Antopäivä:	Voimaantulopäivä:	Voimassa:
20.5.2022	1.6.2022	toistaiseksi

Säädösperusta
Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009) 42 §, sellaisena kuin se on muutettuna lailla 230/2021

Määräyksen vastaisen toiminnan seuraamuksista säädetään:

Laki 617/2009 45 §, 45 a §

Täytäntöönpantava EU-lainsäädäntö:
-

Muutostiedot:
Määräyksellä kumotaan määräys Viestintävirasto 72 A/2018 M

Määräys sähköisistä tunnistus- ja luottamuspalveluista (M72 B/2022)

Sisällys

Luku 1 Yleiset säännökset

1 Soveltamisala

1.1

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

1.2

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 vaatimustenmukaisuuden arviointiin sekä sähköisen allekirjoituksen tai leiman luontivälineiden sertifiointiin.

1.3

Tätä määräystä sovelletaan Euroopan komissiolle ilmoitettaviin 1 kohdassa tarkoitettuihin vahvan sähköisen tunnistamisen järjestelmiin tai 2 kohdassa 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.

2 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.

3 Määritelmät

3.1

Tässä määräyksessä tarkoitetaan:

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

2) *varmenteella* sähköistä todistusta, jonka tarkoitus on osoittaa, että todistuksen haltija on tietty henkilö, organisaatio tai järjestelmä ja jolla liitetään todentamistiedot haltijaan.

3.2

Lisäksi tässä määräyksessä noudatetaan tunnistus- ja luottamuspalvelulain 2 §:ssä, eIDAS-asetuksen 3 artiklassa ja eIDAS-asetuksen 8 artiklan 3 kohdan mukaisesti annetun komission täytäntöönpanoasetuksen (EU) 2015/1502, jäljempänä *sähköisen tunnistamisen varmuustasoasetus*, liitteen 1 kohdassa annettuja määritelmiä.

Luku 2 Tunnistuspalvelun tietoturvavaatimukset

4 Tunnistuspalvelun tarjoajan tietoturvallisuuden hallintajärjestelmä

4.1 Tietoturvallisuuden hallinnan standardi

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

4.2 Tietoturvallisuuden hallinnan kattavuus

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 tietoturvavaatimukset

5.1 Tunnistusjärjestelmän suojautumiskyky

5.1.1

Tunnistusjärjestelmän tietoliikenne, tietojärjestelmät ja niiden käyttö on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä koko elinkaaren ajan siten, että tunnistuspalvelun eheys ja luottamuksellisuus on suojattu. Tunnistuspalvelulla on oltava suojautumiskyky vähintään tunnistuspalvelun varmuustason mukaista sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.3 tarkoitettua kohtuullisen tai korkean vakavuustason uhkaa ja hyökkäyspotentiaalia vastaan.

5.1.2

Tunnistuspalvelun tarjoajien välisten sekä tunnistuspalvelun ja luottavan osapuolen välisten tietoliikenneyhteyksien salausvaatimukset määrätään kohdassa 7. Tunnistusjärjestelmän muiden tietoliikenneyhteyksien sekä tietojärjestelmien ja tiedon salauksessa on käytettävä teknisesti soveltuvin osin määräyksen 7 kohdan mukaisia salausratkaisuja, ellei suojautumiskyky kokonaisuutena arvioiden toteudu muilla turvatoimenpiteillä.

5.2 Tietoliikenneturvallisuus

Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:

a) verkon rakenteellinen turvallisuus;

b) tietoliikenneverkon vyöhykkeistäminen;

c) suodatussäännöt vähimpien oikeuksien periaatteilla;

d) suodatuksen ja valvontajärjestelmien hallinnointi;

e) turvalliset hallintayhteydet; sekä

f) käytettävä kansainvälisesti tai kansallisesti suositeltuja salausratkaisuja.

5.3 Tietojärjestelmäturvallisuus

Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:

a) pääsyoikeuksien hallinta vähimpien oikeuksien periaatteella;

b) järjestelmien käyttäjien yksilöity tunnistaminen;

c) järjestelmien koventaminen;

d) haittaohjelmasuojaus;

e) turvallisuuteen liittyvien tapahtumien jäljityskyky ja jäljitysprosessi;

f) poikkeamien havainnointikyky ja korjausprosessi; sekä

g) käytettävä kansainvälisesti tai kansallisesti suositeltuja salausratkaisuja.

