA) tai rekisteröintiviranomaisen (RA) toiminnan lopettaminen

— OVR-6.4.9-02 TSP:n toiminnan lopettamissuunnitelman on oltava asetuksen (EU) N:o 910/2014 [i.1] 24 artiklan 5 kohdan nojalla hyväksytyissä täytäntöönpanosäädöksissä vahvistettujen vaatimusten mukainen.

11) 6.5.1 Avainparien luominen ja asentaminen

— OVR-6.5.1-01A CA:n avainparien luominen on suoritettava käyttäen algoritmia, joka on Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [7] mukainen CA:n allekirjoitustarkoituksia varten.

— OVR-6.5.1-01B CA:n allekirjoitusavainta varten valitun avaimen pituuden ja algoritmin on oltava Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [7] mukainen CA:n allekirjoitustarkoituksia varten.

— OVR-6.5.1-01C [EHDOLLINEN] Jos CA luo käyttäjän avaimet, CA:n luomien käyttäjän avainten on oltava Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [7] mukaisia niitä tarkoituksia varten, jotka on ilmoitettu CP:ssä varmenteen voimassaoloaikana.

12) 6.5.2 Yksityisen avaimen suojaaminen ja salausmoduulien tekninen valvonta

— GEN-6.5.2-01 Kaikkia standardin ETSI EN 319 411-1 [2] lausekkeessa 6.5.2 määriteltyjä vaatimuksia sovelletaan, lukuun ottamatta vaatimuksia OVR-6.5.2-01, OVR-6.5.2-03 ja OVR-6.5.2-04.

— GEN-6.5.2-02 TSP:n avainparien luominen, mukaan lukien peruuttamis- ja rekisteröintipalvelujen käyttämät avaimet, on suoritettava suojatulla salauslaitteella, joka on seuraavien mukaisesti sertifioitu luotettava järjestelmä:

— 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: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

— yhteisiin kriteereihin perustuva eurooppalainen kyberturvallisuuden sertifiointijärjestelmä (EUCC) [8][9], joka on sertifioitu vähintään tasolle EAL 4; tai

— 31.12.2030 saakka FIPS PUB 140-3 [11] 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 [8][9]-sertifiointi, laite on konfiguroitava ja sitä on käytettävä kyseisen sertifioinnin mukaisesti.

— GEN-6.5.2-03 CA:n yksityistä allekirjoitusavainta on säilytettävä ja käytettävä suojatussa salauslaitteessa, joka täyttää kohtien GEN-6.5.2-01 ja GEN-6.5.2-02 vaatimukset.

13) 6.5.7 Verkon turvatarkastukset

— OVR-6.5.7-02 Standardin ETSI EN 319 401 [1] kohdassa REQ-7.8-13 edellytetty haavoittuvuuskartoitus on tehtävä vähintään neljännesvuosittain.

— OVR-6.5.7-03 Standardin ETSI EN 319 401 [1] kohdassa REQ-7.8-17X edellytetty tunkeutumistesti on tehtävä vähintään neljännesvuosittain.

— OVR-6.5.7-04 Palomuurit on konfiguroitava siten, että estetään kaikki protokollat ja liittymät, joita ei tarvita TSP:n toiminnassa.

14) 6.6.1 Varmenneprofiili

— GEN-6.6.1-05 Varmenteessa on oltava jokin kohdassa GEN-6.3.3-03 [VALINNAINEN] yksilöidyistä politiikan tunnisteista. Varmenteeseen voi sisältyä muita TSP:n myöntämiä OID-tunnisteita.

2. ETSI EN 319 412-2

1) 2.1 Velvoittavat viittaukset

— [2] ETSI EN 319 412-5 V2.5.1 ”Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements”.

— [9] Euroopan kyberturvallisuuden sertifiointiryhmä, Salausta käsittelevä alaryhmä: ENISAn julkaisema asiakirja ”Agreed Cryptographic Mechanisms”.

2) 4.2.2 Allekirjoitus

— GEN-4.2.2-2 Allekirjoitusalgoritmi on valittava Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [9] mukaisesti.

— HUOMAUTUS Tyhjä.

3) 4.2.3.1 Myöntäjä, joka on oikeushenkilö

— GEN-4.2.3.1-3 Jos tiedetään, että asianmukainen rekisterinumero on olemassa, myöntäjän identiteettiin on sisällyttävä attribuutti organizationIdentifier, jonka arvo on sama kuin on ilmoitettu vastaavassa virallisessa rekisterissä, jossa rekisterinumero on vahvistettu.

4) 4.2.5 Käyttäjän julkisen avaimen tiedot

— GEN-4.2.5-2 Käyttäjän julkinen avain on valittava Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [9] mukaisesti.

