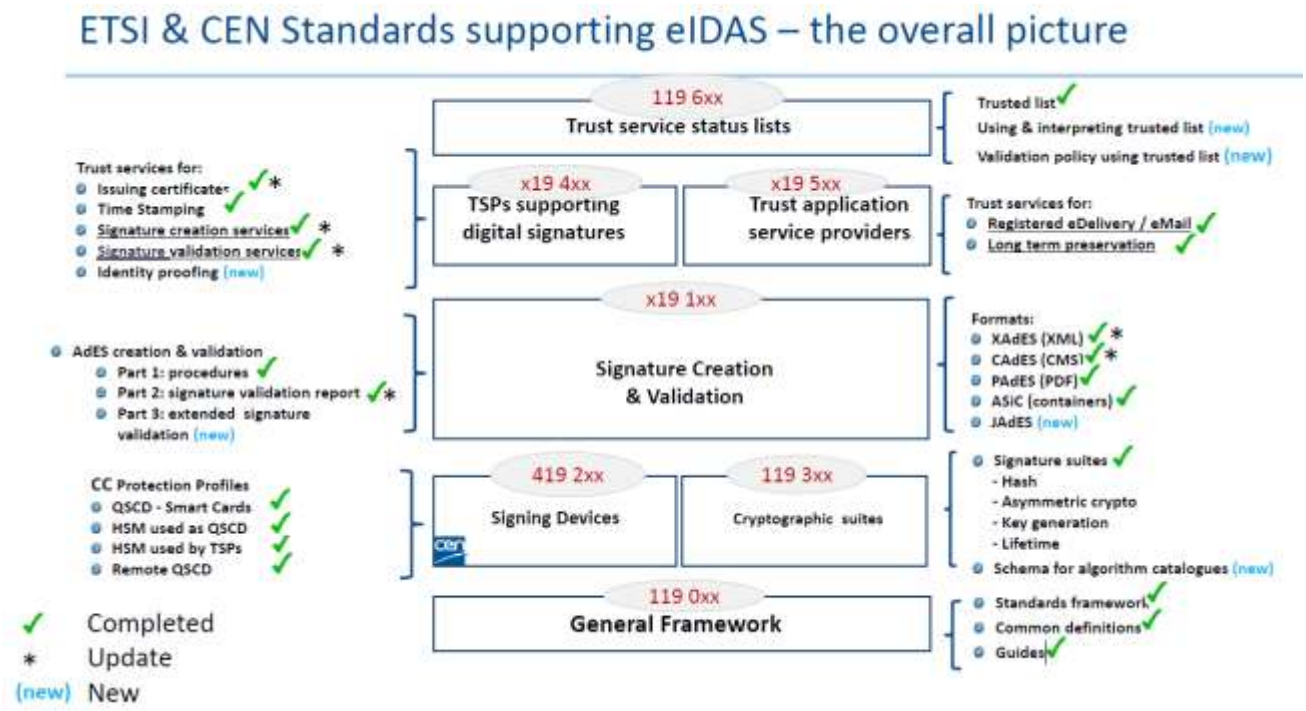
M72 valmistelumuistio 2021, luottamuspalvelut, arviointi- ja sertifiointilaitokset

Contents

LUONNOS 9.4.2021

LUONNOS 9.4.2021

1 Kuva



Kuva 1 ETSI standardit ja luottamuspalvelut, syyskuu 2020. Lähde: Nick Pope, ETSI ESI Vice chair.

2 Säännös ja perustelut (voimassa olevat)

2.1 Säännös 20 § Hyväksytyn luottamuspalvelun tarjoajan arviointikriteerit

20 § Hyväksytyn luottamuspalvelun tarjoajan arviointikriteerit

eIDAS-asetuksessa asetettujen vaatimusten lisäksi hyväksytyn luottamuspalvelun tarjoajan tulee täyttää standardin EN 319 401 vaatimukset.

Varmenteita tarjoavan hyväksytyn luottamuspalvelun tarjoajan tulee momentin 1 vaatimusten lisäksi täyttää standardin EN 319 411-1 vaatimukset.

Sähköisten allekirjoitusten tai leimojen hyväksyttyjä varmenteita tai hyväksyttyjä verkkosivuvarmenteita myöntävän hyväksytyn luottamuspalvelun tarjoajan tulee edellä 1 ja 2 momentissa säädettyjen vaatimusten lisäksi täyttää standardin EN 319 411-2 vaatimukset.

Hyväksyttyjä aikaleimoja myöntävän hyväksytyn luottamuspalvelun tarjoajan tulee edellä 1 ja 2 momentissa säädettyjen vaatimusten lisäksi täyttää standardin EN 319 421 vaatimukset.

Vaatimusten täyttämisen voi osoittaa edellä 1 - 4 momenteissa mainittujen standardien noudattamisella tai muulla tavalla, jolla saavutetaan vastaava luotettavuus.

LUONNOS

2.1.1 Perustelumuistio

Perustelut

eIDAS-asetuksessa määritellään vaatimukset, jotka hyväksytyn luottamuspalvelun tarjoajan tulee täyttää. Vaatimusten sisältöä tarkentamaan Euroopan telestandardointi-instituutti ETSI on laatinut komission mandaatilla luottamuspalveluiden tarjoajia koskevia standardeja. Standardeihin on koottu yksityiskohtaiset konkreettiset vaatimukset, joiden täyttyminen varmistaa sen, että luottamuspalvelun tarjoaja on eIDAS-asetuksen mukainen.

Standardit eivät ole pakollisia, vaan toiminnot voi toteuttaa muullakin tavalla. Standardit osoittavat kuitenkin sen, millaista luotettavuustasoa eIDAS-asetus edellyttää. Jos käytetään muuta vastaavat vaatimukset sisältävää standardia, palvelun toteuttajan on erikseen osoitettava, että toiminta täyttää eIDAS-asetuksen vaatimukset. Määräyksessä viitataan niihin standardeihin, jotka ovat määräyksen antamisen ajankohdalla valmiita.

Luottamuspalveluiden sääntelyn ja määräyksen tavoitteita käsitellään yleisesti vaikutusarvioinnin (ks. A-osa) 3.1 luvussa.

ETSI:n standardit

ETSI standardit on saatettu sellaisenaan voimaan Suomessa ja ne löytyvät myös SFS-standardeina. Tällöin merkitsemistapa on esimerkiksi SFS-EN 319 401.

Seuraavassa on ryhmitelty pykälässä viitattuja standardeja ja kerrottu tällä hetkellä sovellettava standardin versio.

Hyväksytyn luottamuspalvelun tarjoajan yleiset vaatimukset

ETSI EN 319 401 V2.1.1 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [28]

Standardi sisältää yleiset palveluriippumattomat vaatimukset hyväksytyn luottamuspalvelun tarjoajalle. Se sisältää vaatimuksia mm. riskien arvioinnille, tietoturvapolitiikalle ja -käytännölle sekä toiminnan johtamiselle.

Varmenteita myöntävän luottamuspalvelun tarjoajan vaatimukset

ETSI EN 319 411-1 V1.1.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [29]

Standardi sisältää yleiset vaatimukset varmenteita tarjoavalle luottamuspalvelun tarjoajalle. Se täydentää ja tarkentaa standardissa EN 319 401 esitettyjä vaatimuksia. Standardi sisältää yksityiskohtaisia vaatimuksia mm. varmennepolitiikalle ja varmennuskäytännölle. Standardiin liittyy informatiivinen liite C (Conformity Assessment Check list), johon on koottu standardin vaatimukset tarkistuslistan muodossa. Tarkistuslistaa voi hyödyntää esimerkiksi luottamuspalvelun tarjoajan auditoinnissa.

Hyväksyttyjä varmenteita myöntävän luottamuspalvelun tarjoajan vaatimukset

ETSI EN 319 411-2 V2.1.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates [30]

LUONNOS 9.4.2021

Standardi sisältää vaatimukset eIDAS-asetuksen mukaisia hyväksyttyjä varmenteita tarjoavalle luottamuspalvelun tarjoajalle. Se täydentää standardissa EN 319 411-1 esitettyjä vaatimuksia vastaamaan eIDAS-asetuksen erityisvaatimuksia. Lisävaatimukset kohdistuvat mm. varmennepolitiikkaan ja varmennuskäytäntöön.

Standardiin liittyy informatiivinen liite B (Conformity Assessment Check list), johon on koottu standardin vaatimukset tarkistuslistan muodossa. Tarkistuslistaa voi hyödyntää esimerkiksi luottamuspalvelun tarjoajan auditoinnissa.

Hyväksyttyjä aikaleimoja myöntävän luottamuspalvelun tarjoajan vaatimukset

ETSI EN 319 421 V1.1.1 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps [31]

Standardi sisältää tietoturvapolitiikka- ja tietoturvavaatimukset sähköisiä aikaleimoja tarjoavalle luottamuspalvelun tarjoajalle. Standardi viittaa pääsääntöisesti standardin EN 319 401 vaatimuksiin, mutta tarkentaa niitä joiltain osin. Standardi sisältää yksityiskohtaiset vaatimukset aikaleiman allekirjoitusavaimen sisältävän yksikön TSU (Time-Stamping Unit) hallinnalle. Standardiin liittyy informatiivinen liite H (Conformity Assessment Check list), johon on koottu standardin vaatimukset tarkistuslistan muodossa. Tarkistuslistaa voi hyödyntää esimerkiksi luottamuspalvelun tarjoajan auditoinnissa.

2.2 Säännös 21 Hyväksytyn luottamuspalvelun arviointikriteerit

21 § Hyväksytyn luottamuspalvelun arviointikriteerit

Hyväksytyn luottamuspalvelun myöntämien varmenteiden tulee täyttää eIDAS-asetuksessa sähköisen allekirjoituksen ja leiman varmenteille sekä verkkosivujen varmenteille asetettujen vaatimusten lisäksi standardeissa EN 319 412-1, EN 319 412-2, EN 319 412-3, EN 319 412-4 ja EN 319 412-5 esitetyt vaatimukset soveltuvin osin.

Hyväksytyssä aikaleimapalvelussa tulee käyttää standardin EN 319 422 mukaista protokollaa ja aikaleiman profiilia.

Vaatimusten täyttämisen voi osoittaa edellä 1 - 2 momenteissa mainittujen standardien noudattamisella tai muulla tavalla, jolla saavutetaan vastaava luotettavuus.

2.2.1 Perustelumuistio

Perustelut ja soveltaminen

EU-säädännössä hyväksyttyjä luottamuspalveluita voivat olla ovat sähköiset allekirjoitukset ja leimat, niihin liittyvät validointi- ja säilyttämispalvelut, sähköiset aikaleimat, sähköiset rekisteröidyt jakelupalvelut ja verkkosivustojen todentaminen (ks. tarkemmin LIITE 1)

Sähköisten allekirjoitusten, sähköisten leimojen ja verkkosivustojen todentamisen hyväksytyt varmenteet

eIDAS-asetuksen liitteissä I, III ja IV määritellään sähköisten allekirjoitusten, sähköisten leimojen ja verkkosivustojen todentamisen hyväksyttyjä varmenteita koskevat vaatimukset.

LUONNOS 9.4.2021

Vaatimusten sisältöä tarkentamaan Euroopan telestandardointi-instituutti ETSI on laatinut komission mandaatilla määräystekstissä luetellut standardit. Standardeihin on koottu yksityiskohtaiset konkreettiset vaatimukset, joiden täyttyminen varmistaa sen, että luottamuspalvelu on eIDAS-asetuksen mukainen.

Standardit eivät ole pakollisia, vaan palvelut voi toteuttaa muullakin tavalla. Standardit osoittavat kuitenkin sen, millaista luotettavuustasoa eIDAS-asetus edellyttää palveluissa. Jos palvelun toteuttaa viitatun standardin mukaisesti, eIDAS-asetuksen vaatimukset tulevat huomioiduksi. Jos käytetään muuta vastaavat vaatimukset sisältävää standardia, palvelun toteuttajan on erikseen osoitettava, että palvelu täyttää eIDAS-asetuksen vaatimukset.

Määräyksessä lueteltuihin varmenneprofiileihin sisältyvät yleiset vaatimukset sisältävä standardi, varmenteen tarkoitetun sovelluksen mukaisia standardeja sekä hyväksyttyjen varmenteiden sisällön (statements) määrittelevä standardi. Siltä osin kuin standardeissa on eritelty EU-säädännön vaatimusten täyttymistä koskevat ja muita vaatimuksia koskevat osat, tämän määräyksen kannalta soveltuvina osina pidetään EU-säädännön täyttymiseen liittyviä vaatimuksia.

Varmenneprofiilit - yleinen: *ETSI EN 319 412-1 V1.1.0 (2015-12) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures [32]*

Varmenneprofiilit - luonnollinen henkilö: *ETSI EN 319 412-2 V2.1.0 (2015-12) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons [33]*

Varmenneprofiilit - oikeushenkilö: *ETSI EN 319 412-3 V1.1.0 (2015-12) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons [34]*

Varmenneprofiilit - verkkosivuvarmenteet: *ETSI EN 319 412-4 V1.1.0 (2015-12) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates [35]*

Varmenneprofiilit - QCStatements: *ETSI EN 319 412-5 V2.1.0 (2015-12) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements [36]*

Hyväksytty sähköinen aikaleima

eIDAS asetuksen 42 artikla sisältää vaatimukset hyväksytylle sähköiselle aikaleimalle. Toistaiseksi vaatimusten sisältöä tarkentamaan Euroopan telestandardointi-instituutti ETSI on laatinut komission mandaatilla ainoastaan määräystekstissä mainitun standardin EN 319 422. Jos aikaleimapalvelun protokolla ja profiili on toteutettu kyseisen standardin mukaisesti, eIDAS-asetuksen vaatimukset niiltä osin täyttyvät. Jos käytetään muuta vastaavat vaatimukset sisältävää standardia, palvelun toteuttajan on erikseen osoitettava, että eIDAS-asetuksen vaatimukset täyttyvät.

