Euroopan unionin
virallinen lehti

FI
L-sarja

2026/1735

22.7.2026

KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2026/1735,

annettu 15 päivänä heinäkuuta 2026,

täytäntöönpanoasetuksen (EU) 2025/1569 muuttamisesta sovellettavien standardien 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 d artiklan 5 kohdan, 45 e artiklan 2 kohdan, 45 f artiklan 6 kohdan ja 45 f artiklan 7 kohdan,

sekä katsoo seuraavaa:

(1) Jotta eurooppalaisten digitaalisen identiteetin lompakoiden kehittämisessä voidaan varmistaa mahdollisimman suuri yhdenmukaistaminen jäsenvaltioiden kesken, lompakoiden tekniset eritelmät perustuvat komission suosituksen (EU) 2021/946 ([2]) perusteella tehtyyn työhön ja erityisesti siihen kuuluvaan arkkitehtuuriin ja viitekehykseen. Koska arkkitehtuuri ja viitekehys ovat kehittyneet merkittävästi täytäntöönpanoasetuksen (EU) 2025/1569 ([3]) hyväksymisen jälkeen, asetusta (EU) 2025/1569 olisi nyt muutettava vastaavasti sen mukauttamiseksi uusiin standardeihin ja eritelmiin.

(2) Asetuksen (EU) N:o 910/2014 tavoitteiden mukaisesti sähköisten attribuuttitodistusten myöntämiseen, hallinnointiin ja tarkastamiseen sovellettavien vaatimusten täyttämiseksi on valittu joukko standardeja. Näiden standardien olisi heijastettava vakiintuneita käytäntöjä, ja niiden olisi oltava laajasti tunnustettuja kyseessä olevilla aloilla. Näitä standardeja olisi tarvittaessa mukautettava tai täydennettävä, jotta voidaan varmistaa sähköisten attribuuttitodistusten turvallisuuden ja eheyden korkea taso ja samalla helpottaa rajat ylittävää yhteentoimivuutta ja sisämarkkinoiden tehokasta toimintaa. Tämän tavoitteen mukaisesti tällä asetuksella saatetaan ajan tasalle vaatimukset, joita sovelletaan hyväksyttyjen sähköisten attribuuttitodistusten ja virallisesta lähteestä vastaavan julkisen sektorin elimen myöntämien tai sen puolesta myönnettyjen sähköisten attribuuttitodistusten myöntämiseen ja peruuttamiseen, ja otetaan käyttöön vaatimukset, jotka koskevat virallisiin lähteisiin perustuvien todentamistulosten allekirjoittamista ja leimaamista.

(3) Kaikkiin tämän asetuksen mukaisiin henkilötietojen käsittelytoimiin sovelletaan Euroopan parlamentin ja neuvoston asetusta (EU) 2016/679 ([4]) ja tarvittaessa Euroopan parlamentin ja neuvoston direktiiviä 2002/58/EY ([5]).

([1]) EUVL L 257, 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Komission suositus (EU) 2021/946, annettu 3 päivänä kesäkuuta 2021, unionin yhteisestä välineistöstä eurooppalaista digitaalisen identiteetin kehystä koskevaa koordinoitua lähestymistapaa varten (EUVL L 210, 14.6.2021, s. 51, ELI: http://data.europa.eu/eli/reg/2021/946/oj).

([3]) Komission täytäntöönpanoasetus (EU) 2025/1569, annettu 29 päivänä heinäkuuta 2025, Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 soveltamissäännöistä hyväksyttyjen sähköisten attribuuttitodistusten ja virallisesta lähteestä vastaavan julkisen sektorin elimen myöntämien tai sen puolesta myönnettyjen sähköisten attribuuttitodistusten osalta (EUVL L, 2025/1569, 30.7.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([4]) 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).

([5]) 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).

(4) Euroopan tietosuojavaltuutettua on kuultu Euroopan parlamentin ja neuvoston asetuksen (EU) 2018/1725 ([6]) 42 artiklan 1 kohdan mukaisesti, ja hän antoi lausuntonsa 17 päivänä huhtikuuta 2026 ([7]).

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

ON HYVÄKSYNYT TÄMÄN ASETUKSEN:

1 artikla

Täytäntöönpanoasetuksen (EU) 2025/1569 muuttaminen

Muutetaan täytäntöönpanoasetus (EU) 2025/1569 seuraavasti:

1) Korvataan 3 artiklan 2 kohta seuraavasti:

”2. Jos hyväksyttyjen sähköisten attribuuttitodistusten tarjoajat ja virallisesta lähteestä vastaavan julkisen sektorin elimen myöntämien tai sen puolesta myönnettyjen sähköisten attribuuttitodistusten tarjoajat myöntävät sähköisiä attribuuttitodistuksia, jotka sisältyvät attribuuttitodistusten myöntämisjärjestelmien luetteloon rekisteröityihin järjestelmiin, niiden on täytettävä vastaavan attribuuttitodistusten myöntämisjärjestelmän vaatimukset. Periaatteiden ja menettelyjen, joita todistusten myöntäjät ovat ottaneet käyttöön noudattaakseen attribuuttitodistusten myöntämisjärjestelmien vaatimuksia, on oltava osa asetuksella (EU) N:o 910/2014 vahvistettua vaatimustenmukaisuuden arviointia.”