5.4 Käyttöturvallisuus

Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:

a) muutosten hallinta;

b) tiedon luokitteluun perustuva salassa pidettävän aineiston käsittely-ympäristö ja säilytys;

c) etäkäytön ja -hallinnan suojaaminen etäkäyttöympäristön uhkilta;

d) ohjelmistokehityksen ja ohjelmistohaavoittuvuuksien hallinta;

e) varmuuskopiointi; sekä

f) käytettävä kansainvälisesti tai kansallisesti suositeltuja salausratkaisuja.

5.5 Tunnistusjärjestelmän tuotantoverkon hallinta- ja etäyhteydet

Tuotantoverkko ja sen edellä 5.2.e) ja 5.4.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

6.1 Tunnistusmenetelmän ominaispiirteet ja suojautumiskyky

6.1.1

Tunnistusmenetelmän todentamistekijät, todentamismekanismi ja turvatoimenpiteet on suunniteltava, toteutettava ja ylläpidettävä siten, että ne suojaavat tunnistusmenetelmän eheyden ja luottamuksellisuuden. Tunnistusmenetelmällä on oltava suojautumiskyky vähintään tunnistuspalvelun varmuustason mukaista sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.3 tarkoitettua kohtuullisen tai korkean vakavuustason uhkaa ja hyökkäyspotentiaalia vastaan.

Suojautumiskyvyn on perustuttava riskiarvioon, jossa arvioidaan erikseen hallussapitoon, tietoon ja ominaisuuteen perustuviin todentamistekijöihin ja todentamismekanismiin kohdistuvat uhkat sekä uhkilta suojaavat turvatoimenpiteet.

6.1.2

Tunnistusmenetelmän ominaispiirteiden ja turvatoimenpiteiden on estettävä se, että yhden todentamistekijän vaarantuminen vaarantaisi muiden todentamistekijöiden luotettavuuden. Tunnistusmenetelmän turvatoimenpiteillä on eriytettävä ja suojattava todentamistekijät erityisesti, jos niitä käytetään samalla päätelaitteella.

6.1.3

Tunnistusmenetelmässä ja todentamisessa on käytettävä kansainvälisesti tai kansallisesti suositeltuja salausratkaisuja. Tunnistusvälineen ja tunnistusjärjestelmän välisellä tietoliikenneyhteydellä on käytettävä teknisesti soveltuvin osin määräyksen 7 kohdan mukaisia salausratkaisuja, ellei suojautumiskyky kokonaisuutena arvioiden toteudu muilla turvatoimenpiteillä.

6.2 Erityiset turvatoimenpiteet

6.2.1

Tunnistuspalvelun on näytettävä tunnistusvälineen käyttäjälle tunnistustapahtumassa tieto, jonka perusteella käyttäjä voi varmistaa, että tunnistusvälineeseen käyttäjän saama tunnistuspyyntö liittyy käyttäjän omaan asiointitapahtumaan. Tiedon näyttäminen on pakollista sellaisessa tunnistusmenetelmässä, jossa se on teknisesti mahdollista.

6.2.2

Tunnistuspalvelun on näytettävä tunnistusvälineen käyttäjälle tunnistustapahtumassa tieto luottavasta osapuolesta, jolle tunnistus välitetään. Tiedon näyttäminen on pakollista sellaisessa tunnistusmenetelmässä, jossa se on teknisesti mahdollista.

6.2.3

Kertakirjautumisella tarkoitetaan tässä määräyksessä sitä, että tunnistuspalvelu tarjoaa useammalle kuin yhdelle luottavalle osapuolelle vahvistuksen yhden vahvalla sähköisellä tunnistusmenetelmällä tehdyn tunnistusvälineen haltijan todentamisen perusteella.

Tunnistuspalvelun on kertakirjautumisen suunnittelussa, toteutuksessa ja ylläpidossa huolehdittava kertakirjautumiseen liittyvien istuntojen keston, siirtämisen ja lopettamisen hallintaan perustuvista turvatoimenpiteistä sekä 6.2.2 kohdan mukaisten luottavien osapuolten tietojen näyttämisestä käyttäjälle.

6.3 Tunnistusvälineen kytkeminen henkilöön

6.3.1

Tunnistusmenetelmän todentamistekijät on kytkettävä tunnistusjärjestelmässä tunnistusvälineen haltijaan.

6.3.2

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.

