Määräys sähköisistä tunnistus- ja luottamuspalveluista

Annettu Helsingissä 14 päivänä toukokuuta 2018

Viestintävirasto on määrännyt 7 päivänä elokuuta 2009 annetun vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain (617/2009) 42 §:n nojalla, sellaisena kuin se on muutettuna lailla 533/2016:

Luku 1 Yleiset säännökset

1 § Määräyksen tarkoitus

Tämän määräyksen tarkoituksena on

1) edistää vahvojen sähköisten tunnistusvälineiden ja tunnistusvälityspalveluiden tietoturvallisuutta ja teknistä yhteentoimivuutta,

2) tarkentaa vahvan sähköisen tunnistamisen palveluiden vaatimustenmukaisuuden arvioinnin kriteerit ja arviointielinten riippumattomuus- ja pätevyyskriteerit,

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

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

2 § Soveltamisala

Tätä määräystä sovelletaan vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain (617/2009, jäljempänä *tunnistus- ja luottamuspalvelulaki*) tarkoittamien Viestintävirastolle ilmoitettujen vahvan sähköisen tunnistamisen tunnistusvälineiden ja tunnistusvälityspalvelujen tarjontaan sekä näiden vaatimustenmukaisuuden arviointiin.

Tätä määräystä sovelletaan Euroopan parlamentin ja neuvoston (EU) N:o 910/2014 sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta antamassa asetuksessa (jäljempänä *sähköisestä tunnistamisesta ja luottamuspalveluista annettu EU:n asetus* tai *eIDAS-asetus*) tarkoitettuihin hyväksyttyihin sähköisiin luottamuspalveluihin ja näiden vaatimustenmu-

kaisuuden arviointiin sekä sähköisen allekirjoituksen tai leiman luontivälineiden sertifiointiin.

Tätä määräystä sovelletaan Euroopan komissiolle ilmoitettaviin vahvan sähköisen tunnistamisen järjestelmiin tai 2 edellä momentissa tarkoitettuihin luottamuspalveluihin ja näiden vaatimustenmukaisuuden arviointiin sekä sähköisen allekirjoituksen tai leiman luontivälineiden sertifiointiin vain, jollei eIDAS-asetuksesta tai sen nojalla annetuista komission täytäntöönpanosäädöksistä muuta johdu.

3 § Määritelmät

Tässä määräyksessä tarkoitetaan:

1) *rajapinnalla* tiedonsiirtoon liittyviä määrittelyjä ja toteutuksia kahden eri järjestelmän tai niiden osien välillä;

2) *eIDAS-rajapinnalla* kansallisen solmupisteen rajapintaa toisen valtion kansalliseen solmupisteeseen.

Muutoin tässä määräyksessä sovelletaan samoja määritelmiä kuin tunnistus- ja luottamuspalvelulaissa ja eIDAS-asetuksessa.

Luku 2 Tunnistuspalvelun tietoturvavaatimukset

4 § Tunnistuspalvelun tarjoajan tietoturvallisuuden hallinnan vaatimukset

Tunnistuspalveluntarjoajan on käytettävä tunnistusjärjestelmän tietoturvallisuuden hallinnassa ISO/IEC 27001 -standardia tai muuta yleisesti tunnettua vastaavaa tietoturvallisuuden hallinnan standardia. Tietoturvallisuuden hallinta voi perustua myös useamman standardin yhdistelmään.

Tietoturvallisuuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osa-alueet

1) tunnistuspalveluntarjoajan toimintaympäristö kokonaisuutena;

2) tietoturvallisuuden hallinnan johtaminen, organisointi ja ylläpito;

3) tunnistuspalvelun tarjontaan liittyvien tietoturvallisuusriskien hallinta;

4) tietoturvallisuuden resursointi, pätevyys, henkilöstön tietoisuus tietoturvallisuudesta, viestintä ja dokumentointi sekä dokumentoidun tiedon hallinta;

5) tunnistuspalvelun tarjonnan suunnittelu ja ohjaus tietoturvavaatimusten täyttämiseksi; ja

6) tietoturvallisuuden hallinnan tehokkuuden ja toimivuuden arviointi.