— HUOMAUTUS Tyhjä.

5) 4.2.6 Sarjanumero

— GEN-4.2.6-01 Varmenteen serialNumber-tunnisteen (siten kuin se on määritelty standardin IETF RFC 5280 [1] lausekkeessa 4.1.2.2) on oltava yksilöivä kunkin TSP:n myöntämän varmenteen osalta.

LIITE II

Luettelo sähköisten leimojen hyväksyttyjen varmenteiden viitestandardeista ja eritelmistä

Standardeja ETSI EN 319 411-2 V2.6.1 ('ETSI EN 319 411-2'), ETSI EN 319 412-1 V1.6.1 ('ETSI EN 319 412-1'), ETSI EN 319 412-3 V1.3.1 ('ETSI EN 319 412-3'), ETSI EN 319 412-2 V2.4.1 ('ETSI EN 319 412-2') ja ETSI EN 319 412-5 V2.5.1 ('ETSI EN 319 412-5') sovelletaan seuraavin mukautuksin:

1. ETSI EN 319 411-2

1) 2.1 Velvoittavat viittaukset

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

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 1: General requirements", seuraavin mukautuksin:

Muutetaan standardin ETSI EN 319 411-1 V1.5.1 lauseke 2.1 Velvoittavat viittaukset seuraavasti:

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

— [10] ETSI EN 319 412-2 V2.4.1 "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons".

— [14] ETSI EN 319 412-1 V1.6.1 "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".

— [3] ETSI EN 319 412-5 V2.5.1 "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".

— [5] ETSI EN 319 412-1 V1.6.1 "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".

— [6] CEN/TS 419261:2015 "Security requirements for trustworthy systems managing certificates and time-stamps" (CENin tuottama).

— [7] Euroopan kyberturvallisuuden sertifiointiryhmä, Salausta käsittelevä alaryhmä: ENISAn julkaisema asiakirja "Agreed Cryptographic Mechanisms".

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

— [9] Täytäntöönpanoasetus (EU) 2024/3144 täytäntöönpanoasetuksen (EU) 2024/482 muuttamisesta sovellettavien kansainvälisten standardien osalta ja kyseisen täytäntöönpanoasetuksen oikaisemisesta.

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

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

2) 5.2 Varmennuskäytäntöä koskevat vaatimukset

— OVR-5.2-02 Luottamuspalvelun tarjoajan (TSP) asiakirjoissa yksilöidyssä varmennepolitiikassa(-politiikoissa) (CP) on täsmennettävä käytettäviä varmenneprofiileja koskevat vaatimukset.

3) 5.3 Varmennepolitiikan nimi ja tunnistetiedot

— OVR-5.3-01 Jos lausekkeessa 4.2.2 kuvattuun CP:hen tehdään muutoksia, jotka vaikuttavat sen sovellettavuuteen, politiikan tunnistetta on muutettava.

4) 6.1 Julkaisemista ja tallentamista koskevat velvollisuudet

— OVR-6.1-02 Standardin ETSI EN 319 411-1 [2] kohdassa DIS-6.1-04 mainittujen tietojen on oltava julkisesti ja kansainvälisesti saatavilla.

5) 6.2.2 Henkilöllisyyden ensimmäinen vahvistaminen

— REG-6.2.2-01A Käyttäjän henkilöllisyyttä koskevien attribuuttien ja todisteiden kerääminen ja validointi on tehtävä asetuksen (EU) N:o 910/2014 [i.1] 24 artiklan 1 c kohdan nojalla hyväksyttyjen täytäntöönpanosäädösten mukaisesti.

— REG-6.2.2-03 [QCP-n] ja [QCP-n-qscd] Oikeushenkilön henkilöllisyys ja tarvittaessa henkilöön liittyvät erityiset attribuutit on tarkastettava asetuksen (EU) N:o 910/2014 [i.1] 24 artiklan 1 c kohdan nojalla hyväksyttyjen täytäntöönpanosäädösten mukaisesti.

— HUOMAUTUS 3 Katso huomautus 2.

6) 6.3.3 Varmenteen myöntäminen

— GEN-6.3.3-01 Sovelletaan standardin ETSI EN 319 411-1 [2] lausekkeessa 6.3.3 määriteltyjä vaatimuksia GEN-6.3.3-01 – GEN-6.3.3-10.