6.4 Tunnistusmenetelmän haltijakohtaisten tietojen käsittely

6.4.1

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

6.4.2

Tunnistuspalvelun tarjoaja ei saa kopioida tunnistusvälineeseen liittyviä salaisia tietoja.

7 Tunnistusjärjestelmän rajapintojen salausvaatimukset

7.1 Tietoliikenteen salausmenetelmät

7.1.1

Tunnistuspalvelun tarjoajien välisten ja tunnistuspalvelun tarjoajan ja luottavan osapuolen välisten rajapintojen liikenne on salattava. Salauksessa, avaintenvaihdossa, varmenteissa 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 tai epäsymmetrinen salaus:** Käytettäessä RSA:ta sähköiseen allekirjoitukseen tai salaukseen avaimen pituuden tulee olla vähintään 2048 bittiä. Käytettäessä elliptisen käyrän menetelmiä ECDSA:ta tai EdDSA:ta äärellisen kunnan koon tulee olla vähintään 224 bittiä.

3) **Symmetrinen salaus:** Salausalgoritmin on oltava AES, Serpent tai ChaCha20. Avaimen pituuden tulee olla vähintään 128 bittiä. Salausmoodin on oltava CBC, CCM, GCM tai CTR.

4) **Tiivistefunktiot:** Tiivistefunktion tai autentikaatiokoodin on oltava SHA-2, SHA-3, Whirlpool tai Poly1305.

7.1.2

Kohdassa 7.1.1 mainittujen lisäksi voidaan noudattaa menetelmiä ja arvoja, jotka on arvioitu turvallisiksi 1-4 alakohdissa tarkoitettuun käyttöön seuraavien asiakirjojen ajantasaisissa versioissa:

a) Liikenne- ja viestintävirastossa toimivan salaustuotteiden hyväksyntäviranomaisen *(Crypto Approval Authority)* ohje Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset turvallisuusluokat (Dnro 190/651/2015); tai

b) eräiden Euroopan unionin tai ETA-alueen jäsenvaltioissa toimivien sertifiointielinten välisen SOGIS-MRA (*Senior Officers Group for Information Systems, Mutual Recognition Agreement*) asiakirja SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms.

7.1.3

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

7.2 Tietoliikenteen salausprotokolla

Mikäli yhteyskäytännössä käytetään TLS-protokollaa, tulee käyttää vähintään TLS versiota 1.2.

8 Tietoliikenteen osapuolten varmentaminen

8.1 Tietoliikenneyhteyden osapuolten tunnistaminen

Tunnistuspalveluiden välisessä sekä tunnistuspalvelun ja luottavan osapuolen välisessä tietoliikenneyhteyden perustamisessa on todennettava tietoliikenteen tai sanomien salaamisessa käytettävien varmenteiden ja avainten aitous ja eheys sekä niiden haltijat.

Todentamisen on perustuttava eIDAS-asetuksen mukaiseen hyväksyttyyn sähköiseen allekirjoitukseen tai hyväksyttyyn sähköiseen leimaan taikka suoraan kahdenväliseen menettelyyn. Todentaminen ei voi perustua pelkästään yleisesti luotettuun varmenteeseen.

8.2 Varmenteiden ja avainten uusiminen

Edellä 8.1 kohdassa tarkoitetut varmenteet ja avaimet on uusittava säännöllisesti.

Uusien varmenteiden ja avainten aitouden ja eheyden varmistamiseksi uusiminen on tehtävä joko:

a) 8.1 kohdan mukaisella menettelyllä;

b) toimittamalla uudet avaimet tietoliikenneyhteydellä, jonka eheys ja luottamuksellisuus on varmistettu sitomalla osapuolten tietoliikenne 8.1 kohdan mukaisesti toimitettuihin varmenteisiin tai avaimiin; tai

c) allekirjoittamalla uusi avain 8.1 kohdan mukaisesti toimitetulla avaimella tai sellaisesta ketjutetulla avaimella.

9 Tunnistussanomien eheys ja luottamuksellisuus

9.1 Sanomien suojaaminen tunnistuspalveluiden ja luottavan osapuolen välillä

9.1.1

Tunnistuspalveluiden välisessä ja tunnistuspalvelun ja luottavan osapuolen välisessä tietoliikenteessä on suojattava henkilötietoja sisältävien tunnistussanomien eheys ja luottamuksellisuus joko:

a) varmistamalla tietoliikenneyhteyden eheys ja luottamuksellisuus sitomalla osapuolten tietoliikenne 8 kohdan mukaisesti toimitettuihin varmenteisiin tai avaimiin; tai

b) salaamalla ja allekirjoittamalla sanomat 8 kohdan mukaisella menettelyllä toimitetulla avaimella.

