Antopäivä:	Voimaantulopäivä:	Voimassa:
x.x.2022	x.x.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 ja asetukset eivät sisällä ei kriminalisoituja velvoitteita]

Täytäntöönpantava EU-lainsäädäntö:
-

Muutostiedot:
Määräyksellä muutetaan määräystä Viestintävirasto 72 A/2018 M

Määräys sähköisistä tunnistus- ja luottamuspalveluista (M72B/2022)

(Sisällys)

LUKU 1 Yleiset säännökset

1 Soveltamisala

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

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.

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

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

Tässä määräyksessä tarkoitetaan:

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

~~1)~~2) ~~*eIDAS-rajapinnalla* kansallisen solmupisteen rajapintaa toisen valtion kansalliseen solmupisteeseen.~~

Lisäksi ~~Muutoin~~ tässä määräyksessä noudatetaan ~~sovelletaan samoja määritelmiä kuin~~ tunnistus- ja luottamuspalvelulain ~~ssa~~ 2 §:ssä, eIDAS-asetuksen 3 artiklassa ~~ssa.~~ 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 hallinnan vaatimukset

4.1 Tietoturvallisuuden hallinnan standardi

Tunnistuspalveluntarjoajan on noudatettava ~~käytettävä~~ 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 tekniset tietoturvatoimenpiteet

5.1 Tunnistusjärjestelmän turvallisuus ja luotettavuus

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

~~5.1~~5.2 Tietoliikenneturvallisuus

Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti 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) turvalliset hallintayhteydet

5.3 Tietojärjestelmäturvallisuus

Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä

~~2) tietojärjestelmäturvallisuus~~

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 ~~toipuminen~~

g) kansainvälisesti tai kansallisesti suositellut salausratkaisut sen lisäksi, mitä ~~muutoin kuin~~ 7 ja 9 kohdassa määrätään. ~~5:ssä säädetyltä osin~~

Commented [LA1]: Vaatimus ulottuu sekä 5.2. tietoliikenne- että 5.3 tietojärjestelmiin ja 5.4 operointiin.

~~5.2~~5.4 Käyttöturvallisuus

Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä

~~3) käyttöturvallisuus~~

a) huolellinen muutosten hallinta

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

c) etäkäytön~~tö~~ ja -hallinnan ~~ta~~ suojaaminen etäkäyttöympäristön uhkilta

d) ohjelmistokehityksen ja ohjelmistohaavoittuvuuksien hallinta

e) varmuuskopiointi

~~5.3~~5.5 Tunnistusjärjestelmän tuotantoverkon hallinta- ja etäyhteydet

Tuotantoverkko ja sen edellä 5.2 ~~1 momentin 1)~~ e) ~~ja 3)~~ 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 tekniset turvatoimenpiteet

1. Tunnistusmenetelmän todentamistekijät, todentamismekanismi ja turvatoimenpiteet on suunniteltava, toteutettava ja ylläpidettävä siten, että ne suojaavat menetelmän eheyden ja luottamuksellisuuden vähintään varmuustasoon suhteutetulta hyök-

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

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.

3. Tunnistusmenetelmässä ja todentamisessa on käytettävä kansainvälisesti tai kansallisesti suositeltuja salausratkaisuja. Tunnistusvälineen ja tunnistusjärjestelmän välisellä tietoliikenneyhteydellä on käytettävä teknisesti soveltuvin osin ja 1 kohdan uhka- ja riskiarviossa edellytetyllä tavalla määräyksen 7 kohdan mukaisia suositeltuja salausratkaisuja.

~~Siirtymäsäännös (?): riskiarvio menetelmästä laadittava x mennessä, uusilla toimijoilla aloitusilmoituksen yhteydessä.~~

6.2 Erityiset turvatoimenpiteet

1. Tunnistuspalvelun on näytettävä tunnistusvälineen käyttäjälle tunnistustapahtumassa tieto, jonka perusteella käyttäjä voi yhdistää tunnistusvälineeseen saamansa vahvistuspyynnön asiointitapahtumaan (*session binding*). Tieto on näytettävä vain sellaisessa tunnistusmenetelmässä, jossa se on teknisesti mahdollista.

2. Tunnistuspalvelun on näytettävä tunnistusvälineen käyttäjälle tunnistustapahtumassa tieto luottavasta osapuolesta, jolle tunnistus välitetään. Tieto on näytettävä vain sellaisessa tunnistusmenetelmässä, jossa se on teknisesti mahdollista.

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 2 alakohdan mukaisten luottavien osapuolten tietojen näyttämisestä sekä kertakirjautumiseen liittyvien istuntojen keston, siirtämisen ja lopettamisen hallintaan perustuvista turvatoimenpiteistä.

6.3 Tunnistusvälineen kytkeminen henkilöön

1. Tunnistusmenetelmän todentamistekijät on kytkettävä tunnistusjärjestelmässä tunnistusvälineen haltijaan.

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

1. Tunnistus~~P~~palvelun tarjoajan on varmistettava, etteivät tunnistusvälineeseen liittyvät salaiset tiedot paljastu sen henkilöstölle missään tilanteessa.