ETSI EN 319 422 V1.1.0 (2015-12) Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles [37]

21.1 Perustelumuistio 2016: Luottamuspalvelut, joiden vaatimuksista ei määrätä

Hyväksytyn sähköisen rekisteröidyn jakelupalvelun vaatimukset säädetään eIDAS-asetuksen 44 artiklassa. Palveluiden standardointi on kesken, joten määräyksessä

LUONNOS 9.4.2021

ei viitata tarkempiin vaatimuksiin. Sähköisen rekisteröidyn jakelupalvelun standardit on tarkoitus valmistella ETSIssä standardisarjaan EN 319 522-1…4.

Tekeillä on standardi ETSI EN 319 521 Policy & security requirements for electronic registered delivery service providers [38], jonka pohjana tulee olemaan REM (Registered Electronic Mail) -spesifikaatioita koskeva TS 102 640-x -spesifikaatiosarja [39].

REM-spesifikaatiotkin on tarkoitus uusia tulevaisuudessa ja julkaista standardisarjana EN 319 532-1…5. REM-standardeja voi hyödyntää pohjana sähköisen rekisteröidyn jakelupalvelun toteutuksen suunnittelussa, mutta lopulliset vaatimukset tullaan määrittelemään standardisarjassa EN 319 522-1…4.

REM-spesifikaatiot

- *TS 102 640-1 Ver. 2.2.1 Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 1: Architecture*
- *TS 102 640-2 Ver. 2.2.1 Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 2: Data requirements, Formats and Signatures for REM*
- *TS 102 640-3 Ver. 2.1.2 Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 3: Information Security Policy Requirements for REM Management Domains*
- *TS 102 640-4 Ver. 2.1.2 Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 4: REM-MD Conformance Profiles*
- *TS 102 640-5 Ver. 2.1.2 Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 5: REM-MD Interoperability Profiles*

2.3 Säännös 22 § Arviointilaitosten pätevyyden arviointi

22 § Arviointilaitosten pätevyyden arviointi

Luottamuspalveluiden vaatimustenmukaisuuden arviointilaitoksen osalta tunnistus- ja luottamuspalvelulain 33 §:n 1 momentin 3 kohdan ja 4 kohdan vaatimusten täyttymisen edellytyksenä on, että arviointilaitos täyttää standardin EN 319 403 tai vastaavat vaatimukset.

Luottamuspalveluiden vaatimustenmukaisuuden arviointilaitoksen osalta tunnistus- ja luottamuspalvelulain 33 §:n 1 momentin 2 kohdan vaatimuksen täyttymisen edellytyksenä on riittävä pätevyys edellä 20 §:ssa lueteltujen luottamuspalveluiden tarjoajia koskevien ja 21 §:ssa lueteltujen luottamuspalveluita koskevien arviointikriteerien mukaisten arviointien suorittamiseen.

2.3.1 Perustelumuistio

Komissio ei ole laatinut täytäntöönpanopäätöstä, jolla tarkennettaisiin eIDAS-asetuksen 20.4 artiklan nojalla vaatimuksenmukaisuuden arviointilaitosta koskevat standardit.

LUONNOS 9.4.2021

Eurooppalaisten akkreditointiorganisaatioiden yhteistyöelin EA (European Co-operation for Accreditation) on laatinut dokumentin EA Certification Committee Reference Paper; ETSI / EA Recommendations regarding; Preparation for Audit under EU Regulation (EU) No 910/2014 Article 20.1.[40] Siinä määritellään, miten luottamuspalveluiden vaatimustenmukaisuuden arviointilaitosten (Conformity Assessment Bodies, CAB) akkreditoinnissa siirrytään aiemmasta käytännöstä eIDAS-asetuksen mukaiseen käytäntöön ja mitä vaatimuksia akkreditoinnissa edellytetään arviointilaitoksen täyttävän ja minkä asioiden osalta sillä pitää olla pätevyys. Pohjana ovat ETSIn laatimat standardit.

Koska komissio ei ole valmistelemassa asiaa koskevaa täytäntöönpanosäännöstä, EA:n dokumentissa luetellut standardit toimivat pohjana vaatimustenmukaisuuden arviointilaitosten akkreditoinnissa ja hyväksynnässä.

Vaatimustenmukaisuuden arviointilaitoksen vaatimukset on määritelty standardissa ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers [41]. Standardi pohjautuu standardiin ISO/IEC 17065, joka määrittelee yleiset vaatimukset arviointilaitoksille. Standardi EN 319 403 täydentää ISO/IEC-standardin vaatimuksia erityisesti luottamuspalveluiden tarjoajia ja niiden tarjoamia palveluita koskevilla vaatimuksilla.

Tunnistus- ja luottamuspalvelulain mukaisesti arviointilaitoksella tulee olla pätevyys arvioida palveluntarjoajaa ja sen tarjoamia palveluita. Määräyksen 20 § ja 21 § sisältävät vaatimukset luottamuspalveluiden tarjoajalle ja luottamuspalvelulle, joten arviointilaitokselta tulee edellyttää pätevyyttä pykälissä mainittujen standardien mukaiseen arviointiin.

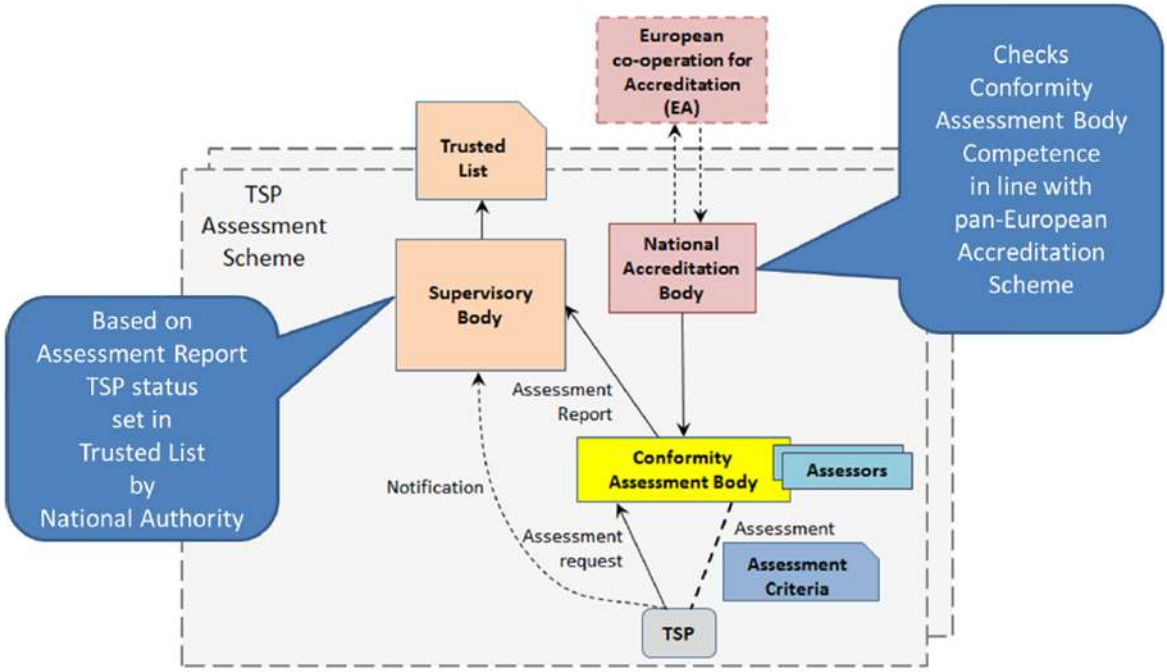
2.3.2 Perustelumuistio 2016: Arviointilaitoksen akkreditointi ja hyväksyntä

Vaatimustenmukaisuuden arviointilaitoksen aseman saaminen edellyttää tunnistus- ja luottamuspalvelulain mukaisten riippumattomuus- ja pätevyysvaatimusten osoittamista FINASilta [4] haettavalla akkreditoinnilla. Kun FINAS tekee vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta annetun lain (920/2005) tarkoittaman päätöksen arviointilaitoksen akkreditoinnin kriteereistä, se voi huomioida muitakin riippumattomuuden ja pätevyyden arviointiin liittyviä vaatimuksia kuin tässä määräyksessä viitatut standardit.

Lisäksi laitoksen tulee hakea hyväksyntä Viestintävirastolta. Hyväksynnän edellytyksenä on FINASin akkreditointi ja selvitys tunnistuslain 33.1 §:n 4 kohdan edellyttämien ohjeista ja niiden seurannasta.

Seuraavassa kuvassa kuvataan yleisen akkreditointisääntelyn ja eIDAS-asetuksen sektorikohtaisen valvonnan suhteita sähköisen luottamuspalvelun vaatimustenmukaisuuden arvioinnissa.

LUONNOS 9.4.2021



Kuva 2: Luottamuspalvelun tarjoajan arvioinnin kaavio

(Lähde Euroopan tietoturvallisuusviraston ENISAn dokumentti *Auditing Framework for TSPs, Guidelines for Trust Service Providers, Versio 1.0 - December 2014* [42])

2.4 Säännös 23 § Sähköisen allekirjoituksen tai leiman luontivälineen vaatimukset

23 § Sähköisen allekirjoituksen tai leiman luontivälineen vaatimukset

Käyttäjän hallussa fyysisesti olevan sirupohjaisen sähköisen allekirjoituksen tai leiman luontivälineen vaatimuksista säädetään EU:n komission täytäntöönpanopäätöksessä (EU) 2016/650[1].

---

[1] *KOMISSION TÄYTÄNTÖÖNPANOPÄÄTÖS (EU) 2016/650, annettu 25 päivänä huhtikuuta 2016, hyväksyttyjen allekirjoituksen ja leiman luontivälineiden tietoturva-arviointia koskevien standardien vahvistamisesta sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:O 910/2014 30 artiklan 3 kohdan ja 39 artiklan 2 kohdan mukaisesti*

2.4.1 Perustelumuistio

Vaatimukset tukeutuvat komission täytäntöönpanopäätökseen (EU) 2016/650 [43].

LUONNOS 9.4.

[1] KOMISSION TÄYTÄNTÖÖNPANOPÄÄTÖS (EU) 2016/650, annettu 25 päivänä huhtikuuta 2016, hyväksyttyjen allekirjoituksen ja leiman luontivälineiden tietoturva-arviointia koskevien standardien vahvistamisesta sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 30 artiklan 3 kohdan ja 39 artiklan 2 kohdan mukaisesti

Komission täytäntöönpanopäätöksessä vahvistetaan sertifioinnin pohjaksi seuraavat standardit. Niistä yleinen IT-tietoturvallisuuden arvioinnin standardi ISO/IEC 15408 Information technology -- Security techniques -- Evaluation criteria for IT security -standardisarja [44] tunnetaan Common Criteria -vaatimuksina.

Muut komission täytäntöönpanopäätöksessä vahvistetut standardit ovat

- ISO/IEC 18045:2008 – Information technology – Security techniques – Methodology for IT security evaluation [45]

- EN 419 211 – Protection profiles for secure signature creation de-vice, osat 1–6 [46] – tarpeen mukaan – seuraavasti:

> *O EN 419211–1:2014 – Protection profiles for secure signature creation device – Part 1: Overview*
>
> *O EN 419211–2:2013 – Protection profiles for secure signature creation device – Part 2: Device with key generation*
>
> *O EN 419211–3:2013 – Protection profiles for secure signature creation device – Part 3: Device with key import*
>
> *O EN 419211–4:2013 – Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted channel to certificate generation application*
>
> *O EN 419211–5:2013 – Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted channel to signature creation application*
>
> *O EN 419211–6:2014 – Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted channel to signature creation application*

2.4.2 Perustelumuistio 2016: Palvelinpohjaisen allekirjoitusvälineen ja allekirjoituspalvelun keskeneräiset standardit

<u>Etäväline</u>

eIDAS-asetus ja komission täytäntöönpanopäätös koskevat myös sellaisia allekirjoituksen tai leiman luontitapoja, joissa luontivälineet eivät ole fyysisesti käyttäjän hallinnassa, vaan jossa ne ovat palvelimella. Standardointi palvelinpohjaisen toteutuksen tietoturvallisuusvaatimuksista on käynnissä, mutta vielä kesken. Koska standardeja ei vielä ole, komission täytäntöönpanopäätöksessä ei ole viittauksia standardeihin tai muita tarkennuksia eIDAS-asetuksen vaatimuksiin.

CEN [47] on valmistelemassa standardeja sellaisen allekirjoituksen luontivälineen vaatimuksista, joka ei ole fyysisesti allekirjoituksen tekijän hallinnassa.

Määräykseen ei ole otettu viittausta keskeneräisiin standardeihin tai pyritty laatimaan kansallisesti tarkempia teknisiä määrittelyjä palvelinpohjaisen allekirjoituksen luontivälineen vaatimuksille. Viestintäviraston näkemyksen mukaan ei ole olemassa edellytyksiä määritellä vaatimuksia, joiden nojalla voitaisiin riittävän perusteellisesti arvioida palvelun luotettavuus siten, että vaatimukset olisivat ennakoitavasti hyväksyttäviä myös muissa EU-maissa.

LUONNOS 9.4.2021

Koska toimijoilla on paljonkin kiinnostusta palvelinpohjaisten allekirjoitusten tuottamiseen, tilanne on markkinoiden kannalta epätyydyttävä sikäli, että luontivälineille ei ole käytännössä mahdollista saada eIDAS-asetuksen mukaista sertifioitua statusta. Tilanne toivottavasti selkeytyy lähivuosina, kun kansainvälinen standardointi etenee.