9.1.2

Tunnistusvälityspalvelun ja luottavan osapuolen välisessä tietoliikenteessä tunnistussanomat on todennettava allekirjoittamalla.

9.2 Sanomien suojaaminen käyttäjärajapinnassa

Jos tunnistussanomat välitetään käyttäjän selaimen tai päätelaitteen kautta, sanomat on salattava ja allekirjoitettava 9.1.1.b) alakohdan mukaisesti.

9.3 Salausalgoritmit ja menettelyt

Sanomien salaamisessa ja allekirjoittamisessa on käytettävä soveltuvin osin 7.1 kohdan mukaisia menettelyjä.

10 Tietoturvavaatimukset kansallisen solmupisteen rajapinnassa

Tunnistusvälityspalvelun tarjoajan ja kansallisen solmupisteen välisessä rajapinnassa tulee täyttää 7—9 kohdissa määrätyt vaatimukset.

11 Tunnistuspalveluntarjoajan häiriöilmoitukset Liikenne- ja viestintävirastolle

11.1 Merkittävät uhkat tai häiriöt

Liikenne- ja viestintävirastolle tunnistus- ja luottamuspalvelulain 16 §:n mukaisesti ilmoitettavia merkittäviä tunnistuspalvelun häiriöitä ovat tapahtumat, jotka liittyvät sähköisen henkilöllisyyden virheellisyyteen tai väärinkäyttöön tai tietoturvauhkaan tai -häiriöön, joka vaarantaa tunnistamisen eheyden ja luotettavuuden. Merkittäviä ovat myös ennakoimattomat toimivuushäiriöt, joilla on vähäistä suurempia haittavaikutuksia luottamusverkostoon.

11.2 Ilmoitettavat tiedot

Liikenne- ja viestintävirastolle tehtävässä merkittävää uhkaa tai häiriötä koskevassa ilmoituksessa on annettava vähintään seuraavat tiedot:

1) tunnistusväline tai tunnistusvälityspalvelu, johon häiriö tai uhka vaikuttaa;

2) kuvaus häiriöstä tai uhkasta ja sen tiedossa olevista syistä sekä kestosta;

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

4) kuvaus korjaustoimenpiteistä; sekä

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

11.3 Ilmoitusmenettely

Ilmoitus merkittävästä häiriöstä tai uhkasta on tehtävä sähköisesti Liikenne- ja viestintäviraston verkkolomakkeella, sähköpostilla tai turvasähköpostilla.

Ilmoituksen tietoja voi täydentää myöhemmin, jos kaikki tiedot eivät ole käytettävissä, kun tehdään ensi-ilmoitus tunnistus- ja luottamuspalvelulain 16 §:n mukaisesti ilman aiheetonta viivästystä.

Luku 3 Tunnistuspalveluiden yhteentoimivuus

12 Luottamusverkostossa välitettävät vähimmäistiedot

12.1 Pakolliset tiedot

Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on välitettävä:

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

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

3) tieto tunnistusvälineen korotetusta tai korkeasta varmuustasosta; sekä

4) tunnistusvälityspalvelun varmistama tieto luottavasta osapuolesta.

12.2 Valinnaiset tiedot

Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on oltava teknisesti suunniteltu 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; ja

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.

12.3 Tunnistuksen pseudonymisointi

Edellä 12.1 ja 12.2 kohdassa määrätyt velvoitteet koskevat tunnistusvälineen käyttäjän todentamisessa tunnistusvälineen ja tunnistusvälityspalvelun välistä rajapintaa siinäkin tapauksessa, että tunnistusvälityspalvelu ilmoittaa tunnistus- ja luottamuspalvelulain 8 §:n 2 momentissa tarkoitetulla tavalla luottavalle osapuolelle vain tunnistusvälineen käyttäjän salanimen tai rajoitetun määrän henkilötietoja.

13 Rajat ylittävän tunnistamisen edellyttämät tiedot

Tunnistauduttaessa suomalaisella eIDAS-asetuksen mukaisesti ilmoitetulla tunnistusvälineellä ulkomaiseen asiointipalveluun tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on välitettävä samat tiedot kuin luottamusverkostossa on välitettävä 12 kohdan 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.