2) Muutetaan 4 artikla seuraavasti:

a) Kumotaan 1 kohta.

b) Korvataan 3 kohta seuraavasti:

”3. Hyväksyttyjen sähköisten attribuuttitodistusten tarjoajien ja virallisesta lähteestä vastaavan julkisen sektorin elimen myöntämien tai sen puolesta myönnettyjen sähköisten attribuuttitodistusten tarjoajien on peruutettava todistukset ainakin seuraavissa olosuhteissa aina, kun todistukset on myönnetty yli 24 tunnin voimassaoloajaksi:

a) sen henkilön pyynnöstä, jolle sähköinen attribuuttitodistus on myönnetty, tai tarvittaessa todistuksen kohteena olevan henkilön pyynnöstä;

b) kun tarjoaja saa tietoonsa, että hyväksyttyjen sähköisten attribuuttitodistusten tai virallisesta lähteestä vastaavan julkisen sektorin elimen myöntämien tai sen puolesta myönnettyjen sähköisten attribuuttitodistusten turvallisuus tai luotettavuus on vaarantunut;

c) muissa tilanteissa, joissa sitä edellytetään unionin tai kansallisessa lainsäädännössä.”

c) Korvataan 4 kohta seuraavasti:

”4. Hyväksyttyjen sähköisten attribuuttitodistusten tarjoajien ja virallisesta lähteestä vastaavan julkisen sektorin elimen myöntämien tai sen puolesta myönnettyjen sähköisten attribuuttitodistusten tarjoajien on otettava käyttöön peruuttamistekniikat ja hallintamenetelmät, jotka ovat yksityisyyttä suojaavia ja estävät tietojen yhdistämisen tai jäljittämisen. Peruuttamistekniikoiden on oltava liitteessä II vahvistettujen vaatimusten mukaisia.”

([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 Commission Implementing Regulation as regards applicable standards and specifications for the registration of wallet-relying parties | European Data Protection Supervisor.

3) Muutetaan 9 artikla seuraavasti:

a) Lisätään 2 kohdan jälkeen 2 a kohta seuraavasti:

”2 a. Tarkastusmekanismien on oltava liitteessä IV vahvistettujen vaatimusten mukaisia.”

b) Korvataan 4 kohta seuraavasti:

”4. Tarkastustuloksessa on ilmoitettava se, onko attribuutti tarkastettu vai ei, ja täsmennettävä virallisesta lähteestä vastaava julkisen sektorin elin tai tapauksen mukaan julkisen sektorin elin, joka on nimetty toimimaan sen virallisen lähteen puolesta, josta attribuutti on tarkastettu.

Virallisesta lähteestä vastaavan julkisen sektorin elimen tai kansallisella tasolla tunnustetun nimetyn välittäjän on allekirjoitettava tai leimattava tarkastustulos käyttäen vähintään sähköisten allekirjoitusten hyväksyttyyn varmenteeseen perustuvaa kehittynyttä sähköistä allekirjoitusta tai sähköisten leimojen hyväksyttyyn varmenteeseen perustuvaa kehittynyttä sähköistä leimaa.”

4) Korvataan liite I tämän asetuksen liitteessä I olevalla tekstillä.

5) Korvataan liite II tämän asetuksen liitteessä II olevalla tekstillä.

6) Lisätään tämän asetuksen liitteessä III oleva teksti liitteeksi IV.

2 artikla

Voimaantulo

Tämä asetus tulee voimaan kahdentenakymmenentenä päivänä sen jälkeen, kun se on julkaistu *Euroopan unionin virallisessa lehdessä*.

Asetuksen 1 artiklan 3 kohtaa sovelletaan 1 päivästä tammikuuta 2027.

Tämä asetus on kaikilta osiltaan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa.

Tehty Brysselissä 15 päivänä heinäkuuta 2026.

Komission puolesta
Puheenjohtaja
Ursula VON DER LEYEN

LIITE I

”LIITE I

Luettelo 3 artiklassa tarkoitetuista viitestandardeista ja -eritelmistä

Sovelletaan standardia ETSI TS 119 471 V1.1.1 (2025-05) seuraavin mukautuksin:

1) 2.1 Normative references:

[1] ETSI EN 319 401 V3.2.1 (2026-01): ”Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers”;

[2] Euroopan kyberturvallisuuden sertifiointiryhmä, Salausta käsittelevä alaryhmä: Euroopan kyberturvallisuusviraston (ENISA) julkaisema asiakirja ”Agreed Cryptographic Mechanisms”;

[3] FIPS PUB 140-3 (2019) ”Security Requirements for Cryptographic Modules”;

[4] Komission täytäntöönpanoasetus (EU) 2024/482 ([1]), 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 ([2]), 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”.