5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet

Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän

1) tietoliikenneturvallisuus

   a) verkon rakenteellinen turvallisuus

   b) tietoliikenneverkon vyöhykkeistäminen

   c) suodatussäännöt vähimpien oikeuksien periaatteilla

   d) suodatuksen ja valvontajärjestelmien hallinnointi koko elinkaaren ajan

   e) hallintayhteydet

2) tietojärjestelmäturvallisuus

   a) pääsyoikeuksien hallinta

   b) järjestelmien käyttäjien tunnistaminen

   c) järjestelmien koventaminen

   d) haittaohjelmasuojaus

   e) turvallisuuteen liittyvien tapahtumien jäljitys

   f) poikkeamien havainnointikyky ja toipuminen

   g) kansainvälisesti tai kansallisesti suositellut salausratkaisut muutoin kuin 7 §:ssä säädetyltä osin

3) käyttöturvallisuus

   a) muutosten hallinta

   b) salassa pidettävän aineiston käsittely-ympäristö

   c) etäkäyttö ja -hallinta

   d) ohjelmistohaavoittuvuuksien hallinta

   e) varmuuskopiointi

Tuotantoverkko ja sen edellä 1 momentin 1) e) ja 3) c) alakohdissa tarkoitetut hallintayhteydet ja etäkäyttö- ja etähallinta on toteutettava siten, että organisaation muiden palveluiden kuten sähköpostin tai web-selailun kautta aiheutuvat tietoturvauhat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvauhat on

a) korotetulla varmuustasolla erityisesti arvioitu ja minimoitu ja

b) korkealla varmuustasolla kokonaisuutena arvioiden estetty.

6 § Tunnistusmenetelmän tietoturvavaatimukset

Tunnistusvälinettä ei saa yhdistää hakijaan ennen hakijan ensitunnistamista tai tunnistusvälineen myöntämisprosessissa on muutoin varmistettava, että tunnistusväline ei ole käytettävissä ennen kuin tunnistus- ja luottamuspalvelulain 17 §:n mukainen ensitunnistaminen on tehty.

Palveluntarjoajan on varmistettava, etteivät tunnistusvälineeseen liittyvät salaiset tiedot paljastu sen henkilöstölle missään tilanteessa.

Palveluntarjoaja ei saa kopioida tunnistusvälineeseen liittyviä salaisia tietoja.

7 § Tunnistusjärjestelmän ja rajapintojen salausvaatimukset

Tunnistuspalveluntarjoajien välisten ja tunnistuspalveluntarjoajan ja asiointipalvelun välisten rajapintojen liikenne on salattava. Salauksessa, avaintenvaihdossa sekä salaukseen liittyvässä allekirjoituksessa on noudatettava seuraavia menetelmiä:

1) **Avaintenvaihto**: Avaintenvaihdossa on käytettävä DHE-menetelmiä tai elliptisiä käyriä käyttäviä ECDHE-menetelmiä. Laskutoimituksissa käytetyn äärellisen kunnan (*finite field*) koon tulee olla DHE-menetelmässä vähintään 2048 bittiä ja ECDHE-menetelmässä vähintään 224 bittiä.

2) **Allekirjoitus**: Käytettäessä RSA:ta sähköiseen allekirjoitukseen, avaimen pituuden tulee olla vähintään 2048 bittiä. Käytettäessä elliptisen käyrän menetelmää ECDSA:ta alla olevan kunnan koon tulee olla vähintään 224 bittiä.

3) **Symmetrinen salaus**: Salausalgoritmin on oltava AES tai Serpent. Avaimen pituuden tulee olla vähintään 128 bittiä. Salausmoodin on oltava CBC, GCM, XTS tai CTR.

4) **Tiivistefunktiot**: Tiivistefunktion on oltava SHA-2, SHA-3 tai Whirlpool. SHA-2:lla tarkoitetaan funktioita SHA224, SHA256, SHA384 ja SHA512.

Salausasetukset tulee teknisesti pakottaa edellä lueteltuihin vähimmäistasoihin, jotta yhteyskättelyissä ei päädyttäisi vähimmäistasoja heikompiin asetuksiin.

Mikäli yhteyskäytännössä käytetään TLS-protokollaa, tulee käyttää vähintään TLS versiota 1.2 tai uudempaa versiota. TLS versiota 1.1 voi käyttää ainoastaan, jos käyttäjän päätelaite ei tue uudempia versioita.