Allekirjoituspalvelun standardoinnin tilanne

ETSIssä on käynnistynyt standardointityö allekirjoituspalveluiden vaatimusten määrittelemiseksi.

Valmisteilla ovat seuraavat standardit:

- *(119 432-1) DTS/ESI-0019432-1 Protocol for TSPs providing signature generation services - Part 1 Trusted Service manager [48]*
- *(119 432-2) DTS/ESI-0019432-2 Protocol for TSPs providing signature generation services - Part 2: local signing on mobile device*
- *(119 432-3) DTS/ESI-0019432-3 Protocol for TSPs providing signature generation services - Part 3: local signing on general device*
- *(119 432-4) DTS/ESI-0019432-4 Protocol for TSPs providing signature generation services - Part 4: remote signing*
- *(119 442) DTS/ESI-0019442 Protocol for TSPs providing signature validation services [49]*

Vaikutusarvioinnin (ks. A osa) luvussa 3.8 käsitellään sitä, että Suomessa ei merkitä luotetulle listalle muita kuin eIDAS-asetuksen mukaisia hyväksyttyjä luottamuspalveluja, mikä pitää sisällään sekä palvelutyyppien rajoitukset että hyväksyntäperusteet.

2.5 Säännös 24 Sertifiointilaitosta koskevat vaatimukset

24 § Sertifiointilaitosta koskevat vaatimukset

Tunnistus- ja luottamuspalvelulain 36 § vaatimusten täyttymisen edellytyksenä on riittävä pätevyys ja resurssit eIDAS-asetuksessa ja edellä 23 §:ssä mainitussa komission täytäntöönpanopäätöksessä asetettujen vaatimusten todentamiseen sertifioitavana olevassa välineessä.

Edellä 1 momentissa tarkoitettujen vaatimusten täyttymisen voi osoittaa akkreditoinnilla tai muulla riippumattomalla selvityksellä. Pätevyyden osoituksena voi olla myös kuuluminen eräiden Euroopan unionin tai ETA-alueen jäsenvaltioissa toimivien sertifiointielinten välisen SOGIS-MRA (Senior Officers Group for Information Systems, Mutual Recognition Agreement) –sopimuksen piiriin.

2.5.1 Perustelumuistio

Jos jokin suomalainen sertifioija haluaa hakeutua hyväksytyksi sertifiointilaitokseksi, se voi hakea hyväksyntää Viestintävirastolta tunnistus- ja luottamuspalvelulain 36 §:n mukaisesti ja pykälässä säädetyillä edellytyksillä.

Tämän määräyksen 24 pykälän 2 momentissa määrätään siitä, miten pätevyyden voi osoittaa. Mahdollisia tapoja ovat ainakin akkredointi, joka tarkoittaa FINASin

LUONNOS 9.4.2021

tekemään pätevyyden arviointia, tai liittyminen SOGIS-MRA -sopimuksen vertaisarviointiin perustuvaan pätevyyden arviointimenettelyyn.

SOGIS-MRA (Senior Officers Group for Information Systems, Mutual Recognition Agreement)[50] on eurooppalainen järjestelmä sertifiointien keskinäiseen tunnustamiseen. Mukana on kahdeksan maata, joilla on omia sertifioijia (qualified/authorising participant) ja kaksi maata (consuming participant), joilla ei ole omia sertifioijia (mm. Suomi). Järjestelmässä käytettävät standardit SSCD (Secure Signature Creation Device) -alueella ovat komission täytäntöönpanosäännöksen nimeämät EN 419 211-sarjan standardit.

EU:n tai ETA-alueen jäsenvaltioiden komissiolle ilmoittamien jäsenvaltioissa hyväksyttyjen sertifiointilaitosten tekemät sertifioinnit ovat sellaisenaan pätevä myös Suomessa. Tällä hetkellä suuri osa komissiolle ilmoitetuista sertifiointielimistä kuuluu myös SOGIS-MRA -sopimuksen piiriin.

2.6 Perustelumuistio 2016, C-osa Määräyksen aihepiiriin liittyvät muut asiat, Kehittyneet sähköiset allekirjoitukset

Tausta

Joissain laeissa edellytetään allekirjoittamista kehittyneellä sähköisellä allekirjoituksella, josta säädetään eIDAS-asetuksessa.

Esimerkiksi sähköisestä asioinnista viranomaistoiminnassa annetun lain 16 §:ssä edellytetään kehittynyttä sähköistä allekirjoitusta tai muuta vastaavankaltaista tapaa:

> *Päätösasiakirja voidaan allekirjoittaa sähköisesti. Viranomaisen on allekirjoitettava asiakirja sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 26 artiklassa tarkoitetulla kehittyneellä sähköisellä allekirjoituksella tai muuten sellaisella tavalla, että asiakirjan alkuperäisyydestä ja eheydestä voidaan varmistautua.*

Viestintävirastoon tulee kysymyksiä, joissa tiedustellaan, täyttääkö jokin tarjottu palvelu kehittyneeltä sähköiseltä allekirjoitukselta edellytettävät vaatimukset ja kelpaako se siten asiakirjojen allekirjoittamiseen.

eIDAS-asetuksen mukaan kehittyneet sähköiset allekirjoitukset tai allekirjoituspalvelut eivät ole hyväksyttyjä luottamuspalveluita. Tunnistus- ja luottamuspalvelulain 42 a §:n perusteella niitä ei merkitä asetuksen 22 artiklan mukaiseen luotettuun luetteloon. Tunnistus- ja luottamuspalvelulain 42 a §:n ja eIDAS-asetuksen 17.3 artiklan perusteella Viestintävirasto valvoo ei-hyväksyttyjä luottamuspalveluja vain jälkikäteen. Sähköisen asiointipalvelun toteuttajan ja sähköisen allekirjoituspalvelun tarjoajan on siten arvioitava, täyttääkö tietty palvelu kehittyneen sähköisen allekirjoituksen tunnusmerkistön ja vaatimukset.

Tässä luvussa kuvataan kehittyneiden sähköisten allekirjoitusten ominaisuuksia arvioinnin tueksi.

Säädäntötausta

LUONNOS 9.4.2021

Kehittyneen sähköisen allekirjoituksen vaatimukset määritellään eIDAS-asetuksen 26 artiklassa. Sen mukaan kehittyneen sähköisen allekirjoituksen on täytettävä seuraavat vaatimukset:

> *a) se liittyy yksilöivästi allekirjoittajaansa;*
>
> *b) sillä voidaan yksilöidä allekirjoittaja;*
>
> *c) se on luotu käyttäen sähköisen allekirjoituksen luontitietoja, joita allekirjoittaja voi korkealla varmuustasolla käyttää yksinomaisessa valvonnassaan; ja*
>
> *d) se on liitetty sillä allekirjoitettuun tietoon siten, että tiedon mahdollinen myöhempi muuttaminen voidaan havaita.*

Julkisen hallinnon sähköisistä allekirjoituksista säädetään tarkemmin eIDAS-asetuksen 27 artiklassa:

> *1. Jos jäsenvaltio vaatii kehittynyttä sähköistä allekirjoitusta julkisen sektorin elimen tarjoaman tai sen puolesta tarjotun verkkopalvelun käyttämiseksi, kyseisen jäsenvaltion on tunnustettava ainakin ne kehittyneet sähköiset allekirjoitukset, sähköisten allekirjoitusten hyväksyttyyn varmenteeseen perustuvat kehittyneet sähköiset allekirjoitukset sekä hyväksytyt sähköiset allekirjoitukset, jotka ovat 5 kohdassa tarkoitetuissa täytäntöönpanosäädöksissä määritellyissä muodoissa tai joissa käytetään niissä tarkoitettuja menettelyjä.*
>
> *2. Jos jäsenvaltio vaatii hyväksyttyyn varmenteeseen perustuvaa kehittynyttä sähköistä allekirjoitusta julkisen sektorin elimen tarjoaman tai sen puolesta tarjotun verkkopalvelun käyttämiseksi, kyseisen jäsenvaltion on tunnustettava ainakin ne hyväksyttyyn varmenteeseen perustuvat kehittyneet sähköiset allekirjoitukset sekä hyväksytyt sähköiset allekirjoitukset, jotka ovat 5 kohdassa tarkoitetuissa täytäntöönpanosäädöksissä määritellyissä muodoissa tai joissa käytetään niissä tarkoitettuja menettelyjä.*
>
> *3. Jäsenvaltiot eivät saa vaatia julkisen sektorin elimen tarjoaman verkkopalvelun käytössä rajojen yli sähköistä allekirjoitusta, jonka tietoturvataso on korkeampi kuin hyväksytyn sähköisen allekirjoituksen.*
>
> *4. Komissio voi täytäntöönpanosäädöksin vahvistaa kehittyneisiin sähköisiin allekirjoituksiin sovellettavien standardien viitenumerot. Jos kehittynyt sähköinen allekirjoitus vastaa kyseisiä standardeja, sen katsotaan olevan tämän artiklan 1 ja 2 kohdassa sekä 26 artiklassa tarkoitettujen kehittyneitä sähköisiä allekirjoituksia koskevien vaatimusten mukainen. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.*
>
> *5. Komissio määrittelee kehittyneitä sähköisiä allekirjoituksia koskevat viitemuodot tai, jos käytetään vaihtoehtoisia muotoja, viitemenetelmät täytäntöönpanosäädöksillä viimeistään 18 päivänä syyskuuta 2015 ottaen huomioon olemassa olevat käytännöt, standardit ja unionin säädökset. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.*

*Komissio on antanut täytäntöönpanopäätöksen (EU) 2015/1506 eritelmien vahvistamisesta sellaisia **kehittyneiden sähköisten allekirjoitusten ja kehittyneiden***

LUONNOS 9.4.2021

leimojen muotoja *varten, jotka julkisen sektorin elinten on tunnustettava sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 27 artiklan 5 kohdan ja 37 artiklan 5 kohdan mukaisesti. [52]*

Täytäntöönpanopäätöksestä ilmenevät tekniset vaatimukset kuvataan seuraavassa luvussa.

Kehittyneiden sähköisten allekirjoitusten tekniset vaatimukset

Komission täytäntöönpanopäätös (EU) 2015/1506 [52] sisältää luettelon eritelmien vahvistamisesta sellaisia kehittyneiden sähköisten allekirjoitusten ja kehittyneiden leimojen muotoja varten, jotka julkisen sektorin elinten on tunnustettava Eidas-asetuksen 27 artiklan 5 kohdan ja 37 artiklan 5 kohdan mukaisesti. Täytäntöönpanopäätöksessä on luettelo standardeista:

- *XAdES perustason profiili ETSIn tekninen eritelmä 103171 v.2.1.1 [53]*
- *CAdES perustason profiili ETSIn tekninen eritelmä 103173 v.2.2.1 [54]*
- *PAdES perustason profiili ETSIn tekninen eritelmä 103172 v.2.2.2 [55]*
- *Assosioitujen allekirjoitusten säilötiedoston perustason profiili ETSIn tekninen eritelmä 103174 v.2.2.1 [56]*

Jos muita formaatteja käytetään, on tarjottava validointimahdollisuus ((EU) 2015/1506 art. 2). Sähköinen leima noudattaa samoja standardeja kuin allekirjoituskin. Erona on vain se, että leima tehdään oikeushenkilön nimissä ja se mahdollistaa esimerkiksi järjestelmäallekirjoituksen.

Seuraavassa Viestintävirasto esittää alustavia havaintoja kehittyneen sähköisen allekirjoituksen tunnusmerkistön arvioinnista suhteessa siru- ja palvelintoteutuksiin. Mainitut tavat ovat vain havaintoja ja poimintoja mahdollisista toteutustavoista, eikä Viestintävirasto ole arvioinut toteutustapoja tai yksittäisiä palveluita tarkasti tai selvittänyt muiden jäsenvaltioiden viranomaisten kantoja eIDAS-asetuksen tulkinnasta.

Kehittynyt sähköinen allekirjoitus

a) liittyy yksilöivästi allekirjoittajaansa

- *Vaatimuksen voi täyttää esimerkiksi siten, että sirulla säilytetään yksityistä avainta, jolla luotu allekirjoitus voidaan tarkistaa käyttämällä julkisesta hakemistosta haettua varmennetta (joka sisältää julkisen avaimen ja yksilöivät tiedot). Tällainen allekirjoitus liittyy yksilöivästi allekirjoittajaansa*
- *Vaatimuksen voi käyttää myös esimerkiksi siten, että palvelimella allekirjoituksessa yhdistetään tunnistaminen ja asiakirja. Ero edelliseen esimerkkiin on siinä, että palvelin hallinnoi avaintietoja.*
- *Sirupohjaisia PKI-varmenteita tarjoaa ainakin Västörekisterikeskus. Myös mobiilivarmenne mahdollistaa PKI-toteutuksen.*

b) voidaan yksilöidä allekirjoittaja

LUONNOS 9.4.2021

- *Vaatimuksen voi täyttää esimerkiksi siten, että siruun liittyvässä varmennehakemistossa olevassa varmenteessa on henkilön SATU (Sähköisen asioinnin tunniste) tai organisaatiovarmenteessa tieto henkilöstä ja organisaatiosta.*

- *Vaatimuksen voi täyttää myös esimerkiksi siten, että kirjautuja tunnistetaan vahvalla sähköisellä tunnistusvälineellä, kuten TUPAKsella.*

c) luotu käyttäen sähköisen allekirjoituksen luontitietoja, joita allekirjoittaja voi korkealla varmuustasolla käyttää yksinomaisessa valvonnassaan

- *Vaatimuksen voi täyttää esimerkiksi siten, että luontitiedot ovat sirulla käyttäjän hallussa ja suojattuna esimerkiksi PIN-koodilla.*

- *Avoin kysymys on, miten taataan luontitietojen luottamuksellisuus palvelimella.*

- *Yksinomaan vahva sähköinen tunnistaminen ei turvaa luontitietojen hallintaa allekirjoittajalle.*

d) liitetty sillä allekirjoitettuun tietoon siten, että tiedon mahdollinen myöhempi muuttaminen voidaan havaita.