— GEN-6.3.3-02 CP-tunnisteen on oltava [VALINNAINEN]:

a) [QCP-l]

— kuten määritellään lausekkeen 5.3 alakohdassa b ja/tai

— objektitunniste (OID), jonka on antanut TSP tai muu asiaankuuluva sidosryhmä tai joka on annettu sellaisen varmennepolitiikkaa koskevan lisästandardoinnin mukaisesti, joka parantaa tässä asiakirjassa määriteltyjä vastaavia sovellettavia politiikkavaatimuksia.

b) [QCP-l-qscd]

— kuten määritellään lausekkeen 5.3 alakohdassa d ja/tai

— objektitunniste (OID), jonka on antanut TSP tai muu asiaankuuluva sidosryhmä tai joka on annettu sellaisen varmennepolitiikkaa koskevan lisästandardoinnin mukaisesti, joka parantaa tässä asiakirjassa määriteltyjä sovellettavia politiikkaa koskevia vaatimuksia.

7) 6.3.5 Avainparin ja varmenteen käyttö

— SDP-6.3.5-02A [EHDOLLINEN] Jos TSP hallinnoi hyväksytyn sähköisen allekirjoituksen tai leiman luontivälinettä (QSCD) käyttäjän puolesta, TSP:n on oltava hyväksytty luottamuspalvelun tarjoaja, joka tarjoaa hyväksyttyä luottamuspalvelua hyväksytyn sähköisen leiman etäluontivälineen hallinnointia varten asetuksen (EU) N:o 910/2014 [i.1] mukaisesti.

— SDP-6.3.5-11A Tilaajan velvollisuuksiin (ks. lauseke 6.3.4) kuuluvat, jos tilaaja tai käyttäjä tuottaa käyttäjän avaimet:

a) velvollisuus luoda käyttäjän avaimet käyttäen Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [7] mukaista algoritmia CP:ssä määriteltyjä hyväksytyn avaimen käyttötarkoituksia varten; ja

b) velvollisuus käyttää Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [7] mukaista avaimen pituutta ja algoritmia CP:ssä määriteltyjä hyväksytyn avaimen käyttötarkoituksia varten varmenteen voimassaoloaikana.

8) 6.3.10 Varmennetilapalvelut

— CSS-6.3.10-08 [EHDOLLINEN] Jos käytettävissä on varmenteiden sulkulistoja (CRL), TSP:n on säilytettävä viimeisen CRL:n eheys ja käytettävyys vähintään varmennuskäytännössä (CPS) määritetyn ajan, kuten kohdassa CSS-6.3.10-12 edellytetään.

9) 6.4.4 Henkilöstön valvonta

— OVR-6.4.4-02 TSP: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-6.4.4-03 Kohdan OVR-6.4.4-02 noudattamiseen on sisällyttävä säännöllisesti (vähintään 12 kuukauden välein) tehtäviä päivityksiä uusista uhkista ja nykyisistä turvakäytännöistä.

— OVR-6.4.4-04 Standardissa ETSI EN 319 401 [1] (lauseke 7.2-15) määriteltyjen luotettujen roolien lisäksi on tuettava standardissa TS 419261 [6] määriteltyjä rekisteröinti- ja peruutusvirkailijoiden luotettuja rooleja. Tapauksissa, joissa hyväksyttyä luottamuspalvelun tarjoajaa (QTSP) hallinnoi suoraan jäsenvaltio tai julkisen sektorin elin tai se toimii jäsenvaltion tai julkisen sektorin elimen puolesta, nämä ylimääräiset luotetut roolit voi hoitaa yksi tai useampi virallinen edustaja, joka toimii paikallis- tai aluehallinnossa toimivien rekisteröinti- ja peruutusvirkailijoiden nimissä ja puolesta.

10) 6.4.9 Varmenneviranomaisen (CA) tai rekisteröintiviranomaisen (RA) toiminnan lopettaminen

— OVR-6.4.9-02 TSP:n toiminnan lopettamissuunnitelman on oltava asetuksen (EU) N:o 910/2014 [i.1] 24 artiklan 5 kohdan nojalla hyväksytyissä täytäntöönpanosäädöksissä vahvistettujen vaatimusten mukainen.

11) 6.5.1 Avainparien luominen ja asentaminen

— OVR-6.5.1-01A CA:n avainparien luominen on suoritettava käyttäen algoritmia, joka on Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [7] mukainen CA:n allekirjoitustarkoituksia varten.

— OVR-6.5.1-01B CA:n allekirjoitusavainta varten valitun avaimen pituuden ja algoritmin on oltava Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [7] mukainen CA:n allekirjoitustarkoituksia varten.

— OVR-6.5.1-01C [EHDOLLINEN] Jos CA luo käyttäjän avaimet, CA:n luomien käyttäjän avainten on oltava Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [7] mukaisia niitä tarkoituksia varten, jotka on ilmoitettu CP:ssä varmenteen voimassaoloaikana.