Henkilötietoja sisältävien sanomien eheys ja luottamuksellisuus on suojattava edellä 1 momentissa tarkoitetun liikenteen salauksen lisäksi sanomatasolla 1 momentin mukaisesti.

Tunnistusjärjestelmässä säilytettävien tietojen eheydestä ja luottamuksellisuudesta on huolehdittava. Jos tiedon suojaaminen perustuu ainoastaan niiden salaukseen, sovelletaan edellä 1 momentissa allekirjoittamisen, symmetrisen salaamisen ja tiivistefunktioiden vaatimuksia.

8 § Tietoturvavaatimukset tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa

Salausmenetelmien tulee täyttää edellä 7 §:n 1 - 4 momentissa määrätyt vaatimukset.

Osapuolten tunnistamisessa ja tunnistamisessa tarvittavan tiedon välityksessä tulee käyttää metadataa tai vastaavia menettelyitä, jotka takaavat vastaavan tietoturvatason.

Kaikki henkilötiedot tulee salata ja allekirjoittaa sanomatasolla.

9 § Tietoturvavaatimukset asiointipalvelurajapinnassa

Tunnistusvälityspalvelun tarjoajan ja asiointipalvelun välisen rajapinnan tulee täyttää edellä 7 §:n 1 - 4 momentissa määrätyt vaatimukset.

Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tulee huolehtia henkilötietojen luottamuksellisuudesta ja eheydestä asiointipalvelu- ja käyttäjärajapinnassa.

10 § Tietoturvavaatimukset kansallisen solmupisteen rajapinnassa

Tunnistusvälityspalvelun tarjoajan ja kansallisen solmupisteen välisen rajapinnan tulee täyttää edellä 7 §:n 1 - 4 momentissa määrätyt vaatimukset.

11 § Tunnistuspalveluntarjoajan häiriöilmoitukset Viestintävirastolle

Viestintävirastolle tunnistus- ja luottamuspalvelulain 16 §:n mukaisesti tehtävässä merkittävää uhkaa tai häiriötä koskevassa ilmoituksessa on annettava vähintään seuraavat tiedot:

1) tunnistusväline tai välityspalvelu, johon häiriö vaikuttaa;

2) kuvaus häiriöstä ja sen tiedossa olevista syistä;

3) kuvaus häiriön vaikutuksista, mukaan lukien vaikutus uusien tunnistusvälineiden myöntämiseen, käyttäjiin, luottaviin osapuoliin, muihin luottamusverkoston toimijoihin ja rajat ylittävään käyttöön;

4) kuvaus korjaustoimenpiteistä; sekä

5) kuvaus häiriöstä tiedottamisesta luottaville osapuolille, tunnistusvälineiden haltijoille, luottamusverkostolle ja tieto ilmoittamisesta muille viranomaisille.

Häiriön merkittävyyden arvioinnissa merkittävyyttä lisää se, että häiriö liittyy sähköisen henkilöllisyyden virheellisyyteen tai väärinkäyttöön tai tietoturvauhkaan tai -häiriöön, joka vaarantaa tunnistamisen eheyden ja luotettavuuden. Merkittävyyttä lisää myös se, että häiriöllä on vaikutuksia luottamusverkostoon.

Luku 3 Tietojen välittäminen luottamusverkostossa

12 § Luottamusverkostossa välitettävät vähimmäistiedot

Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on välitettävä:

1) luonnollista henkilöä koskevassa tunnistustapahtumassa ainakin henkilön yksilöivä tunniste, henkilön etunimi, henkilön sukunimi ja henkilön syntymäaika;

2) oikeushenkilöä koskevassa tunnistustapahtumassa ainakin oikeushenkilöä edustavan luonnollisen henkilön yksilöivä tunniste, henkilön sukunimi, henkilön etunimi ja organisaation yksilöivä tunniste; sekä

3) tieto tunnistusvälineen korotetusta tai korkeasta varmuustasosta.

Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on oltava valmius välittää:

1) tieto siitä, koskeeko tunnistustapahtuma julkisen hallinnon asiointipalvelua vai yksityistä asiointipalvelua;

2) luonnollista henkilöä koskevassa tunnistustapahtumassa etunimi (-nimet) ja sukunimi (-nimet) syntymähetkellä, syntymäpaikka, nykyinen osoite ja sukupuoli;

3) oikeushenkilöä koskevassa tunnistustapahtumassa

   a) nykyinen osoite;

   b) arvonlisäverotunniste;

   c) verorekisterinumero;

   d) Euroopan parlamentin ja neuvoston direktiivin 2009/101/EY[1] 3 artiklan 1 kohdassa tarkoitettu tunniste;

   e) komission täytäntöönpanoasetuksessa (EU) N:o 1247/2012[2] tarkoitettu oikeushenkilötunnus (LEI);

   f) komission täytäntöönpanoasetuksessa (EU) N:o 1352/2013[3] tarkoitettu taloudellisen toimijan rekisteröinti- ja tunnistenumero (EORI-numero); sekä

   g) neuvoston asetuksen N:o 389/2012[4] 2 artiklan 12 kohdassa tarkoitettu valmisteveronumero.

---

[1] Euroopan parlamentin ja neuvoston direktiivi 2009/101/EY, annettu 16 päivänä syyskuuta 2009, niiden takeiden yhteensovittamisesta samanveroisiksi, joita jäsenvaltioissa vaaditaan perustamissopimuksen 48 artiklan toisessa kohdassa tarkoitetuilta yhtiöiltä niiden jäsenten sekä ulkopuolisten etujen suojaamiseksi (EUVL L 258, 1.10.2009, s. 11).
[2] Komission täytäntöönpanoasetus (EU) N:o 1247/2012, annettu 19 päivänä joulukuuta 2012, kauppatietorekistereihin OTC- johdannaisista, keskusvastapuolista ja kauppatietorekistereistä annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 648/2012 mukaisesti annettavien kauppailmoitusten muotoa ja antamistiheyttä koskevista teknisistä täytäntöönpanostandardeista (EUVL L 352, 21.12.2012, s. 20).
[3] Komission täytäntöönpanoasetus (EU) N:o 1352/2013, annettu 4 päivänä joulukuuta 2013, teollis- ja tekijänoikeuksien tullivalvonnasta annetussa Euroopan parlamentin ja neuvoston asetuksessa (EU) N:o 608/2013 säädettyjen lomakkeiden vahvistamisesta (EUVL L 341, 18.12.2013, s. 10).

13 § Rajat ylittävän tunnistamisen edellyttämät tiedot

Tunnistauduttaessa suomalaisella tunnistusvälineellä ulkomaiseen asiointipalveluun tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on välitettävä samat tiedot kuin luottamusverkostossa on välitettävä 12 §:n mukaan kansallisessa tunnistautumisessa. Tiedot tulee olla mahdollista välittää edelleen tunnistusvälityspalvelun ja kansallisen solmupisteen välillä. Lisäksi on välitettävä tieto siitä, kohdistuuko tunnistustapahtuma julkisen hallinnon asiointipalveluun vai yksityiseen asiointipalveluun.

Tunnistauduttaessa ulkomaisella tunnistusvälineellä suomalaiseen asiointipalveluun kansallisen solmupisteen ja välityspalvelun tarjoajan välisessä rajapinnassa on välitettävä kansainvälisessä eIDAS-rajapinnassa määritellyt minimitiedot ja rajapinnassa on oltava valmius välittää kansainvälisessä eIDAS-rajapinnassa määritellyt valinnaiset tiedot. Henkilön yksilöivä tunnistetieto välitetään siinä muodossa, missä kansallinen solmupiste vastaanottaa sen kansainvälisestä eIDAS-rajapinnasta. Tiedot tulee olla mahdollista välittää edelleen tunnistusvälityspalvelun ja asiointipalvelun välillä. Lisäksi on välitettävä tieto siitä, kohdistuuko tunnistustapahtuma julkisen hallinnon asiointipalveluun vai yksityiseen asiointipalveluun.

14 § Tiedonsiirrossa käytettävä protokolla ja muut vaatimukset

Tunnistusvälineen tarjoaja, tunnistusvälityspalvelun tarjoaja ja asiointipalvelun tarjoaja sekä kansallisen solmupisteen toteuttaja sopivat keskenään niiden välisten rajapintojen muista kuin tässä määräyksessä säädetyistä ominaisuuksista ja käytettävästä protokollasta.