- *Vaatimuksen voi täyttää ainakin kaikilla PKI-toteutuksilla, koska niissä allekirjoitus tehdään laskemalla allekirjoitettavasta tiedosta niin sanottu tiiviste. Jos allekirjoitettavaa tietoa muutetaan, muuttuu myös allekirjoitus (tiiviste). Vertailemalla tiedon allekirjoitusta (tiivistettä) ja tiedon vastaanottajan laskemaa tiivistettä keskenään voidaan havaita, onko allekirjoitettua tietoa muutettu allekirjoittamisen jälkeen.*

- *Lisäksi tiivisteen salaamisella varmistetaan se, ettei allekirjoitetusta dokumentista laskettua tiivistettä voida muuttaa.*

- *Kaiken kaikkiaan on vakiintuneesti nähty PKI-arkkitehtuuri kehittyneen sähköisen allekirjoituksen toteutustapana ja on avoin kysymys, voiko sen toteuttaa muulla tavoin.*

3 Lähteet päivittämiseen

3.1 Yleistä

3.1.1 Hyväksytyt ja ei-hyväksytyt luottamuspalvelutyypit

eIDAS-asetuksen hyväksytyt (qualified) luottamuspalvelut voivat olla seuraavia

- Qualified certificate for electronic signature
- Qualified certificate for electronic seal
- Qualified certificate for website authentication
- Qualified validation Service for qualified electronic signature
- Qualified preservation Service for qualified electronic signature
- Qualified validation Service for qualified electronic seal
- Qualified preservation Service for qualified electronic seal
- Qualified time stamp
- Qualified electronic registrered delivery Service

LUONNOS 9.4.2021

Ei-hyväksytyt (non-qualified) luottamuspalvelut ovat seuraavia (lista on kopioitu komission hakukoneesta)

- Certificate for electronic signature
- Certificate for electronic seal
- Certificate for website authentication
- Validation Service for electronic signature
- Generation Service for electronic signature
- Preservation Service for electronic signature
- Validation Service for electronic seal
- Generation Service for electronic seal
- Preservation Service for electronic seal
- Time stamp Service Electronic registrered delivery
- Service Non-regulatory, nationally defined trust Service
- Undefined type

3.1.2 Määräyksen säännökset ja tarkoitus

Määräyksen 6-8 luvuissa määrätään eIDAS-asetuksen hyväksytyistä luottamuspalveluista, niiden vaatimustenmukaisuuden arviointilaitoksista sekä sähköisen allekirjoituksen tai leiman luontivälineen sertifioinnista.

Luku 6 Hyväksytyt luottamuspalvelut

20 § Hyväksytyn luottamuspalvelun tarjoajan arviointikriteerit

21 § Hyväksytyn luottamuspalvelun arviointikriteerit

Luku 7 Luottamuspalvelujen vaatimustenmukaisuuden arviointilaitokset

22 § Arviointilaitosten pätevyyden arviointi

Luku 8 Hyväksytyn sähköisen allekirjoituksen ja sähköisen leiman luontivälineen sertifiointi

23 § Sähköisen allekirjoituksen tai leiman luontivälineen vaatimukset

24 § Sertifiointilaitosta koskevat vaatimukset

Määräyksen tarkoitus on

• täydentää hyväksyttyjen sähköisten luottamuspalveluiden vaatimuksia ja niiden vaatimustenmukaisuuden arvioinnin riippumattomuus- ja pätevyyskriteereitä siltä osin, kun näistä ei ole säädetty Euroopan unionin lainsäädännössä, sekä

• täydentää sähköisen allekirjoituksen tai sähköisen leiman luontivälineen sertifioinnin kriteereitä siltä osin, kun näistä ei ole säädetty Euroopan unionin lainsäädännössä.

Määräysvaltuus on rajattu ja siinä on tarkoin huomioitava EU-sääntely ja kansainvälisen standardoinnin tilanne.

Viraston arvion mukaan määräysmuutoksessa on keskeisintä tarkastella ETSI:n standardoinnin edistymistä. Määräysvalmistelussa on myös seurattava käynnissä olevaa eIDAS-asetuksen uudelleenarviointia ja mahdollisia komission täytäntöönpanosäädöksiä luottamuspalveluista sekä arviointilaitoksista.

LUONNOS 9.4.2021

3.2 Vuonna 2016 ja 2018 vaikutusarvioinneissa linjatut asiat

3.2.1 Vaikutusarviointi 2016: Tietoyhteiskuntavaikutukset, luottamuspalvelut, arviointitoiminta

Luottamuspalvelut

Yleisesti luottamuspalveluiden sääntelyn tavoitteena on tietoyhteiskunta-kehitys ja luottamuksen lisääminen sähköiseen asiointiin. Luottamuspalveluiden sääntelyllä autetaan sähköisten palveluiden toteuttajia ja käyttäjiä tunnistamaan ne palvelut, joiden avulla on mahdollista toteuttaa sähköisten asiointipalveluiden eri toiminnot mahdollisimman tietoturvallisesti.

Määräyksen tavoitteena on selkeyttää hyväksyttyjen luottamuspalvelujen eIDAS-asetuksessa säädettyjä vaatimuksia viittaamalla EU:n valmistelu-työssä viitoittamiin kansainvälisiin standardeihin siltä osin, kun niihin ei ole ainakaan toistaiseksi tehty viittauksia komission täytäntöönpanosäädöksillä, vaikka siihen olisi eIDAS-asetuksessa toimivalta.

Standardiviittaukset määräyksessä tukevat myös sitä, mitä ainakin tulee huomioida mahdollisten vaatimustenmukaisuuden arviointilaitosten pätevyysvaatimuksena, kun niitä akkreditoidaan.

Arviointitoiminta

Viestintäviraston määräyksen tavoitteena on selkeyttää toimijoille ja vaatimustenmukaisuuden arviointilaitoksille luottamuspalveluiden vaatimuksia siltä osin, kun komissio ei ole käyttänyt luottamuspalveluihin liittyvää säädäntötoimivaltaansa ja antanut täytäntöönpanosäädöksiä, joissa viitattaisiin tarpeellisiin standardeihin.

Tunnistuspalveluiden arvioinnin osalta määräyksen tavoitteena on selkeyttää toimijoille, millä perusteella niiden käyttämät auditoijat ovat päteviä tekemään tunnistusjärjestelmän arviointeja. Tunnistuspalveluntarjoajan arviointielimen ei tarvitse hakea erikseen hyväksyntää, ellei se ole vaatimustenmukaisuuden arviointilaitos. Määräyksen tavoitteena on, että toimijat voisivat mahdollisimman paljon hyödyntää auditointeja, joita ne tekevät tai teettävät jo ennestään.

3.2.2 Vaikutusarviointi 2016: Ei-hyväksytyt luottamuspalvelut ja luotettu luettelo

Arvioitava kysymys: Olisiko Suomessa perusteita tai tarvetta merkitä luotettuun luetteloon (trusted list) muitakin palveluita kuin hyväksyttyjä luottamuspalveluita? Olisiko tämä mahdollista eIDAS-asetuksen ja tunnistus- ja luottamuspalvelulain perusteella?

Näkökohtia arviointiin

eIDAS-asetus sallii ei-hyväksyttyjen luottamuspalveluiden merkitsemisen luotettuun luetteloon tällä statuksella. Palvelut, joita luotettuun luetteloon voisi merkitä, yksilöidään ETSIn spesifikaatiosta TS 119 612 v 2.1.1 (huomaa versionumero) [14]. Ei-hyväksyttyjen luottamuspalveluiden merkitseminen luotettuun luetteloon on jäsenvaltion harkinnassa.

Palvelun merkitseminen luotettuun luetteloon ei-hyväksyttynä luottamuspalveluna voisi eIDAS-asetuksen puitteissa koskea sekä palveluntarjoajia, jotka eivät halua hakea luottamuspalvelulle hyväksyttyä statusta että palvelutyyppejä, joille ei voi sääntelyn perusteella hakea hyväksyntää eli esimerkiksi allekirjoituspalveluja.

LUONNOS 9.4.2021

Sähköisiä palveluita, kuten erilaisia allekirjoituspalveluita tarjoavat yritykset voisivat hyötyä siitä, että niiden palvelut merkittäisiin luotetulle listalle vaikka vain ei-hyväksyttynä luottamuspalveluna. Joissakin maissa toimitaankin näin jo aikaisemman sääntelyn puitteissa (ennen eIDAS-asetuksen voimaantuloa luotettu luettelo on perustunut sähköallekirjoitusdirektiiviin ja palveludirektiiviin).

Muiden kuin hyväksyttyjen luottamuspalveluiden aseman määrittely voisi lisätä myös käyttäjien ja asiointipalveluiden tarjoajien luottamusta ja luotettavuutta sähköisessä asioinnissa.

Tulkintalinjaukset

Luotettuun luetteloon merkitään Suomessa sääntelyn perusteella vain hyväksytyt luottamuspalvelut. Tunnistus- ja luottamuspalvelulain 42 a §:ssä on säädetty Viestintäviraston tehtäväksi ylläpitää luetteloa hyväksytyistä luottamuspalveluista. Laissa ei säädetä ei-hyväksyttyjen luottamuspalvelujen arvioinnin ja valvonnan perusteista tai menettelystä, eikä ohjaukselle tai valvonnalle ole resursseja.

Määräykselle vaihtoehtoiset ohjauskeinot

Suositus/ohje. Ei relevantti. Viranomaisen vahvistama luotettava status edellyttäisi perustetta säädännössä.

Yhteissääntely. Ei relevantti. Oman, erityisesti luotettujen palveluiden ryhmittelyn luominen ja määrittely yhteissääntelynä olisi vaikeaa riittävän tasapuolisesti aiheuttamatta kilpailuoikeudellisia ongelmia.

Informaatio-ohjaus. Ei relevantti. Luotettu lista itsessään on informaatio-ohjauksen luonteinen instrumentti. Mahdolliset muut kilpailevat kansallisesti määritellyt julkaisut (muut kuin luotettu lista) olisivat omiaan aiheuttamaan epäselvyyttä, eivätkä toimijat saavuttaisi niillä EU-tasoista statusta.

3.2.3 Vaikutusarviointi 2016: Sähköisten allekirjoitusten valvonta

Arvioitava kysymys: Miten Viestintävirasto osallistuu siihen arviointiin, onko jokin toteutus kehittynyt sähköinen allekirjoitus?

Näkökohtia arviointiin

eIDAS-asetuksen mukaan kehittyneet sähköiset allekirjoitukset tai allekirjoituspalvelut eivät ole hyväksyttyjä luottamuspalveluita. Tunnistus- ja luottamuspalvelulain 42 a §:n perusteella niitä ei merkitä asetuksen 22 artiklan mukaiseen luotettuun luetteloon. Tunnistus- ja luottamuspalvelulain 42 a §:n ja eIDAS-asetuksen 17.3 artiklan perusteella Viestintävirasto valvoo ei-hyväksyttyjä luottamuspalveluja vain jälkikäteen.

Joissain laeissa edellytetään allekirjoittamista kehittyneellä sähköisellä allekirjoituksella, josta säädetään eIDAS-asetuksen 26 artiklassa. Viestintävirastoon tulee kysymyksiä, joissa tiedustellaan, täyttääkö jokin tarjottu palvelu kehittyneeltä sähköiseltä allekirjoitukselta edellytettävät vaatimukset ja kelpaako se siten asiakirjojen allekirjoittamiseen.

Kuten edellä kohdassa 3.8.1 todettiin, tunnistus- ja luottamuspalvelulaissa laissa ei ole säädetty kehittyneiden sähköisten allekirjoitusten valvonnasta tai valvonnan resursoinnista, mikä vastaa nykytilannetta.

LUONNOS 9.4.2021

Sähköisen asiointipalvelun toteuttajan (esimerkiksi julkishallinnon organisaation) ja sähköisen allekirjoituspalvelun tarjoajan on arvioitava, täyttääkö tietty palvelu kehittyneen sähköisen allekirjoituksen tunnusmerkistön ja vaatimukset.

Sekä asiointipalveluita toteuttavalla julkisella hallinnolla että allekirjoituspalveluiden tuottajilla olisi tarvetta sen arvioinnille, vastaavatko palvelut eIDAS-asetuksen vaatimuksia. Tulkinnan tulisi olla yhtenäistä.

Kehittyneitä sähköisiä allekirjoituksia käsitellään laajemmin C osan luvussa 2.

Linjaukset

Viestintävirasto tuottaa yleistä neuvontaa kehittyneestä sähköisestä allekirjoituksesta, mutta ei arvioi sitä, täyttävätkö yksittäiset toteutukset eIDAS-asetuksen vaatimukset.

Sähköisen asiointipalvelun toteuttajan ja sähköisen allekirjoituspalvelun tarjoajan on arvioitava, täyttääkö tietty palvelu kehittyneen sähköisen allekirjoituksen tunnusmerkistön ja vaatimukset.

Määräykselle vaihtoehtoiset ohjauskeinot

Suositus/ohje. Tämän dokumentin C-osan luvussa 2 käsitellään kehittyneitä sähköisiä allekirjoituksia.

Yhteissääntely. Ei ole tarkasteltu. Vaatimukset sinänsä ovat jo eIDAS-asetuksessa eivätkä yhteissääntelyllä laadittavissa.