2) 3.1 Terms:
Lisätään käsite seuraavasti:

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

3) 4. EAA trust services

— Lauseketta 4.2.2.2 ”Verification of attributes against authentic sources” ei sovelleta.

— REQ-EAASP-4.2.2.3-02: Sähköisen attribuuttitodistuspalvelun tarjoajan (EAASP) on todennettava eurooppalaisen digitaalisen identiteetin lompakon (EUDIW) ilmentymä toteuttamalla vastavuoroiset todentamismekanismit, joissa käytetään voimassa olevaa pääsyvarmennetta.

— REQ-EAASP-4.2.2.3-03: EAASP on validoitava EUDIW:n yksikö ja se, onko EUDIW:n ilmentymä peruutettu.

— Lauseketta 4.3.2 ”EUDIW Specific” ei sovelleta.

4) 6.1 EAAS practice statement:

— REQ-EAASP-6.1-02: EAASP:n on dokumentoitava peruuttamismekanismi sähköisen attribuuttitodistuspalvelun (EAAS) käytäntöselostuksessa.

5) 6.3 Information security policy:

— REQ-EAASP-6.3-02: EAASP:n on vahvistettava menettelyt, joilla valvontaelimelle ilmoitetaan kaikista muutoksista sähköisten attribuuttitodistusten luottamuspalvelun tarjoamisessa ja aikomuksesta lopettaa kyseinen toiminta, liiketoimintavaatimusten ja asiaankuuluvien lakien ja asetusten mukaisesti, myös asetuksen (EU) N:o 910/2014 24 artiklan 5 kohdan nojalla hyväksyttyjen täytäntöönpanosäädösten vaatimusten mukaisesti. EAASP:n on ilmoitettava valvontaelimelle vähintään

— kuukautta ennen muutoksen toteuttamista;

— kolme kuukautta ennen luottamuspalvelun tarjoamisen suunniteltua lopettamista.

([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).

6) 7.5 Cryptographic controls:

— REQ-EAASP-7.5.2-05: tyhjä

— REQ-EAASP-7.5.2-06: tyhjä

— REQ-EAASP-7.5.3-01A: Salausavaimien, salausalgoritmien ja salauslaitteiden hallintaa varten on oltava käytössä asianmukaisia turvatarkastuksia niiden koko elinkaaren ajan, tarvittaessa kryptoketteryyteen perustuvaa lähestymistapaa noudattaen.

— REQ-EAASP-7.5.3-01B: EAASP:n on valittava ja käytettävä luottamuspalvelujensa tarjoamista varten sopivia salaustekniikoita, jotka ovat Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja ENISAn julkaisemien sovittujen salausmekanismien [2] mukaisia.

— REQ-EAASP-7.5.3-02: EAASP:n on varmistettava, että sen EAA:n digitaalista allekirjoitusta tai leimaa varten käyttämä suojattu salauslaite on hyväksytty allekirjoituksen tai leiman luontiväline ja että kaikki muut digitaaliset allekirjoitukset ja leimat, joita käytetään vastaavan sähköisen attribuuttitodistuksen luottamuspalvelun tai sen osan tarjoamiseen, luodaan sellaisen suojatun salauslaitteen avulla, joka on seuraavien mukaisesti sertifioitu luotettava järjestelmä:

a) tietoteknologian turvallisuuden arviointia koskevat yhteiset kriteerit, sellaisina kuin ne on esitetty asiakirjassa ”Common Criteria for Information Technology Security Evaluation”, versio 3.1 (CC3.1) 31.8.2027 saakka tai versiossa CC:2022, osat 1–5, jonka 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, tai siten kuin ne on vahvistettu standardissa ISO/IEC 15408 [6], ja jotka on sertifioitu vähintään tasolle EAL 4; tai

b) yhteisiin kriteereihin perustuva eurooppalainen kyberturvallisuuden sertifiointijärjestelmä (EUCC) [4][5], joka on sertifioitu vähintään tasolle EAL 4; tai

c) FIPS-140-2, taso 3, jota käytetään 31.8.2027 saakka olemassa olevien sertifioitujen järjestelmien osalta, tai FIPS PUB 140-3 [3], taso 3, jota käytetään 31.12.2030 saakka.

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 [4][5]-sertifiointi, laite on konfiguroitava ja sitä on käytettävä kyseisen sertifioinnin mukaisesti.