Luku 4 Tunnistuspalvelun arviointikriteerit

15 § Arviointikriteerit

Tunnistuspalvelun arvioinnin täytyy kattaa vaatimukset, jotka kohdistuvat:

1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän)
    a) tietoturvallisuuden hallintaan
    b) tietojen säilyttämiseen
    c) tiloihin ja henkilökuntaan
    d) teknisiin toimenpiteisiin
2) tunnistusmenetelmään eli tunnistusvälineen
    a) hakemiseen ja rekisteröintiin
    b) hakijan henkilöllisyyden todistamiseen ja varmentamiseen

[4] Neuvoston asetus (EU) N:o 389/2012, annettu 2 päivänä toukokuuta 2012, hallinnollisesta yhteistyöstä valmisteverotuksen alalla ja asetuksen (EY) N:o 2073/2004 kumoamisesta (EUVL L 121, 8.5.2012, s. 1).

c) tunnistamisen menetelmän ominaispiirteisiin ja laatimiseen

d) myöntämiseen, toimittamiseen ja aktivointiin

e) voimassaolon keskeyttämiseen, peruuttamiseen ja uudelleen aktivointiin

f) uusimiseen ja korvaamiseen

g) todentamismekanismeihin

Edellä 1 momentissa mainittujen osa-alueiden arvioinnin on perustuttava tunnistus- ja luottamuspalvelulain ja tämän määräyksen vaatimuksiin, EU:n tai muun kansainvälisen toimielimen antamiin säännöksiin tai ohjeisiin, julkaistuihin ja yleisesti tai alueellisesti sovellettuihin tietoturvallisuutta koskeviin ohjeisiin tai yleisesti käytettyihin tietoturvallisuusstandardeihin tai menettelyihin.

16 § Selvitys muiden vaatimusten täyttämisestä

Tunnistuspalveluntarjoajan on osoitettava omalla kirjallisella selvityksellään tai edellä 15 §:ssä tarkoitetulla arvioinnilla seuraavien tunnistuspalveluntarjoajan luotettavuuteen ja tunnistuspalvelusta annettaviin tietoihin liittyvien vaatimusten täyttyminen:

1) julkaistut ilmoitukset ja käyttäjätiedot, kuten tunnistusperiaatteet, sopimusehdot ja hinnastot

2) vakiintunut organisaatio

3) valmius ottaa vahinkoriskejä

4) riittävät taloudelliset varat

5) vastuu alihankkijoista

6) suunnitelma toiminnan päättämisen varalta

17 § Kansallisen solmupisteen arviointiperusteet

Kansallisen solmupisteen tietoturvallisuuden arvioinnin tulee perustua ISO/IEC 27001 -standardiin ja Euroopan komission täytäntöönpanoasetukseen (EU) 2015/1501[5].

Luku 5 Tunnistuspalvelun arviointielimen pätevyys

18 § Tunnistuspalvelun ulkoisen arviointielimen vaatimukset

Tunnistus- ja luottamuspalvelulain 33 §:ssä arviointielimelle säädettyjen riippumattomuus- ja pätevyysvaatimusten täyttymisen voi osoittaa:

[5] Komission täytäntöönpanoasetus yhteentoimivuusjärjestelmän vahvistamisesta sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 12 artiklan 8 kohdan mukaisesti

1) ISO/IEC 27001 -standardiin perustuvalla akkreditoinnilla tai osoittamalla muutoin pätevyys standardin mukaiseen arviointiin;

2) Webtrust -säännöstöön perustuvalla kansainvälisesti tunnetun itsesääntelyjärjestelyn mukaisesti osoitetulla pätevyydellä;

3) PCI DSS - maksukorttistandardiin perustuvalla akkreditoinnilla tai osoittamalla muutoin pätevyys standardin mukaiseen arviointiin;

4) ISACA:n standardien ja tietojärjestelmien valvontakehikon mukaisesti osoitetulla pätevyydellä; tai

5) muiden edellisiin rinnastettavien yleiseen tietoturvallisuuden hallintaan taikka sektorikohtaiseen sääntelyyn tai standardointiin liittyvien säännösten, ohjeiden tai standardien edellyttämän pätevyyden osoittamisella tai noudattamisella.