14 Tiedonsiirrossa käytettävä protokolla ja muut vaatimukset

14.1 Tiedonsiirrossa käytettävä protokolla

Tunnistuspalvelun tarjoajan on osaltaan mahdollistettava tunnistuslain 17 §:n mukainen ensitunnistamisen ketjuttaminen ja tunnistuslain 12 a §:n mukainen tunnistustapahtumien välitys luottamusverkostossa vähintään OpenID Connect- tai SAML-protokollan mukaisella rajapinnalla.

---

[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).

[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).

14.2 Rajapinnan muut ominaisuudet

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

Luku 4 Tunnistuspalvelun arviointikriteerit

15 Vaatimuksenmukaisuuden arviointikriteerit

15.1 Tunnistusjärjestelmän ja tunnistusmenetelmän arvioitavat toiminnot

Tunnistuspalvelun tunnistus- ja luottamuspalvelulain 29 §:n mukaisen arvioinnin täytyy kattaa kaikki laissa ja tässä määräyksessä asetetut vaatimukset, jotka kohdistuvat:

1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän):
    a) tietoturvallisuuden hallintaan;
    b) tietojen säilyttämiseen ja käsittelyyn;
    c) tiloihin ja henkilökuntaan;
    d) teknisiin toimenpiteisiin; ja
    e) yhteentoimivuuteen luottamusverkostossa; sekä
2) tunnistusmenetelmään eli tunnistusvälineen:
    a) hakemiseen ja rekisteröintiin;
    b) hakijan henkilöllisyyden todistamiseen ja varmentamiseen;
    c) tunnistusmenetelmän ominaispiirteisiin ja laatimiseen;
    d) myöntämiseen, toimittamiseen ja aktivointiin;
    e) voimassaolon keskeyttämiseen, peruuttamiseen ja uudelleen aktivointiin;
    f) uusimiseen ja korvaamiseen; ja
    g) todentamismekanismeihin.

15.2 Arviointikriteeristö

Vaatimuksenmukaisuuden arviointi voi perustua Liikenne- ja viestintäviraston arviointiohjeeseen tai 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. Arviointi voi perustua usean edellä mainitun lähteen yhdistelmään.

16 Selvitys tunnistuspalvelun tarjoajan ja julkaistujen tietojen luotettavuudesta

Tunnistuspalvelun tarjoajan on tunnistus- ja luottamuspalvelulain 10 §:n mukaisessa ilmoituksessa osoitettava omalla kirjallisella selvityksellään tai riippumattomalla ja pätevällä selvityksellä tai arvioinnilla seuraavien tunnistuspalvelun tarjoajan luotettavuuteen ja tunnistuspalvelusta annettaviin tietoihin liittyvien vaatimusten täyttyminen:

1) tunnistuspalvelusta vastaava vakiintunut oikeushenkilö ja vastuuhenkilöiden toimintakelpoisuus ja luotettavuus;

2) julkaistut ilmoitukset ja käyttäjätiedot, kuten tunnistusperiaatteet, tietosuojaperiaatteet, käyttörajoitukset, sopimusehdot ja hinnastot;

3) riittävät taloudelliset voimavarat toiminnan järjestämiseksi ja mahdollisen vahingonkorvausvastuun kattamiseksi;

4) vastuu alihankkijoista; sekä

5) suunnitelma toiminnan päättämisen varalta palvelun hallitusta lopettamisesta tai siirrosta, tietojen käsittelystä sekä ilmoituksista viranomaisille, luottamusverkostolle, luottaville osapuolille ja käyttäjille.

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

18.1 Osoittamismenettelyt

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

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.

[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

18.2 Pätevyys

Pätevyyden osoittaminen tunnistusjärjestelmän arviointiin edellyttää sitä, että osoitetaan myös, miten ja miltä osin 18.1 kohdassa tarkoitetut säännökset, ohjeet tai standardit kohdistuvat tunnistusjärjestelmälle asetettuihin vaatimuksiin.

19 Tunnistuspalvelun sisäisen tarkastuslaitoksen vaatimukset

19.1 Riippumattomuus

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.