Informaatio-ohjaus. Tiedonvaihto kehittyneen allekirjoituksen tarjoajista tai käyttäjien (esim. valtionhallinnossa) olisi hyvin mahdollista. Tieto ei vahvistaisi palveluntarjoajien palvelun statusta kehittyneenä sähköisenä allekirjoituksena, vaan tarjoaisi lähinnä vertaistietoa. Viestintävirasto ei ole toistaiseksi suunnitellut resursointia tiedonvaihdon organisoimiseen.

3.3 Lähteet/referenssit/standardit

Seuraavassa on asiaan liittyviä lähteitä:

Enisa, Trust services

- https://www.enisa.europa.eu/publications/security-framework-for-trust-providers
- https://www.enisa.europa.eu/publications/security-framework-for-qualified-trust-providers
- https://www.enisa.europa.eu/publications/reccomendations-for-qtsps-based-on-standards
- https://www.enisa.europa.eu/publications/enisa-report-remote-id-proofing

Linkki: ETSI Digital signature pääsivu

- https://www.etsi.org/technologies/digital-signature

Lista ajantasaisista ja tulevista standardeista

- https://www.etsi.org/committee/1399-esi

LUONNOS 9.4.2021

Linkki: ETSI ja etäallekirjoitus (remote/cloud signing)

- https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.01.01_60/ts_119432v010101p.pdf
- https://www.etsi.org/deliver/etsi_ts/119400_119499/11943101/01.01.01_60/ts_11943101v010101p.pdf
- https://www.etsi.org/deliver/etsi_ts/119400_119499/11943101/01.01.01_60/ts_11943101v010101p.pdf

Linkki: ETSI standards ja full list

- https://www.etsi.org/committee/1399-esi

Linkki: Komission eIDAS-observatory

- https://ec.europa.eu/futurium/en/eidas-observatory

Linkki: Komission eIDAS-sivut

- https://digital-strategy.ec.europa.eu/en/policies/trust-services-and-eid

Linkki: Komission sivut eIDAS-asetus ja täytäntöönpanosäädökset

- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
- https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32014R0910&from=EN
- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016D0650

Linkki: Komission lausuntopyyntö 24.7.2020-2.10.2020 (kyselyssä on oma osio luottamuspalveluista)

- https://ec.europa.eu/digital-single-market/en/news/digital-identity-and-trust-commission-launches-public-consultation-eidas-regulation

3.4 Toimialakysely 2020 muutostarpeista

71) Hyväksytyt luottamuspalvelut. Onko määräyksessä luottamuspalveluihin liittyviä muutostarpeita? Olisiko hyväksyttyjen luottamuspalveluiden vaatimustenmukaisuutta mielestänne arvioitava joidenkin muiden kuin ETSIn standardien perusteella? Minkä?

72) Akkreditoidut arviointilaitokset. Onko määräyksessä arviointilaitoksiin liittyviä muutostarpeita?

73) Sertifiointilaitokset. Onko määräyksessä sertifiointilaitoksiin liittyviä muutostarpeita?

74) Vaikuttavuus. Onko määräyksellä ollut vaikutusta hyväksyttyjen luottamuspalveluiden tarjontaan?

LUONNOS 9.4.2021

3.4.1 Toimijoiden vastaukset

DVV

71) Teknologianeutraalisuuden tavoite toteutuu nykyisessä Määräyksessä ja viittaus esimerkiksi ETSI-standardeihin on suuntaa antava ja toimiva palveluntarjoajan näkökulmasta.

72) Asetuksen tavoitteen, palveluiden laajan leviämisen, kannalta olisi tärkeää, että kynnys aloittaa markkinaehtoisia arviointipalveluita olisi mahdollisimman matala. Ohjeistamalla ja Määräyksen/Suosituksen selkeydellä on yhdenmukaisten arviointiraporttien tuottamiseksi keskeinen rooli, joka täsmentyy sitä mukaa, kun kokemusta arvioinneista ja raporteista on saatavilla.

eIDAS-sääntely on tarkastelussa EU:ssa ja yksi tarkastelun lähtökohta on tunnistus- ja luottamuspalvelusääntelyn harmonisointi. Tämä harmonisointi tulisi myös huomioida tarvittavilta osin määräyksessä. Määräyksen laajempi uudistaminen on hyvä synkronoida aikataulullisesti mahdollisten eIDAS-sääntelyn muutoksien jälkeiseen aikaan.

73) Ei tunnistettuja muutostarpeita.

74) On vaikutusta, jos määräys on selkeä ja helposti hahmotettava ja se kannustaa osaltaan tarjoamaan luottamuspalveluita sekä arviointipalveluita, vaikkakin kysymys on viime kädessä liiketoiminnasta.

Vaikutusta voi arvioida vertaamalla kansallisesti tarjottujen luottamuspalvelujen määrää muiden EU-jäsenmaiden vastaaviin. Suomeen rekisteröityjä luottamuspalveluntarjoajia ei DVV:n lisäksi ole.

3.5 Viraston eIDAS arviomuistio 10.6.2020 ja siihen annettu palaute

Traficom laati kesäkuussa 2020 arviomuistion eIDAS-asetuksesta ja pyysi siitä lausuntoja (dnro Traficom/9355/09.02.00/2020)

Muistio 10.6.2020: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Traficomin%20arviomuistio%2010.6.2020%20eIDAS-asetuksesta.PDF

Lausuntopyyntö 10.6.2020: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Traficomin%20lausuntopyynt%C3%B6%2010.6.2020%20eIDAS-asetuksen_arvioinnista.PDF

Lausuntoyhteenveto 9.9.2020: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Lausuntoyhteenveto%209.9.2020%20Traficomin%20eIDAS-arviomuistiosta.pdf

Seuraavassa on poimittu lausuntoyhteenvedosta asiat, jotka liittyvät käsillä olevaan määräyspäivitykseen

- Luottamuspalveluista yleisesti tuotiin esille, että selkeät keinot hankkia hyväksyntä luottamuspalvelulle helpottaisi palveluntarjoajan valintaa. (Pankit).
- Korostettiin kuitenkin, että palvelukokonaisuus ratkaisee, millainen palvelu on yritykselle sopiva ja ei-hyväksytyt luottamuspalvelut voivat siksi täyttää tarpeet yhtä lailla kuin hyväksytyt. (Pankit)

LUONNOS 9.4.2021

- Hidasteena luottamuspalveluiden käyttöönotolle mainittiin standardoimattomat palvelut sekä aikaa vievä palveluprosessien sähköistäminen ja analogisten ja digitaalisten prosessien yhteensovittaminen. (Pankit)

- Vaatimustenmukaisuuden arviointilaitosten akkreditointia ja arviointiraporttia koskevan sääntelyn tarkentaminen ja standardien hyödyntäminen olisi perusteltua. Kotimaisten toimijoiden akkreditoituminen olisi myönteistä kehitystä, ja palveluntarjoajia tulisikin rohkaista ja kannustaa akkreditoitumaan laajemmin, jotta eIDAS-asetuksen tavoitteet näiden palveluiden laajamittaisesta leviämisestä toteutuisivat asetuksen päämäärän mukaisesti. Kansallisella palveluntarjonnalla olisi myös myönteinen vaikutus arvioinnin kustannuksiin. (DVV)

- Sähköiset allekirjoituspalvelut tai sähköisen allekirjoituksen luontipalvelut ovat keskeisimpiä luottamuspalveluista. (Pankit)

- Traficomin arviomuistio antaa kuvan sähköisestä allekirjoituksesta Suomessa. Suomessa on kasvava tarve mm. luotettaville sähköisen allekirjoituksen palveluille sekä arviointikriteereille. Tällä hetkellä toimijoille ei ole selvää, minkä tasoisia allekirjoituksia palveluissa oikeasti tehdään. Kolmannella osapuolella tulisi olla mahdollisuus varmistua sähköisesti allekirjoitettujen dokumenttien aitoudesta ja eheydestä. (Pankit)

- Sähköisen allekirjoituksen käytön laajentaminen edellyttäisi standardien selkeyttämistä. (Pankit)

- Sähköisen allekirjoituksen käytön laajentaminen edellyttäisi allekirjoituspalveluiden prosessuaalisten vaatimusten selkeyttämistä sekä selkeyttä siitä, mikä täyttää kirjallisen muodon vaatimuksen. (Pankit)

- Ehdotettiin kehittyneen sähköisen allekirjoituksen reunaehtojen tarkentamista ja toivottiin viranomaisen neuvontaa ja tulkintaohjeita tai selvitystä palveluiden käytön edistämiseksi. (Pankit)

- Ehdotettiin myös kansallista eIDAS-asetuksen kehittyneen sähköisen allekirjoituksen vaatimusten tulkinnan lieventämistä, jotta vahvaan tunnistukseen perustuva sähköinen allekirjoitus voisi täyttää kehittyneen sähköisen allekirjoituksen ehdot. (Pankit)

- Traficom referoi seuraavassa lausuntoa, jonka Avaintec antoi aikaisemmin muussa yhteydessä: Sähköinen tunnistaminen ja sähköinen allekirjoittaminen eivät ole sama asia. Viranomaisen neuvonta parantaisi digitaalisten palveluiden tarjonnan mahdollisuutta ja kuluttajien uskallusta ja ymmärrystä ottaa palveluita käyttöön. Myös muuhun kuin vahvaan tunnistamiseen tai muuhun kuin kehittyneeseen sähköiseen allekirjoitukseen perustuvat eli myös perustason sähköiseen allekirjoitukseen (kuten Avaintecin sähköpostiosoitteeseen perustuva allekirjoituspalvelu) perustuvat oikeustoimet ja asiointi ovat monessa tilanteessa riittäviä, koska prosessin liittyy myös muuta kommunikaatiota, jonka perusteella osapuolet luottavat prosessiin. Edellä mainituista syistä ei ole tarpeellista, että viranomainen edistää vain vahvan sähköisen tunnistamisen käyttöä, mikä edistää epätasapuolisesti vahvan tunnistamisen tarjoajien palveluiden tarjontaa. Suomen ulkopuoliset yritykset, kumppanit ja kuluttajat eivät voi käyttää suomalaisia tunnistusmetodeja ja niiden käytön edistämistä voi siksi pitää lyhytnäköisenä. (Avaintec)

LUONNOS 9.4.2021

- Sähköisten allekirjoitusten käyttö työ- ja virkatehtävien hoitamisen yhteydessä on käytännössä vaihtelevaa ja yksityisellä ja julkisella sektorilla on erilainen tietämys, valmiudet ja resurssit erilaisten kehittyneiden sähköisten allekirjoitusten käyttöön. (DVV)

4 2021 muutosehdotukset

4.1 Hyväksytyn luottamuspalveluntarjoajan (QTSP) ja luottamuspalvelun (QTS) standardiviittaukset

Arvioitava kysymys: ETSI-standardiviittausten päivittäminen ja täydentäminen (20 §, 21 §)

4.1.1 Säänteymuutokset

- Määräyksen vaatimukset hyväksytyille luottamuspalveluille perustetaan niihin ETSI:n standardeihin, joita on saatu valmiiksi kullekin luottamuspalvelutyypille komission standardointimandaatin nojalla.
- Määräykseen lisätään voimassa olevat standardiviittaukset

4.1.2 Standardipäivitykset säännös 20 Hyväksytyn luottamuspalvelun tarjoajan arviointikriteerit

ETSI:n standardit

ETSI standardit on saatettu sellaisenaan voimaan Suomessa ja ne löytyvät myös SFS-standardeina. Tällöin merkitsemistapa on esimerkiksi SFS-EN 319 401.

Seuraavassa on ryhmitelty pykälässä viitattuja standardeja ja kerrottu tällä hetkellä sovellettava standardin versio. Viimeisin julkaistu versio on merkitty

Hyväksytyn luottamuspalvelun tarjoajan yleiset vaatimukset

ETSI EN 319 401 V2.1.1 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [28]

ETSI EN 319 401 V2.2.1 (2018-04)

Standardi sisältää yleiset palveluriippumattomat vaatimukset hyväksytyn luottamuspalvelun tarjoajalle. Se sisältää vaatimuksia mm. riskien arvioinnille, tietoturvapolitiikalle ja - käytännölle sekä toiminnan johtamiselle.

Varmenteita myöntävän luottamuspalvelun tarjoajan vaatimukset

ETSI EN 319 411-1 V1.1.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [29]

ETSI EN 319 411-1 V1.2.2 (2018-04) ja hyväksyntäkierroksella oleva ETSI EN 319 411-1 V1.3.0 (2021-02)

Standardi sisältää yleiset vaatimukset varmenteita tarjoavalle luottamuspalvelun tarjoajalle. Se täydentää ja tarkentaa standardissa EN 319 401 esitettyjä vaatimuksia. Standardi sisältää yksityiskohtaisia vaatimuksia mm. varmennepolitiikalle

LUONNOS 9.4.2021

ja varmennuskäytännölle. Standardiin liittyy informatiivinen liite C (Conformity Assessment Check list), johon on koottu standardin vaatimukset tarkistuslistan muodossa. Tarkistuslistaa voi hyödyntää esimerkiksi luottamuspalvelun tarjoajan auditoinnissa.

Hyväksyttyjä varmenteita myöntävän luottamuspalvelun tarjoajan vaatimukset

ETSI EN 319 411-2 V2.1.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates [30]

ETSI EN 319 411-2 V2.2.2 (2018-04) ja hyväksyntäkierroksella oleva ETSI EN 319 411-2 V2.3.0 (2021-02)

Standardi sisältää vaatimukset eIDAS-asetuksen mukaisia hyväksyttyjä varmenteita tarjoavalle luottamuspalvelun tarjoajalle. Se täydentää standardissa EN 319 411-1 esitettyjä vaatimuksia vastaamaan eIDAS-asetuksen erityisvaatimuksia. Lisävaatimukset kohdistuvat mm. varmennepolitiikkaan ja varmennuskäytäntöön.