— REQ-EAASP-7.5.5-01: tyhjä

— REQ-EAASP-7.5.5-02: tyhjä

— REQ-EAASP-7.5.5-04: tyhjä

7) 7.9 Vulnerabilities and Incident management:

— REQ-EAASP-7.9-02: Seurantatoimissa on otettava huomioon kerättyjen tai analysoitujen tietojen arkaluonteisuus.

8) 7.12 EAASP and EAAS termination and termination plans:

— REQ-EAASP-7.12-04: EAASP:n toiminnan lopettamissuunnitelman on oltava asetuksen (EU) N:o 910/2014 [i.1] 24 artiklan 5 kohdan nojalla hyväksytyissä täytäntöönpanosäädöksissä vahvistettujen vaatimusten mukainen.”

LIITE II

”LIITE II

3 ja 4 artiklassa tarkoitetut tekniset eritelmät

Hyväksyttyjen sähköisten attribuuttitodistusten tarjoajien ja virallisesta lähteestä vastaavan julkisen sektorin elimen myöntämien tai sen puolesta myönnettyjen sähköisten attribuuttitodistusten tarjoajien on myönnettävä todistuksensa vähintään yhden komission täytäntöönpanoasetuksen (EU) 2024/2979 ([1]) liitteessä II mainitun standardin mukaisesti ja sovellettava vastaavia peruuttamistekniikoita, jotka on myös esitetty komission täytäntöönpanoasetuksen (EU) 2024/2979 liitteessä II.”

([1]) Komission täytäntöönpanoasetus (EU) 2024/2979, annettu 28 päivänä marraskuuta 2024, Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 soveltamissäännöistä eurooppalaisten digitaalisen identiteetin lompakoiden eheyden ja ydintoimintojen osalta (EUVL L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

LIITE III

”LIITE IV

Luettelo 9 artiklassa tarkoitetuista viitestandardeista ja -eritelmistä

Tämän asetuksen 9 artiklassa tarkoitettujen tarkastusmekanismien on oltava jommankumman tai molempien seuraavien eritelmien mukaisia seuraavin mukautuksin:

a) tekniset eritelmät, jotka on esitetty asiakirjan ETSI TS 119 478 V1.1.1 (2026-01) ”Electronic Signatures and Trust Infrastructures (ESI); Specification of interfaces related to Authentic Sources” lausekkeessa 6.1.1;

— REQ-ASIP-6.1.1.2-04-01 [EHDOLLINEN]: Jos attributeVerificationResult on joko http://uri.etsi.org/19478/VerificationResult/Match tai http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, attributeVerificationResult voi sisältää elementin attributeValue.

— REQ-ASIP-6.1.1.2-04-02 [EHDOLLINEN]: Jos palautettu attributeVerificationResult on http://uri.etsi.org/19478/VerificationResult/Match ja attributeVerificationResult sisältää attributeValue-elementin, attributeValue-elementin on sisällettävä arvo sellaisena kuin se on pyynnössä.

— REQ-ASIP-6.1.1.2-04-03 [EHDOLLINEN]: Jos palautettu attributeVerificationResult on http://uri.etsi.org/19478/VerificationResult/MatchWithVariation ja attributeVerificationResult sisältää attributeValue-elementin, attributeValue-elementin on sisällettävä attribuutin arvo sellaisena kuin se on tallennettu viralliseen lähteeseen.

— REQ-ASIP-6.1.1.2-06-04-01 [EHDOLLINEN]: Jos fragmentVerificationResult on joko http://uri.etsi.org/19478/VerificationResult/Match tai http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, attributeVerificationResult voi sisältää elementin fragmentValue.

— REQ-ASIP-6.1.1.2-06-04-02 [EHDOLLINEN]: Jos palautettu fragmentVerificationResult on http://uri.etsi.org/19478/VerificationResult/Match ja attributeVerificationResult sisältää fragmentValue-elementin, fragmentValue-elementin on sisällettävä arvo sellaisena kuin se on pyynnössä.

— REQ-ASIP-6.1.1.2-06-04-03 [EHDOLLINEN]: Jos palautettu fragmentVerificationResult on http://uri.etsi.org/19478/VerificationResult/MatchWithVariation ja attributeVerificationResult sisältää fragmentValue-elementin, fragmentValue-elementin on sisällettävä fragmentin arvo sellaisena kuin se on tallennettu viralliseen lähteeseen.

b) tekniset eritelmät, jotka on esitetty asiakirjan ETSI TS 119 478 V1.1.1 (2026-01) ”Electronic Signatures and Trust Infrastructures (ESI); Specification of interfaces related to Authentic Sources” lausekkeessa 6.2.3;

— REQ-ASIP-6.2.3.2.1-08-04: AttributeVerificationResponse-elementti voi sisältää täsmälleen yhden valinnaisen alielementin, joka voi olla TextValue, XMLValue tai AttributeProperties.”