2. Tunnistusp~~P~~alvelun tarjoaja ei saa kopioida tunnistusvälineeseen liittyviä salaisia tietoja.

Commented [LA2]: Ensimmäinen käsittely sidosryhmien kanssa 12.5.2021

Voi kaivata sanamuotojen parantamista. Ks. perusteluluonnos.

Commented [LA3]: Ensimmäinen käsittely sidosryhmien kanssa 12.5.2021

7 Tunnistusjärjestelmän ja rajapintojen salausvaatimukset

7.1 Tietoliikenteen salaus

1. Tunnistuspalveluntarjoajien välisten ja tunnistuspalveluntarjoajan ja luottavan osapuolen ~~asiointipalvelun~~ 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 ~~alla olevaan~~ äärellisen kunnan koon tulee olla vähintään 224 bittiä.

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

4) **Tiivistefunktiot:** Tiivistefunktion tai autentikaatiokoodin on oltava SHA-2, SHA-3, ~~tai~~ Whirlpool tai Poly1305. ~~SHA-2:lla tarkoitetaan funktioita SHA224, SHA256, SHA384 ja SHA512.~~

5) Edellä kohdissa 1-4 mainittujen lisäksi voidaan noudattaa menetelmiä ja arvoja, jotka on arvioitu turvallisiksi mainituissa kohdissa 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.

2. 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. ~~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 Tietoliikenteen osapuolten varmentaminen ~~turvavaatimukset tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa~~

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 eikä se voi perustua pelkästään osapuolen yleisesti luotettuun varmenteeseen.

8.2 Varmenteiden ja avainten uusiminen

Edellä kohdassa 8.1 tarkoitetut varmenteet ja avaimet on uusittava säännöllisesti joko:

a) 8.1 kohdan mukaisella menettelyllä,

b) allekirjoittamalla uudet avaimet 8.1 kohdan mukaisesti toimitetulla avaimella tai

c) toimittamalla uudet avaimet tietoliikenneyhteydellä, jonka eheys ja luottamuksellisuus on varmistettu sitomalla osapuolten tietoliikenne kohdan 8.1 mukaisesti toimitettuihin varmenteisiin tai avaimiin (*certificate pinning* tai *key pinning*).

~~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 Tunnistussanomien eheys ja luottamuksellisuus ~~Tietoturvavaatimukset asiointipalvelurajapinnassa~~

9.1 Sanomien suojaaminen tunnistuspalveluiden ja luottavan osapuolen välillä

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 kohdan 8 mukaisesti toimitettuihin varmenteisiin tai avaimiin (*certificate pinning tai key pinning*) tai

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

2. Tunnistusvälityspalvelun ja luottavan osapuolen välisessä tietoliikenteessä tunnistusanomat on todennettava allekirjoittamalla.

Commented [LA4]: Ensimmäinen käsittely sidosryhmien kanssa 12.5.2021

9.2 Sanomien suojaaminen käyttäjärajapinnassa

Jos tunnistussanomat välitetään käyttäjän selaimen tai päätelaitteen kautta, sanomat on salattava ja allekirjoitettava 9.1.b alakohdan mukaisesti.

9.3 Salausalgoritmit ja menettelyt

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

~~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 välisessä ~~n~~ rajapinnassa~~n~~ tulee täyttää 7 - 9 kohdissa ~~edellä 7 §:n 1 – 4 momentissa~~ määrätyt vaatimukset.

11 Tunnistuspalveluntarjoajan häiriöilmoitukset Liikenne- ja v~~V~~iestintävirastolle

11.1 Ilmoitettavat tiedot

Liikenne- ja v~~V~~iestintävirastolle 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.

11.2 Merkittävät häiriöt

Merkittäviä tunnistuspalvelun häiriöitä ovat tapahtumat, jotka ~~Häiriön merkittävyyden arvioinnissa merkittävyyttä lisää se, että häiriö~~ liittyvät~~y~~ sähköisen henkilöllisyyden virheellisyyteen tai väärinkäyttöön tai tietoturvauhkaan tai -häiriöön, joka vaarantaa tunnistamisen eheyden ja luotettavuuden. Merkittäviä ovat myös ennakoimattomat toimivuushäiriöt, joilla on vähäistä suurempia ~~yyttä lisää myös se, että häiriöllä on~~ haittavaikutuksia luottamusverkostoon.

Luku 3 Tietojen välittäminen luottamusverkostossa

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 sukunimi, henkilön etunimi ja organisaation yksilöivä tunniste; ~~sekä~~

3) tieto tunnistusvälineen korotetusta tai korkeasta varmuustasosta; sekä

~~3)~~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;

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

[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).

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

12.3 Tunnistuksen pseudonymisointi

Edellä 1 ja 2 kohdassa määrätyt velvoitteet koskevat tunnistusvälineen ja tunnistusvälityspalvelun välistä rajapintaa ja tunnistusvälineen käyttäjän todentamista siinäkin tapauksessa, että tunnistusvälityspalvelu ilmoittaa tunnistus- ja luottamuspalvelulain 8 §:n 2 momentissa tarkoitetulla tavalla luottavalle osapuolelle vain tunnistusvälineen käyttäjän salanimen tai rajoitetun määrän henkilötietoja.