Standardiin liittyy informatiivinen liite B (Conformity Assessment Check list), johon on koottu standardin vaatimukset tarkistuslistan muodossa. Tarkistuslistaa voi hyödyntää esimerkiksi luottamuspalvelun tarjoajan auditoinnissa.

Hyväksyttyjä aikaleimoja myöntävän luottamuspalvelun tarjoajan vaatimukset

ETSI EN 319 421 V1.1.1 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps [31]

[Ajantasainen]

Standardi sisältää tietoturvapolitiikka- ja tietoturvavaatimukset sähköisiä aikaleimoja tarjoavalle luottamuspalvelun tarjoajalle. Standardi viittaa pääsääntöisesti standardin EN 319 401 vaatimuksiin, mutta tarkentaa niitä joiltain osin. Standardi sisältää yksityiskohtaiset vaatimukset aikaleiman allekirjoitusavaimen sisältävän yksikön TSU (Time-Stamping Unit) hallinnalle. Standardiin liittyy informatiivinen liite H (Conformity Assessment Check list), johon on koottu standardin vaatimukset tarkistuslistan muodossa. Tarkistuslistaa voi hyödyntää esimerkiksi luottamuspalvelun tarjoajan auditoinnissa.

4.1.3 Standardipäivitykset säännös 21 Hyväksytyn luottamuspalvelun arviointikriteerit

~~Ajantasaversiot: https://www.etsi.org/standards-search#page=1&search=319412&title=0&etsiNumber=1&content=0&version=1&onApproval=1&published=1&historical=0&startDate=1988-01-15&endDate=2021-03-22&harmonized=0&keyword=&TB=607&stdType=&frequency=&mandate=&collection=&sort=3~~

eIDAS-asetuksen hyväksytyt (qualified) luottamuspalvelut voivat olla seuraavia

- Qualified certificate for electronic signature
- Qualified certificate for electronic seal
- Qualified certificate for website authentication
- Qualified validation Service for qualified electronic signature
- Qualified preservation Service for qualified electronic signature
- Qualified validation Service for qualified electronic seal
- Qualified preservation Service for qualified electronic seal
- Qualified time stamp

LUONNOS 9.4.2021

- Qualified electronic registrered delivery Service

4.1.3.1 Sähköisten allekirjoitusten, sähköisten leimojen ja verkkosivustojen todentamisen hyväksytyt varmenteet

eIDAS-asetuksen liitteissä I, III ja IV määritellään sähköisten allekirjoitusten, sähköisten leimojen ja verkkosivustojen todentamisen hyväksyttyjä varmenteita koskevat vaatimukset.

Vaatimusten sisältöä tarkentamaan Euroopan telestandardointi-instituutti ETSI on laatinut komission mandaatilla määräystekstissä luetellut standardit. Standardeihin on koottu yksityiskohtaiset konkreettiset vaatimukset, joiden täyttyminen varmistaa sen, että luottamuspalvelu on eIDAS-asetuksen mukainen.

Standardit eivät ole pakollisia, vaan palvelut voi toteuttaa muullakin tavalla. Standardit osoittavat kuitenkin sen, millaista luotettavuustasoa eIDAS-asetus edellyttää palveluissa. Jos palvelun toteuttaa viitatun standardin mukaisesti, eIDAS-asetuksen vaatimukset tulevat huomioiduksi. Jos käytetään muuta vastaavat vaatimukset sisältävää standardia, palvelun toteuttajan on erikseen osoitettava, että palvelu täyttää eIDAS-asetuksen vaatimukset.

Määräyksessä lueteltuihin varmenneprofiileihin sisältyvät yleiset vaatimukset sisältävä standardi, varmenteen tarkoitetun sovelluksen mukaisia standardeja sekä hyväksyttyjen varmenteiden sisällön (*statements)* määrittelevä standardi. Siltä osin kuin standardeissa on eritelty EU-säädännön vaatimusten täyttymistä koskevat ja muita vaatimuksia koskevat osat, tämän määräyksen kannalta soveltuvina osina pidetään EU-säädännön täyttymiseen liittyviä vaatimuksia.

Varmenneprofiilit - yleinen: ETSI EN 319 412-1 V1.1.0 (2015-12) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures [32]

ETSI EN 319 412-1 V1.4.1 (2020-06) ja hyväksyntäkierroksella oleva ETSI EN 319 412-1 V1.4.2 (2020-07)

Varmenneprofiilit - luonnollinen henkilö: ETSI EN 319 412-2 V2.1.0 (2015-12) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons [33]

ETSI EN 319 412-2 V2.2.1 (2020-07)

Varmenneprofiilit - oikeushenkilö: ETSI EN 319 412-3 V1.1.0 (2015-12) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons [34]

ETSI EN 319 412-3 V1.2.1 (2020-07)

Varmenneprofiilit - verkkosivuvarmenteet: ETSI EN 319 412-4 V1.1.0 (2015-12) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates [35]

ETSI EN 319 412-4 V1.1.1 (2016-02)

Varmenneprofiilit - QCStatements: ETSI EN 319 412-5 V2.1.0 (2015-12) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements [36]

LUONNOS 9.4.2021

ETSI EN 319 412-5 V2.3.1 (2020-04)

4.1.3.2 Hyväksytty sähköinen aikaleima

eIDAS asetuksen 42 artikla sisältää vaatimukset hyväksytylle sähköiselle aikaleimalle. Toistaiseksi vaatimusten sisältöä tarkentamaan Euroopan telestandardointi-instituutti ETSI on laatinut komission mandaatilla ainoastaan määräystekstissä mainitun standardin EN 319 422. Jos aikaleimapalvelun protokolla ja profiili on toteutettu kyseisen standardin mukaisesti, eIDAS-asetuksen vaatimukset niiltä osin täyttyvät. Jos käytetään muuta vastaavat vaatimukset sisältävää standardia, palvelun toteuttajan on erikseen osoitettava, että eIDAS-asetuksen vaatimukset täyttyvät.

ETSI EN 319 422 V1.1.0 (2015-12) Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles [37]

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

- https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf
- *This document specifies a profile for the format and procedures for time-stamping as specified in RFC 3161, based upon TS 101 861*
- *The present document defines a profile for the time-stamping protocol and the time-stamp token defined in IETF RFC 3161 [1] including optional ESS-CertIDv2 update in IETF RFC 5816 [4].*
- *It defines what a time-stamping client supports and what a time-stamping server supports.*
- *Time-stamp validation is out of scope and is defined in ETSI EN 319 102 [i.4].*
- *Annex C defines media type and file-extension for time-stamp tokens.*

ETSI EN 319 421 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

- https://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.01.01_60/en_319421v010101p.pdf
- *This document specifies policy requirements for TSPs providing Time-stamping services based on RFC 3161. It references EN 319 401 for generic requirements and is to be based upon TS 102 023*
  An Annex will include a check list that may be used by conformity assessors to check conformance.

Tarkistetaan aikaleimaan liittyvät muut (jos on)

4.1.3.3 Hyväksytty sähköinen rekisteröity jakelupalvelu (eDelivery, QERDS)

Hyväksytyn sähköisen rekisteröidyn jakelupalvelun vaatimukset säädetään eIDAS-asetuksen 44 artiklassa.

Seuraavat lisätty ETSIN listoilta, ei tarkistettu sisältöä

LUONNOS 9.4.2021

ETSI EN 319 521 V1.1.1 (2019-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers

- https://www.etsi.org/deliver/etsi_en/319500_319599/319521/01.01.01_60/en_319521v010101p.pdf

ETSI EN 319 522-1 V1.1.1 (2018-09) Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture

- https://www.etsi.org/deliver/etsi_en/319500_319599/31952201/01.01.01_60/en_31952201v010101p.pdf

ETSI EN 319 522-2 V1.1.1 (2018-09) Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic contents

- https://www.etsi.org/deliver/etsi_en/319500_319599/31952202/01.01.01_60/en_31952202v010101p.pdf

ETSI EN 319 522-3 V1.1.1 (2018-09) Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 3: Formats

- https://www.etsi.org/deliver/etsi_en/319500_319599/31952203/01.01.01_60/en_31952203v010101p.pdf

ETSI EN 319 522-4-1 V1.1.1 (2018-09) Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 1: Message delivery bindings

- https://www.etsi.org/deliver/etsi_en/319500_319599/3195220401/01.01.01_60/en_3195220401v010101p.pdf

ETSI EN 319 522-4-2 V1.1.1 (2018-09) Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 2: Evidence and identification bindings

- https://www.etsi.org/deliver/etsi_en/319500_319599/3195220402/01.01.01_60/en_3195220402v010101p.pdf

ETSI EN 319 522-4-3 V1.1.1 (2018-09) Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 3: Capability/requirements bindings

- https://www.etsi.org/deliver/etsi_en/319500_319599/3195220403/01.01.01_60/en_3195220403v010101p.pdf

LUONNOS 9.4.2021

4.1.3.4 REM-standardit

2016: REM-spesifikaatiotkin on tarkoitus uusia tulevaisuudessa ja julkaista standardisarjana EN 319 532-1…5. REM-standardeja voi hyödyntää pohjana sähköisen rekisteröidyn jakelupalvelun toteutuksen suunnittelussa, mutta lopulliset vaatimukset tullaan määrittelemään standardisarjassa EN 319 522-1…4.

REM-spesifikaatiot, 2016 tilanne:

TS 102 640-1 Ver. 2.2.1 Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 1: ArchitectureTS 102 640-2 Ver. 2.2.1 Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 2: Data requirements, Formats and Signatures for REMTS 102 640-3 Ver. 2.1.2 Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 3: Information Security Policy Requirements for REM Management Domains

TS 102 640-4 Ver. 2.1.2 Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 4: REM-MD Conformance Profiles

TS 102 640-5 Ver. 2.1.2 Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 5: REM-MD Interoperability Profiles

ETSI standardit:

ETSI EN 319 532-1 V1.1.1 (2018-09) Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 1: Framework and architecture

ETSI EN 319 532-2 V1.1.1 (2018-09) Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 2: Semantic contents

ETSI EN 319 532-3 V1.1.1 (2018-09) Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 3: Formats

ETSI EN 319 532-4 V1.1.1 (2018-09) Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 4: Interoperability profiles

Arvio: koska eDelivery-standardit on annettu, informaatiolle REM-standardeista ei ole tarvetta perustelumuistiossa.

4.1.3.5 Säilytys ja validointi

Arvioitava, ovatko seuraavat standardit soveltuvat viitattavaksi säännöksessä.

ETSI TS 119 512 V1.1.1 (2020-01) Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services

- https://www.etsi.org/deliver/etsi_ts/119500_119599/119512/01.01.01_60/ts_119512v010101p.pdf

ETSI TS 119 511 V1.1.1 (2019-06) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques

Liikenne 9.4.2021

- https://www.etsi.org/deliver/etsi_ts/119500_119599/119511/01.01.01_60/ts_119511v010101p.pdf

ETSI TS 119 441 V1.1.1 (2018-08) Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing **signature validation services**

- https://www.etsi.org/deliver/etsi_ts/119400_119499/119441/01.01.01_60/ts_119441v010101p.pdf

- *An update is in preparation.*

- *The present document, based on the general policy requirements specified in ETSI EN 319 401 [2], specifies policy and security requirements for signature validation services operated by a TSP.*

    - *NOTE 1: Beside signature validation, other signature services, like signature creation, signature augmentation or signature preservation can also be offered by TSPs. Such services can be provided as stand-alone services or combined (e.g. augmentation can be used to support a preservation service). The present document does not provide requirements on signature services beyond validation and does not provide requirements on how to combine signature related services.*

    - *NOTE 2: A distinct Technical Specification (TS) provides policy and security requirements for TSP offering signature augmentation services as a stand-alone service or in complement to one of the above-mentioned services.*

- *The present document is aimed at trust services supporting the validation of digital signatures in accordance with ETSI TS 119 102-1 [3]. It takes into account the relevant requirements for signature validation application specified in ETSI TS 119 101 [1] as they relate to TSPs.*

- *It is aimed at supporting the validation of digital signatures in European and other regulatory frameworks.*

    - *NOTE 3: Specifically, but not exclusively, the present document is aimed at qualified and non-qualified trust services, supporting the validation of digital signatures in accordance with the requirements of the Regulation (EU) No 910/2014 [i.1] for validation of electronic signatures and electronic seals (both advanced and qualified).* ***Annex B complements the requirements for signature validation service providers offering a Qualified Validation Service for qualified electronic signatures or for qualified electronic seals as specified by Regulation (EU) No 910/2014 [i.1].***

    - *NOTE 4: Specifically, but not exclusively, digital signatures in the present document cover electronic signatures, advanced electronic signatures, qualified electronic signatures, electronic seals, advanced electronic seals, and qualified electronic seals as per Regulation (EU) No 910/2014 [i.1].*

- *The present document may be used by competent bodies as the basis for confirming that an organization is trustworthy in validating digital signatures on behalf of other persons or on its own behalf.*

LUONNOS 9.4.2021

- *NOTE 5: See ETSI EN 319 403 [i.13] for guidance on assessment of TSP processes and services.*

- *The user's interface is outside the scope of the main TSP service. However, the present document provides in annex D recommendations for the user's interfaces (for inputting the request and to visualize the validation report).*

- *The TSP has connections with external (trust) services that can be contacted for provisioning validation information, or to relay the validation request. The present document does not put requirements on the trust service policies applied by such external services.*

- *The present document identifies specific controls needed to address specific risks associated with validation services.*

ETSI SR 019 510 V1.1.1 (2017-05) Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures

- https://www.etsi.org/deliver/etsi_sr/019500_019599/019510/01.01.01_60/sr_019510v010101p.pdf

- *The objective of this work item is to specify the general requirements with respect to long-term data preservation and clearly identify which are the "objects" whose preservation falls in the scope of a preservation service as defined by the Regulation (EU) No. 910/2014 and which objects are outside the scope of the Regulation but worth to be considered, the set of processes and technologies to be supported by a preservation service provider and the different types of preservation service provider, a catalogue of existing specifications and standards, a list of well-established and active communities in the fields of archival and preservation (possible candidates for liaisons) and an extension to the Rationalised Framework (RF) specifically targeted to data preservation services and providers to identify any additional standard or technical specification beyond those already specified by RF. The Scoping study and framework for standardization will be supporting the (qualified) preservation services as per Regulation (EU) No 910/2014 and also preservation services with a broader scope for industry at the International level.*

4.1.4 Muut ohjauskeinot

Ohje
Suositus
Yhteissääntely
Informaatiolla ohjaaminen

Ei huomioita.