Pätevyyden osoittaminen tunnistusjärjestelmän arviointiin edellyttää sitä, että osoitetaan myös, miten ja miltä osin edellä 1 momentissa tarkoitetut säännökset, ohjeet tai standardit kohdistuvat tunnistusjärjestelmään.

19 § Tunnistuspalvelun sisäisen tarkastuslaitoksen vaatimukset

Tunnistus- ja luottamuspalvelulain 33 §:ssä sisäiselle tarkastuslaitokselle säädettyjen riippumattomuusvaatimusten täyttymisen voi osoittaa:

1) IIA:n ammattistandardien (sisäisen tarkastuksen riippumattomuus ja objektiivisuus, ml. organisatorinen riippumattomuus) noudattamisella;

2) ISACA:n standardien ja tietojärjestelmien valvonnan kehikoiden noudattamisella;

3) BIS:in (Bank for International Settlements) sisäistä tarkastusta koskevien ohjeiden noudattamisella;

4) Finanssivalvonnan määräys- ja ohjekokoelman sisäistä tarkastusta koskevien määräysten ja ohjeiden noudattamisella;

5) muiden ETA-alueen jäsenvaltioiden vastaavien valvontaviranomaisten antamien ohjeiden tai määräysten noudattamisella; tai

6) muilla edellisiin rinnastettavilla viranomaissääntelyyn tai yleiseen riippumattoman sisäisen tarkastuksen hallintaan liittyvien standardien noudattamisella.

Pätevyyden osoittaminen tunnistusjärjestelmän arviointiin edellyttää sitä, että osoitetaan myös, miten ja miltä osin 1 momentissa tarkoitettujen säännösten, ohjeiden tai standardien mukaisesti organisoitu sisäinen tarkastus kohdistuu tunnistusjärjestelmään.

Luku 6 Hyväksytyt luottamuspalvelut

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.

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.

Luku 7 Luottamuspalvelujen vaatimustenmukaisuuden arviointilaitokset

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.

Luku 8 Hyväksytyn sähköisen allekirjoituksen ja sähköisen leiman luontivälineen sertifiointi

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[6].

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.

Luku 9 Voimaantulosäännökset

25 § Voimaantulo ja siirtymäsäännökset

Tämä määräys tulee voimaan 22.5.2018 ja on voimassa toistaiseksi.

Tällä määräyksellä kumotaan Viestintäviraston 2.11.2016 antama määräys 72/2016 M sähköisistä tunnistus- ja luottamuspalveluista.

Jos tunnistuspalvelun rajapinnoissa käytetään Tupas-protokollaa, 2 luvun 7 §:n 4 momentin ja 8 §:n 3 momentin vaatimukset henkilötietojen sanomatasoisesta salauksesta sekä 9 §:n 2 momentin vaatimus henkilötietojen suojaamisesta asiointipalvelu- ja päätelaiterajapinnassa on toteutettava

[6] 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

kaikilta osin viimeistään 1.10.2019. Tunnistuspalvelun tarjoajan on määriteltävä tämän määräyksen vaatimukset täyttävä toteutus teknisesti viimeistään 1.10.2018 ja saatettava muutetut rajapinnat tarjolle luottamusverkostossa sekä luottaville osapuolille viimeistään 1.3.2019.

Valmius määräyksen 12 §:n 2 momentin mukaisten tietojen välittämiseen tunnistusjärjestelmässä on suunniteltava teknisesti viimeistään 1.10.2018.

26 § Tiedonsaanti ja julkaiseminen

Tämä määräys on julkaistu Viestintäviraston määräyskokoelmassa ja se on saatavissa Viestintäviraston asiakaspalvelusta:

Käyntiosoite	Itämerenkatu 3 A, Helsinki
Postiosoite	PL 313, 00181 Helsinki
Puhelin	0295 390 100
Faksi	0295 390 270
WWW-sivusto	http://www.viestintävirasto.fi/
Y-tunnus	0709019-2

Helsingissä 14 päivänä toukokuuta 2018

Kirsi Karlamaa
pääjohtaja

Jarkko Saarimäki
johtaja