Commented [LA5]: Ensimmäinen käsittely sidosryhmien kanssa 12.5.2021

13 Rajat ylittävän tunnistamisen edellyttämät tiedot

13.1 Tunnistautuminen suomalaisella tunnistusvälineellä

Tunnistauduttaessa suomalaisella tunnistusvälineellä ulkomaiseen asiointipalveluun tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on välitettävä samat tiedot kuin luottamusverkostossa on välitettävä 12 kohdan ~~§: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.

13.2 Tunnistautuminen ulkomaisella tunnistusvälineellä

Tunnistauduttaessa ulkomaisella notifioidulla 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

14.1 Tiedonsiirrossa käytettävä protokolla

Tunnistuspalvelun tarjoajan on osaltaan mahdollistettava ensitunnistamisen ketjuttaminen ja tunnistustapahtumien välitys luottamusverkostossa vähintään Open IDConnect- tai SAML -protokollan mukaisella rajapinnalla, joka täyttää 7-9 kohdissa ja 12 kohdassa määrätyt vaatimukset.

Commented [LA6]: Ensimmäinen käsittely sidosryhmien kanssa 12.5.2021

14.2 Rajapinnan muut ominaisuudet

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

Luku 4 Tunnistuspalvelun arviointikriteerit

[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).

15 Vaatimuksenmukaisuuden a~~A~~rviointikriteerit

15.1 Tunnistusjärjestelmän ja tunnistusmenetelmän arvioitavat toiminnot ~~[alakohdan nimi]~~

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
   ~~d)~~e) yhteentoimivuuteen luottamusverkostossa
2) tunnistusmenetelmään eli tunnistusvälineen
   a) hakemiseen ja rekisteröintiin
   b) hakijan henkilöllisyyden todistamiseen ja varmentamiseen
   c) tunnistamisen menetelmän ominaispiirteisiin ja laatimiseen
   d) myöntämiseen, toimittamiseen ja aktivointiin
   e) voimassaolon keskeyttämiseen, peruuttamiseen ja uudelleen aktivointiin
   f) uusimiseen ja korvaamiseen
   g) todentamismekanismeihin

15.2 Arviointikriteeristö

1. Edellä 1 kohdassa ~~momentissa~~ mainittujen toimintojen ~~osa-alueiden~~ vaatimuksenmukaisuuden ~~-~~arvioinnin on katettava kaikki ~~perustuttava~~ tunnistus- ja luottamuspalvelulain ja tämän määräyksen vaatimukset. ~~iin,~~

2. 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 ~~muiden vaatimusten täyttämisestä~~

~~16.1 [alakohdan nimi]~~

Tunnistuspalveluntarjoajan on osoitettava omalla kirjallisella selvityksellään tai edellä säännöksessä 15 ~~§:ssä~~ tarkoitetulla arvioinnilla seuraavien tunnistuspalveluntarjoajan

luotettavuuteen ja tunnistuspalvelusta annettaviin tietoihin liittyvien tunnistus- ja luottamuspalvelulaissa säädettyjen vaatimusten täyttyminen:

1) julkaistut ilmoitukset ja käyttäjätiedot, kuten tunnistusperiaatteet, sopimusehdot ja hinnastot
2) tunnistuspalvelusta vastaava vakiintunut oikeushenkilö ~~organisaatio~~
3) valmius ottaa vahinkoriskejä
4) riittävät taloudelliset varat
5) vastuu alihankkijoista
6) suunnitelma toiminnan päättämisen varalta

17 Kansallisen solmupisteen arviointiperusteet

17.1 [alakohdan nimi]

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 [alakohdan nimi]~~

1. 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.

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

[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

19 Tunnistuspalvelun sisäisen tarkastuslaitoksen vaatimukset

~~**19.1 [alakohdan nimi]**~~

1. 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.

2. 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

20.1 [alakohdan nimi]

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

21.1 [alakohdan nimi]

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

22.1 [alakohdan nimi]

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

23.1 [alakohdan nimi]

Käyttäjän hallussa fyysisesti olevan sirupohjaisen sähköisen allekirjoituksen tai leiman luontivälineen vaatimuksista säädetään EU:n komission täytäntöönpanopäätöksessä (EU) 2016/650[6].

24 Sertifiointilaitosta koskevat vaatimukset

24.1 [alakohdan nimi]

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.

[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

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 X

25.1 [alakohdan nimi]

26 Voimaantulo ja/tai siirtymäaika

[Voimaantuloaika merkitään määräyksen alussa ylätunnisteessa oleviin ”metatietoihin”, mutta se voidaan haluttaessa sisällyttää myös omaksi kohdakseen määräyksen loppuun. Siirtymäsäännökset / siirtymäaika voidaan haluttaessa sisällyttää samaan kohtaan tai erottaa omiksi kohdikseen.]

Helsingissä (pv) päivänä (kk)kuuta 20(vv)

Ratkaisija

Esittelijä