4.2 Arviointilaitoksen ja arviointikertomuksen standardiviittaukset (22 §)

Arvioitava kysymys: Onko syytä lisätä määräykseen ETSI-standardin (ml. uusi osa arviointikertomuksesta) vaatimukset luottamuspalveluiden akkreditoitujen vaatimustenmukaisuuden arviointilaitokselle ja arvioinnille

LUONNOS 9.4.2021

4.2.1 Sääntelymuutokset

Arvio: Standardin versio on muuttunut, mutta sillä ei ole vaikutusta säännöstekstiin

ETSI EN 319 403-**1** V2.3.1 (2020-06)

ETSI TS 119 403-**3** V1.1.1 (2019-03) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers

https://www.etsi.org/deliver/etsi_ts/119400_119499/11940303/01.01.01_60/ts_11940303v010101p.pdf

Arvio: Liikenne- ja viestintäviraston määräysvaltuutus tunnistus- ja luottamuspalvelulain 42 §:ssä ei koske luottamuspalvelun vaatimuksenmukaisuuden arviointikertomusta, vaan ainoastaan arviointikriteerejä.

4.2.2 Muut ohjauskeinot

Ohje

Ks. ohje 215/2019 *Hyväksytyn eIDAS-luottamuspalvelun arviointikertomus*

- https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/O215_Hyv%C3%A4ksytyn_eIDAS-luottamuspalvelun_arviointikertomus_%289_10_2019%29.pdf
- **Arvioitava, olisiko perusteita päivittää ohjetta huomioiden seuraava standarditäydennys?**

Vrt. ETSI TS 119 403-2 V1.2.1 (2019-04) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates

> *The present document is part 2 of a multi-part deliverable covering Trust Service Provider Conformity Assessment, as identified below:*
>
> *Part 1: "Requirements for conformity assessment bodies assessing Trust Service Providers" (now existing as ETSI EN 319 403 to be issued as Part 1 when revised);*
>
> *Part 2: "Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates";*
>
> *Part 3: "Additional requirements for conformity assessment bodies assessing EU qualified trust service providers*
>
> *The present document defines specific supplementary requirements to those defined in ETSI EN 319 403 [1] for CABs performing audits based on ETSI EN 319 411-1 [i.9] and those from CA/Browser Forum, [i.7] and [i.8]. In particular,* ***the present document defines the requirements for audit attestations, including their content.***

LUONNOS 9.4.2021

Suositus
Yhteissääntely
Informaatiolla ohjaaminen

4.3 Allekirjoituksen ja leiman luontivälineen sertifiointilaitos ja sertifiointikriteerit (23 §)

Arvio: päivitetään säännöksessä viittaus, jos komissio päivittää täytäntöönpanopäätöstä. Päivitetään perusteluihin tiedot allekirjoituksen luontivälineen standardeista.

Arvio: Sertifiointilaitoksen kriteerejä ei arvioida uudestaan. Toimintaan ei ole osoitettu kiinnostusta Suomessa.

2016: Määräykseen ei ole otettu viittausta keskeneräisiin standardeihin tai pyritty laatimaan kansallisesti tarkempia teknisiä määrittelyjä palvelinpohjaisen allekirjoituksen luontivälineen vaatimuksille. Viestintäviraston näkemyksen mukaan ei ole olemassa edellytyksiä määritellä vaatimuksia, joiden nojalla voitaisiin riittävän perusteellisesti arvioida palvelun luotettavuus siten, että vaatimukset olisivat ennakoitavasti hyväksyttäviä myös muissa EU-maissa.

4.3.1 (EU) 2016/650 ja standardit

Vaatimukset tukeutuvat komission täytäntöönpanopäätökseen (EU) 2016/650 [43].

Komission täytäntöönpanopäätöksessä vahvistetaan sertifioinnin pohjaksi seuraavat standardit. Niistä yleinen IT-tietoturvallisuuden arvioinnin standardi ISO/IEC 15408 Information technology -- Security techniques -- Evaluation criteria for IT security-standardisarja [44] tunnetaan Common Criteria -vaatimuksina.

<u>Muut komission täytäntöönpanopäätöksessä vahvistetut standardit ovat</u>

- ISO/IEC 18045:2008 – Information technology – Security techniques – Methodology for IT security evaluation [45]

- EN 419 211 – Protection profiles for secure signature creation device, osat 1–6 [46] – tarpeen mukaan – seuraavasti:

o EN 419211–1:2014 – Protection profiles for secure signature creation device – Part 1: Overview

o EN 419211–2:2013 – Protection profiles for secure signature creation device – Part 2: Device with key generation

o EN 419211–3:2013 – Protection profiles for secure signature creation device – Part 3: Device with key import

o EN 419211–4:2013 – Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted channel to certificate generation application

o EN 419211–5:2013 – Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted channel to signature creation application

LUONNOS 9.4.2021

o EN 419211–6:2014 – Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted channel to signature creation application

Palvelinpohjaisen allekirjoitusvälineen standardit

Komission täytäntöönpanopäätöksessä ei ole vielä viittauksia standardeihin tai muita tarkennuksia eIDAS-asetuksen vaatimuksiin, mutta täytäntöönpanopäätöksen päivittäminen on valmistelussa.

CEN on valmistellut standardeja sellaisen allekirjoituksen luontivälineen vaatimuksista, joka ei ole fyysisesti allekirjoituksen tekijän hallinnassa.

Vuonna 2019 valmistuneet standardit:

Otsikot/selitteet (Nyt TS, eikä EN)

- https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.01.01_60/ts_119432v010101p.pdf
- https://www.etsi.org/deliver/etsi_ts/119400_119499/11943101/01.01.01_60/ts_11943101v010101p.pdf
- https://www.etsi.org/deliver/etsi_ts/119400_119499/11943101/01.01.01_60/ts_11943101v010101p.pdf

CEN:

- EN 419241-1:2018
- EN 419241-2:2019
- EN 419221-5:2018

ISO:

- ISO/IEC 15408 — Information technology — Security techniques — Evaluation criteria for IT security, Parts 1 to 3 as listed below:
- ISO/IEC 15408-1:2009 — Information technology — Security techniques — Evaluation criteria for IT security — Part 1. ISO, 2009.
- ISO/IEC 15408-2:2008 — Information technology — Security techniques — Evaluation criteria for IT security — Part 2. ISO, 2008.
- ISO/IEC 15408-3:2008 — Information technology — Security techniques — Evaluation criteria for IT security — Part 3. ISO, 2008,

Ks. myös Enisa Assessment of Standards related to eIDAS (December 14, 2018)

- https://www.enisa.europa.eu/publications/assessment-of-standards-related-to-eidas

LUONNOS 9.4.2021

4.4 Kehittyneen allekirjoitus- tai leimapalvelun kysymykset eivät sisälly määräykseen

Arvioitava kysymys: Kehittyneen sähköisen allekirjoituksen/luontipalvelun ja leiman/luontipalvelun informatiiviset osat poistaminen määräyksen perusteluista. Käsittely muussa yhteydessä, missä?

4.4.1 Ei-hyväksyttyjen luottamuspalvelujen valvonta

Kehittyneen sähköisen allekirjoituksen vaatimukset eivät kuulu viraston sääntelytoimivaltaan, joten niistä ei voida määrätä miltään osin.

Sähköisen allekirjoituksen ja leiman tai niiden luontipalveluiden vaatimustenmukaisuuden arviointi ei kuulu liikenne- ja viestintäviraston toimivaltaan ja säädettyihin tehtäviin. Toimivaltaan kuuluu tunnistus- ja luottamuspalvelulain 42 a.3 §:n 3 kohdan viittauksen perusteella toimia eIDAS-asetuksen 17 artiklassa tarkoitettuna valvontaelimenä ja hoitaa sille asetuksessa säädettyjä tehtäviä. Tehtäviin kuuluu ei-hyväksyttyjen luottamuspalvelujen jälkikäteinen valvonta, jos joku tuo viranomaisen tietoon, että ei-hyväksytty luottamuspalvelun tarjoaja ei väitetysti täytä eIDAS-asetuksen asetuksen vaatimuksia.

eIDAS-asetus, 17 art.3 b)

> *Valvontaelimellä on seuraavat tehtävät:*
>
> *b) toimien toteuttaminen tarvittaessa nimeävän jäsenvaltion alueelle sijoittautuneiden ei-hyväksyttyjen luottamuspalvelun tarjoajien suhteen jälkikäteen toteutettavin valvontatoimin, jos sille ilmoitetaan, että nämä ei-hyväksytyt luottamuspalvelun tarjoajat tai niiden tarjoamat luottamuspalvelut eivät väitetysti täytä tässä asetuksessa säädettyjä vaatimuksia.*

eIDAS-asetuksen johdantokappale

> *(36) Kaikkia luottamuspalvelun tarjoajia koskevan valvontajärjestelmän perustamisessa olisi varmistettava tasapuoliset edellytykset niiden toimien ja palvelujen tietoturvalle ja vastuuvelvollisuudelle, jolloin edistetään käyttäjien suojelua ja sisämarkkinoiden toimintaa. Ei-hyväksyttyihin luottamuspalvelun tarjoajiin olisi sovellettava joustavia ja reaktiivisia jälkikäteen toteutettavia valvontatoimia, jotka ovat perusteltavissa niiden palvelujen ja toimien luonteella. Valvontaelimellä ei siis pitäisi olla yleistä velvoitetta valvoa ei-hyväksyttyjä palveluntarjoajia. Valvontaelimen pitäisi toteuttaa toimia vain silloin, kun se saa tietää (esimerkiksi ei-hyväksytyn luottamuspalvelun tarjoajan itsensä tai muun valvontaelimen taholta, käyttäjän tai liikekumppanin ilmoituksen perusteella tai oman tutkintansa perusteella), että ei-hyväksytty luottamuspalvelun tarjoaja ei täytä tämän asetuksen vaatimuksia.*

LUONNOS 9.4.2021

4.4.2 Muut ohjauskeinot

4.4.2.1 Linjaus

Sähköisiä allekirjoituksia ja leimoja koskevat informatiiviset osat vuoden 2016 perustelumuistiosta jätetään pois päivitettävästä perustelumuistiosta, koska asiasta ei voida määrätä.

eIDAS-asetusta ja ETSI:n standardia voidaan käsitellä tarvittaessa muussa yhteydessä.

Tunnistus- ja luottamuspalvelulaissa laissa ei ole säädetty kehittyneiden sähköisten allekirjoitusten valvonnasta tai valvonnan resursoinnista.

Sähköisen asiointipalvelun toteuttajan (esimerkiksi julkishallinnon organisaation) ja sähköisen allekirjoituspalvelun tarjoajan on arvioitava, täyttääkö tietty palvelu kehittyneen sähköisen allekirjoituksen tunnusmerkistön ja vaatimukset.

Sekä asiointipalveluita toteuttavalla julkisella hallinnolla että allekirjoituspalveluiden tuottajilla olisi tarvetta sen arvioinnille, vastaavatko palvelut eIDAS-asetuksen vaatimuksia. Tulkinnan tulisi olla yhtenäistä.

Linjaukset 2016

Viestintävirasto tuottaa yleistä neuvontaa kehittyneestä sähköisestä allekirjoituksesta, mutta ei arvioi sitä, täyttävätkö yksittäiset toteutukset eIDAS-asetuksen vaatimukset.

Sähköisen asiointipalvelun toteuttajan ja sähköisen allekirjoituspalvelun tarjoajan on arvioitava, täyttääkö tietty palvelu kehittyneen sähköisen allekirjoituksen tunnusmerkistön ja vaatimukset.

4.4.2.2 Ohjauksen tarve

Liikenne- ja viestintäviraston saaminen neuvontapyyntöjen, eIDAS-asetuksen arviomuistiosta 2020 saadun palautteen ja yleisen sekä teknisen eIDAS-ryhmän antaman palautteen perusteella ohjauksen ja informaation tarvetta liittyy erityisesti siihen, miten sähköisen allekirjoituksen tai leiman luontipalvelut vastaavat eIDAS-asetuksessa säädettyjä tasoja ja miten tämä voitaisiin luotettavasti vahvistaa asiakkaille.