12) 6.5.2 Yksityisen avaimen suojaaminen ja salausmoduulien tekninen valvonta

— GEN-6.5.2-01 Kaikkia standardin ETSI EN 319 411-1 [2] lausekkeessa 6.5.2 määriteltyjä vaatimuksia sovelletaan, lukuun ottamatta vaatimuksia OVR-6.5.2-01, OVR-6.5.2-03 ja OVR-6.5.2-04.

— GEN-6.5.2-02 TSP:n avainparien luominen, mukaan lukien peruuttamis- ja rekisteröintipalvelujen käyttämät avaimet, on suoritettava suojatulla salauslaitteella, joka on seuraavien mukaisesti sertifioitu luotettava järjestelmä:

  — 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: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

  — yhteisiin kriteereihin perustuva eurooppalainen kyberturvallisuuden sertifiointijärjestelmä (EUCC) [8][9], joka on sertifioitu vähintään tasolle EAL 4; tai

  — 31.12.2030 saakka FIPS PUB 140-3 [11] 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 [8][9]-sertifiointi, laite on konfiguroitava ja sitä on käytettävä kyseisen sertifioinnin mukaisesti.

— GEN-6.5.2-03 CA:n yksityistä allekirjoitusavainta on säilytettävä ja käytettävä suojatussa salauslaitteessa, joka täyttää kohtien GEN-6.5.2-01 ja GEN-6.5.2-02 vaatimukset.

13) 6.5.7 Verkon turvatarkastukset

— OVR-6.5.7-02 Standardin ETSI EN 319 401 [1] kohdassa REQ-7.8-13 edellytetty haavoittuvuus-kartoitus on tehtävä vähintään neljännesvuosittain.

— OVR-6.5.7-03 Standardin ETSI EN 319 401 [1] kohdassa REQ-7.8-17X edellytetty tunkeutumistesti on tehtävä vähintään neljännesvuosittain.

— OVR-6.5.7-04 Palomuurit on konfiguroitava siten, että estetään kaikki protokollat ja liittymät, joita ei tarvita TSP:n toiminnassa.

14) 6.6.1 Varmenneprofiili

— GEN-6.6.1-05 Varmenteessa on oltava jokin kohdassa GEN-6.3.3-02 [VALINNAINEN] yksilöidyistä politiikan tunnisteista.

2. ETSI EN 319 412-3

1) 2.1 Velvoittavat viittaukset

— [2] ETSI EN 319 412-2 V2.4.1 ”Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate Profile for certificates issued to natural persons”.

2) 4.2.1 Käyttäjä

— LEG-4.2.1-6 Attribuuttiin organizationIdentifier on sisällyttävä käyttäjäorganisaation tunniste, joka poikkeaa organisaation nimestä. Jos tiedetään, että asianmukainen rekisterinumero on olemassa, attribuuttiin organizationIdentifier on sisällyttävä tämän rekisterinumeron arvo, siten kuin se on ilmoitettu vastaavassa virallisessa rekisterissä, jossa rekisterinumero on vahvistettu.

3. ETSI EN 319 412-2

1) 2.1 Velvoittavat viittaukset

— [2] ETSI EN 319 412-5 V2.5.1 ”Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements”.

— [9] Euroopan kyberturvallisuuden sertifiointiryhmä, Salausta käsittelevä alaryhmä: ENISAn julkaisema asiakirja ”Agreed Cryptographic Mechanisms”.

2) 2.2 Lähdeviitteet

— [i.7] Tyhjä.

3) 4.2.2 Allekirjoitus

— GEN-4.2.2-2 Allekirjoitusalgoritmi on valittava Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [9] mukaisesti.

— HUOMAUTUS Tyhjä.

4) 4.2.3.1 Myöntäjä, joka on oikeushenkilö

— GEN-4.2.3.1-3 Jos tiedetään, että asianmukainen rekisterinumero on olemassa, myöntäjän identiteettiin on sisällyttävä attribuutti organizationIdentifier, jonka arvo on sama kuin on ilmoitettu vastaavassa virallisessa rekisterissä, jossa rekisterinumero on vahvistettu.

5) 4.2.5 Käyttäjän julkisen avaimen tiedot

— GEN-4.2.5-2 Käyttäjän julkinen avain on valittava Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [9] mukaisesti.

— HUOMAUTUS Tyhjä.

6) 4.2.6 Sarjanumero

— GEN-4.2.6-01 Varmenteen serialNumber-tunnisteen (siten kuin se on määritelty standardin IETF RFC 5280 [1] lausekkeessa 4.1.2.2) on oltava yksilöivä kunkin TSP:n myöntämän varmenteen osalta.