19.2 Pätevyys

Pätevyyden osoittaminen tunnistusjärjestelmän arviointiin edellyttää sitä, että osoitetaan myös, miten ja miltä osin 19.1 kohdassa tarkoitettujen säännösten, ohjeiden tai standardien mukaisesti organisoitu sisäinen tarkastus kohdistuu tunnistusjärjestelmälle asetettuihin vaatimuksiin.

Luku 6 Hyväksytyt luottamuspalvelut

20 Hyväksytyn luottamuspalvelun tarjoajan arviointikriteerit

20.1 Standardit

20.1.1

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

20.1.2

Sähköisten allekirjoitusten tai leimojen hyväksyttyjä varmenteita tai hyväksyttyjä verkkosivuvarmenteita myöntävän hyväksytyn luottamuspalvelun tarjoajan tulee 20.1.1 kohdan vaatimusten lisäksi täyttää standardien EN 319 411-1 ja EN 319 411-2 vaatimukset.

20.1.3

Hyväksyttyjä aikaleimoja myöntävän hyväksytyn luottamuspalvelun tarjoajan tulee 20.1.1 kohdan vaatimusten lisäksi täyttää standardin EN 319 421 vaatimukset.

20.2 Standardien vapaaehtoisuus

Vaatimusten täyttämisen voi osoittaa 20.1 kohdassa mainittujen standardien noudattamisella tai muulla tavalla, jolla saavutetaan vastaava luotettavuus.

21 Hyväksytyn luottamuspalvelun arviointikriteerit

21.1 Standardit

21.1.1

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.

21.1.2

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

21.1.3

Hyväksytyn sähköisen allekirjoituksen tai leiman hyväksytyssä validointipalvelussa tulee täyttää eIDAS-asetuksessa asetettujen vaatimusten lisäksi standardissa EN 319 102-1 esitetyt vaatimukset.

21.1.4

Hyväksytyssä sähköisessä rekisteröidyssä jakelupalvelussa tulee täyttää eIDAS-asetuksessa asetettujen vaatimusten lisäksi standardeissa EN 319 521 ja EN 319 522 esitetyt vaatimukset.

21.2 Standardien vapaaehtoisuus

Vaatimusten täyttämisen voi osoittaa 21.1 kohdassa mainittujen standardien noudattamisella tai muulla tavalla, jolla saavutetaan vastaava luotettavuus.

Luku 7 Luottamuspalvelujen vaatimustenmukaisuuden arviointilaitos

22 Arviointilaitosten pätevyyden arviointi

22.1 Arviointilaitoksen toiminta

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.

22.2 Pätevyys

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

Luku 8 Hyväksytyn sähköisen allekirjoituksen ja sähköisen leiman luontivälineen sertifiointi

23 Sähköisen allekirjoituksen tai leiman luontivälineen sertifiointilaitos

Tunnistus- ja luottamuspalvelulain 36 §:n vaatimusten täyttymisen edellytyksenä on riittävä pätevyys ja resurssit eIDAS-asetuksessa ja komission täytäntöönpanopäätöksessä (EU) 2016/650[6] tai sen korvaavassa päätöksessä asetettujen vaatimusten todentamiseen sertifioitavana olevassa välineessä.

Sertifiointilaitoksen 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 Siirtymäsäännökset ja allekirjoitukset

24 Voimaantulo ja siirtymäsäännökset

24.1

Määräys tulee voimaan 1.6.2022

24.2

Määräyksen 6.2.1 kohdan, 6.2.2 kohdan ja 12.1.4) alakohdan vaatimukset on toteutettava viimeistään 1.6.2023.

24.3

Määräyksen 8.1 kohdan vaatimus osapuolten tunnistamisesta on toteutettava

a) tunnistuspalveluiden välillä viimeistään 1.6.2023 ja

b) tunnistusvälityspalveluiden ja luottavien osapuolten välillä viimeistään 1.6.2023.

Määräyksen 8.2 kohdan vaatimus avainten ja varmenteiden päivittämisestä on otettava käyttöön viimeistään 1.6.2023.

[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

24.4

Määräyksen 9.1.1.a) alakohdan menettelyä voidaan käyttää, kun 8 kohdan vaatimusten mukainen avain tai varmenne on käytettävissä.

Määräyksen 9.1.1.b) alakohdan ja 9.1.2 kohdan vaatimukset on toteutettava viimeistään 24.3 kohdan siirtymäajassa.

Helsingissä 20 päivänä toukokuuta 2022

Kirsi Karlamaa
pääjohtaja

Sauli Pahlman
ylijohtaja