Seuraavaan on poimittu viraston eIDAS-arviomuistion lausuntoyhteenvedosta sähköistä allekirjoitusta koskevat (ks. tämän valmistelumuistion kohta 3.5)

- Sähköiset allekirjoituspalvelut tai sähköisen allekirjoituksen luontipalvelut ovat keskeisimpiä luottamuspalveluista. (Pankit)
- Traficomin arviomuistio antaa kuvan sähköisestä allekirjoituksesta Suomessa. Suomessa on kasvava tarve mm. luotettaville sähköisen allekirjoituksen palveluille sekä arviointikriteereille. Tällä hetkellä toimijoille ei ole selvää, minkä tasoisia allekirjoituksia palveluissa oikeasti tehdään. Kolmannella osapuolella tulisi olla mahdollisuus varmistua sähköisesti allekirjoitettujen dokumenttien aitoudesta ja eheydestä. (Pankit)
- Sähköisen allekirjoituksen käytön laajentaminen edellyttäisi standardien selkeyttämistä. (Pankit)

LUONNOS 9.4.2021

- Sähköisen allekirjoituksen käytön laajentaminen edellyttäisi allekirjoituspalveluiden prosessuaalisten vaatimusten selkeyttämistä sekä selkeyttä siitä, mikä täyttää kirjallisen muodon vaatimuksen. (Pankit)

- Ehdotettiin kehittyneen sähköisen allekirjoituksen reunaehtojen tarkentamista ja toivottiin viranomaisen neuvontaa ja tulkintaohjeita tai selvitystä palveluiden käytön edistämiseksi. (Pankit)

- Ehdotettiin myös kansallista eIDAS-asetuksen kehittyneen sähköisen allekirjoituksen vaatimusten tulkinnan lieventämistä, jotta vahvaan tunnistukseen perustuva sähköinen allekirjoitus voisi täyttää kehittyneen sähköisen allekirjoituksen ehdot. (Pankit)

- Traficom referoi seuraavassa lausuntoa, jonka Avaintec antoi aikaisemmin muussa yhteydessä: Sähköinen tunnistaminen ja sähköinen allekirjoittaminen eivät ole sama asia. Viranomaisen neuvonta parantaisi digitaalisten palveluiden tarjonnan mahdollisuutta ja kuluttajien uskallusta ja ymmärrystä ottaa palveluita käyttöön. Myös muuhun kuin vahvaan tunnistamiseen tai muuhun kuin kehittyneeseen sähköiseen allekirjoitukseen perustuvat eli myös perustason sähköiseen allekirjoitukseen (kuten Avaintecin sähköpostiosoitteeseen perustuva allekirjoituspalvelu) perustuvat oikeustoimet ja asiointi ovat monessa tilanteessa riittäviä, koska prosessin liittyy myös muuta kommunikaatiota, jonka perusteella osapuolet luottavat prosessiin. Edellä mainituista syistä ei ole tarpeellista, että viranomainen edistää vain vahvan sähköisen tunnistamisen käyttöä, mikä edistää epätasapuolisesti vahvan tunnistamisen tarjoajien palveluiden tarjontaa. Suomen ulkopuoliset yritykset, kumppanit ja kuluttajat eivät voi käyttää suomalaisia tunnistusmetodeja ja niiden käytön edistämistä voi siksi pitää lyhytnäköisenä. (Avaintec)

- Sähköisten allekirjoitusten käyttö työ- ja virkatehtävien hoitamisen yhteydessä on käytännössä vaihtelevaa ja yksityisellä ja julkisella sektorilla on erilainen tietämys, valmiudet ja resurssit erilaisten kehittyneiden sähköisten allekirjoitusten käyttöön. (DVV)

4.4.2.3 Mahdolliset määräykselle vaihtoehtoiset ohjauskeinot

Ohje, suositus

- 2021: Viranomainen voi antaa ohjeita ja suosituksia vain asioista, jotka kuuluvat viranomaiselle säädettyyn toimivaltaan. Virasto ottaa huomioon sen, että sähköisen allekirjoituksen ja leiman ja niiden luontipalvelujen sääntely eIDAS-asetuksessa on osittain teknisesti tulkinnanvaraista. Ennakoiva vaatimusten tulkinta edellyttäisi viraston näkemyksen mukaan yhtenäistä tulkintatapaa jäsenvaltioissa eikä sellaista ole muodostunut. Virastolla ei siten näyttäisi olevan perusteita ottaa kattavasti ennakoivasti kantaa näiden palveluiden vaatimustenmukaisuuteen

Yhteissääntely

- 2016: Ei ole tarkasteltu. Vaatimukset sinänsä ovat jo eIDAS-asetuksessa eivätkä yhteissääntelyllä laadittavissa.

- 2021: ei perusteita arvioida uudestaan siitä näkökulmasta, että jokin ryhmä toimijoita määrittelisi kansallisesti vaatimuksia.

Informaatiolla ohjaaminen

LUONNOS 9.4.2021

- 2016: Tiedonvaihto kehittyneen allekirjoituksen tarjoajista tai käyttäjien (esim. valtionhallinnossa) olisi hyvin mahdollista. Tieto ei vahvistaisi palveluntarjoajien palvelun statusta kehittyneenä sähköisenä allekirjoituksena, vaan tarjoaisi lähinnä vertaistietoa. Viestintävirasto ei ole toistaiseksi suunnitellut resursointia tiedonvaihdon organisoimiseen.
- **2021: asiassa voisi harkita ETSIn standardointiin perustuvan Q&A -patteriston tai jonkin vastaavan neuvontamateriaalin laatimista. Sähköiset allekirjoitukset ovat olleet alustavasti esillä viraston kaikille avoimessa teknisessä eIDAS-ryhmässä ja eIDAS-foorumissa marraskuussa 2020.**

4.4.3 Allekirjoituspalvelun standardoinnin tilanne

4.4.3.1 2016

ETSIssä on käynnissä standardointityö allekirjoituspalveluiden vaatimusten määrittelemiseksi.

-(119 432-1) DTS/ESI-0019432-1 Protocol for TSPs providing signature generation services - Part 1 Trusted Service manager [48]

-(119 432-2) DTS/ESI-0019432-2 Protocol for TSPs providing signature generation services - Part 2: local signing on mobile device

-(119 432-3) DTS/ESI-0019432-3 Protocol for TSPs providing signature generation services - Part 3: local signing on general device

-(119 432-4) DTS/ESI-0019432-4 Protocol for TSPs providing signature generation services - Part 4: remote signing

-(119 442) DTS/ESI-0019442 Protocol for TSPs providing signature validation services [49]

4.4.3.2 Remote signature

ETSI TS 119 432 V1.2.1 (2020-10) Electronic Signatures and Infrastructures (ESI); **Protocols for remote digital signature creation**

ETSI TS 119 431-1 V1.1.1 (2018-12) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; **Part 1: TSP service components operating a remote QSCD / SCDev**

- *https://www.etsi.org/deliver/etsi_ts/119400_119499/11943101/01.01.01_60/ts_11943101v010101p.pdf*
- *An update is in preparation.*

4.4.3.3 AdES

ETSI TS 119 431-2 V1.1.1 (2018-12) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; **Part 2: TSP service components supporting AdES digital signature creation**

LUONNOS 9.4.2021

- https://www.etsi.org/deliver/etsi_ts/119400_119499/11943102/01.01.01_60/ts_11943102v010101p.pdf

- *The present document provides policy and security requirements for trust service providers (TSP) implementing a service component supporting AdES digital signature creation. This component contains a signature creation application and is thus called signature creation application service component (SCASC). However, it is more than just the SCA. It contains service elements around which parts of the driving application as defined in ETSI TS 119 102-1 [1] and ETSI TS 119 101 [2] can be implemented. The present document does not give restrictions on whether something is covered within a signature creation application or outside, as long as it is done by the SCASC. The present document gives no restrictions on the type of TSP implementing such a service component.*

ETSI TS 119 102-1 V1.2.1 (2018-08) Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; **Part 1: Creation and Validation**

- https://www.etsi.org/deliver/etsi_ts/119100_119199/11910201/01.02.01_60/ts_11910201v010201p.pdf

- *The present document specifies procedures for:*
  - *the creation of AdES digital signatures (specified in ETSI EN 319 122-1 [i.2], ETSI EN 319 132-1 [i.4], ETSI EN 319 142-1 [i.6] respectively);*
  - *establishing whether an AdES digital signature is technically valid;*
- *whenever the AdES digital signature is based on public key cryptography and supported by public key certificates.*

- ETSI EN 319 102-1 V1.1.1 (2016-05), EN 319 102-1 - V1.1.1 (2016-05) - Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation (etsi.org)

ETSI TS 119 102-2 V1.2.1 (2019-02) Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; **Part 2: Signature Validation Report**

- https://www.etsi.org/deliver/etsi_ts/119100_119199/11910202/01.02.01_60/ts_11910202v010201p.pdf

- *The present document specifies a general structure and an XML format for reporting the validation of AdES digital signatures (specified in ETSI EN 319 122-1 [i.1], ETSI EN 319 132-1 [4], ETSI EN 319 142-1 [i.3] respectively). The present document is aligned with the requirements specified in ETSI TS 119 102-1 [1].*

- *An update is in preparation.*

- ETSI TS 119 102-2 V1.1.1 (2018-08) , https://www.etsi.org/deliver/etsi_ts/119100_119199/11910202/01.01.01_60/ts_11910202v010101p.pdf

LUONNOS 9.4.2021

ETSI TS 119 441 V1.1.1 (2018-08) Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing **signature validation services**

- https://www.etsi.org/deliver/etsi_ts/119400_119499/119441/01.01.01_60/ts_119441v010101p.pdf
- *An update is in preparation.*
- *The present document, based on the general policy requirements specified in ETSI EN 319 401 [2], specifies policy and security requirements for signature validation services operated by a TSP.*
    - ***NOTE 1: Beside signature validation, other signature services, like signature creation, signature augmentation or signature preservation can also be offered by TSPs. Such services can be provided as stand-alone services or combined (e.g. augmentation can be used to support a preservation service). The present document does not provide requirements on signature services beyond validation and does not provide requirements on how to combine signature related services.***
    - *NOTE 2: A distinct Technical Specification (TS) provides policy and security requirements for TSP offering signature augmentation services as a stand-alone service or in complement to one of the above-mentioned services.*
- ***The present document is aimed at trust services supporting the validation of digital signatures in accordance with ETSI TS 119 102-1 [3]**. It takes into account the relevant requirements for signature validation application specified in ETSI TS 119 101 [1] as they relate to TSPs.*
- *It is aimed at supporting the validation of digital signatures in European and other regulatory frameworks.*
    - *NOTE 3: Specifically, but not exclusively, the present document is aimed at qualified and non-qualified trust services, supporting the validation of digital signatures in accordance with the requirements of the Regulation (EU) No 910/2014 [i.1] for validation of electronic signatures and electronic seals (both advanced and qualified). Annex B complements the requirements for signature validation service providers offering a Qualified Validation Service for qualified electronic signatures or for qualified electronic seals as specified by Regulation (EU) No 910/2014 [i.1].*
    - *NOTE 4: Specifically, but not exclusively, digital signatures in the present document cover electronic signatures, advanced electronic signatures, qualified electronic signatures, electronic seals, advanced electronic seals, and qualified electronic seals as per Regulation (EU) No 910/2014 [i.1].*
- *The present document may be used by competent bodies as the basis for confirming that an organization is trustworthy in validating digital signatures on behalf of other persons or on its own behalf.*

LUONNOS 9.4.2021

- *NOTE 5: See ETSI EN 319 403 [i.13] for guidance on assessment of TSP processes and services.*

- *The user's interface is outside the scope of the main TSP service. However, the present document provides in annex D recommendations for the user's interfaces (for inputting the request and to visualize the validation report).*

- *The TSP has connections with external (trust) services that can be contacted for provisioning validation information, or to relay the validation request. The present document does not put requirements on the trust service policies applied by such external services.*

- *The present document identifies specific controls needed to address specific risks associated with validation services.*

ETSI SR 019 020 V1.1.2 (2016-08) The framework for standardization of signatures; Standards for AdES digital signatures in mobile and distributed environments

- https://www.etsi.org/deliver/etsi_sr/019000_019099/019020/01.01.02_60/sr_019020v010102p.pdf

- *The present document provides the framework for further standardisation for the creation and validation of advanced electronic signatures (AdES) in mobile environments (i.e. in environments where mobile devices are supported by networked services for signature creation and/or validation) taking into account recent improvements in the capabilities of mobile devices and their overlap with the capabilities other computing devices. It identifies the recommended scope of such standards and any suggested provision thought appropriate to these standards.*

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

- https://www.etsi.org/deliver/etsi_ts/119100_119199/119101/01.01.01_60/ts_119101v010101p.pdf

- *This document provides policy requirements for electronic Signature Creation and Validation (Applications). This would include procedural aspects that are not directly machine processable, as well as aspects which may be defined in a machine processable.*
  Policy requirements for electronic Signature Creation and Validation (Applications), including procedural aspects that are not directly machine processable, as well as aspects which may be defined in a machine processable, will be produced here taking into account STF member expertise , in business application and technical implementation of electronic signatures, and in conformity assessment of electronic signatures.

LUONNOS 9.4.2021

5 Säädäntö

5.1 Määräyksen antamisen perusta

42 § (23.11.2018/1009) Yleinen ohjaus sekä Liikenne- ja viestintäviraston määräykset

Vahvan sähköisen tunnistamisen ja sähköisten luottamuspalveluiden yleinen ohjaus ja kehittäminen kuuluvat liikenne- ja viestintäministeriölle.

Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä:

…

5) 29, 30 ja 32 §:ssä tarkoitetuista arvioitavan tunnistus- tai luottamuspalvelun sekä kansallisen solmupisteen vaatimustenmukaisuuden arviointiperusteista;

6) 33 §:ssä säädetyistä vaatimustenmukaisuuden arviointielimen pätevyysvaatimuksista ottaen huomioon, mitä sähköisestä tunnistamisesta ja luottamuspalveluista annetussa EU:n asetuksessa säädetään;

7) 35 §:ssä tarkoitettuun hakemukseen sisällytettävistä tiedoista ja niiden toimittamisesta Liikenne- ja viestintävirastolle;

8) 36 §:ssä tarkoitettua sertifiointilaitosta koskevista vaatimuksista, sertifioinnissa noudatettavasta menettelystä sekä sähköisen allekirjoituksen ja leiman luontivälinettä koskevista vaatimuksista ottaen huomioon, mitä sähköisestä tunnistamisesta ja luottamuspalveluista annetussa EU:n asetuksessa säädetään.

5.2 Asiaan liittyvät säännökset

5.3 Muu sääntely

LUONNOS 9.4.2021