|  |  |  |
| --- | --- | --- |
| Antopäivä:x.x.2022 | Voimaantulopäivä:x.x.2022 | Voimassa: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 3

2 Tarkoitus 3

3 Määritelmät 4

**Luku 2 Tunnistuspalvelun tietoturvavaatimukset**

4 Tunnistuspalvelun tarjoajan tietoturvallisuuden hallintajärjestelmä 4

4.1 Tietoturvallisuuden hallinnan standardi 4

4.2 Tietoturvallisuuden hallinnan kattavuus 4

5 Tunnistusjärjestelmän tietoturvavaatimukset 4

5.1 Tunnistusjärjestelmän suojautumiskyky 4

5.2 Tietoliikenneturvallisuus 5

5.3 Tietojärjestelmäturvallisuus 5

5.4 Käyttöturvallisuus 5

5.5 Tunnistusjärjestelmän tuotantoverkon hallinta- ja etäyhteydet 6

6 Tunnistusmenetelmän tietoturvavaatimukset 6

6.1 Tunnistusmenetelmän ominaispiirteet ja suojautumiskyky 6

6.2 Erityiset turvatoimenpiteet 6

6.3 Tunnistusvälineen kytkeminen henkilöön 7

6.4 Tunnistusmenetelmän haltijakohtaisten tietojen käsittely 7

7 Tunnistusjärjestelmän rajapintojen salausvaatimukset 7

7.1 Tietoliikenteen salausmenetelmät 7

7.2 Tietoliikenteen salausprotokolla 8

8 Tietoliikenteen osapuolten varmentaminen 8

8.1 Tietoliikenneyhteyden osapuolten tunnistaminen 8

8.2 Varmenteiden ja avainten uusiminen 8

9 Tunnistussanomien eheys ja luottamuksellisuus 9

9.1 Sanomien suojaaminen tunnistuspalveluiden ja luottavan osapuolen välillä 9

9.2 Sanomien suojaaminen käyttäjärajapinnassa 9

9.3 Salausalgoritmit ja menettelyt 9

10 Tietoturvavaatimukset kansallisen solmupisteen rajapinnassa 9

11 Tunnistuspalveluntarjoajan häiriöilmoitukset Liikenne- ja viestintävirastolle 9

11.1 Merkittävät uhkat tai häiriöt 9

11.2 Ilmoitettavat tiedot 10

11.3 Ilmoitusmenettely 10

**Luku 3 Tunnistuspalveluiden yhteentoimivuus**

12 Luottamusverkostossa välitettävät vähimmäistiedot 10

12.1 Pakolliset tiedot 10

12.2 Valinnaiset tiedot 10

12.3 Tunnistuksen pseudonymisointi 11

13 Rajat ylittävän tunnistamisen edellyttämät tiedot 11

14 Tiedonsiirrossa käytettävä protokolla ja muut vaatimukset 12

14.1 Tiedonsiirrossa käytettävä protokolla 12

14.2 Rajapinnan muut ominaisuudet 12

**Luku 4 Tunnistuspalvelun arviointikriteerit**

15 Vaatimuksenmukaisuuden arviointikriteerit 12

15.1 Tunnistusjärjestelmän ja tunnistusmenetelmän arvioitavat toiminnot 12

15.2 Arviointikriteeristö 12

16 Selvitys tunnistuspalvelun tarjoajan ja julkaistujen tietojen luotettavuudesta 13

17 Kansallisen solmupisteen arviointiperusteet 13

**Luku 5 Tunnistuspalvelun arviointielimen pätevyys**

18 Tunnistuspalvelun ulkoisen arviointielimen vaatimukset 13

18.1 Osoittamismenettelyt 13

18.2 Pätevyys 14

19 Tunnistuspalvelun sisäisen tarkastuslaitoksen vaatimukset 14

19.1 Riippumattomuus 14

19.2 Pätevyys 14

**Luku 6 Hyväksytyt luottamuspalvelut**

20 Hyväksytyn luottamuspalvelun tarjoajan arviointikriteerit 14

20.1 Standardit 14

20.2 Standardien vapaaehtoisuus 15

21 Hyväksytyn luottamuspalvelun arviointikriteerit 15

21.1 Standardit 15

21.2 Standardien vapaaehtoisuus 15

**Luku 7 Luottamuspalvelujen vaatimustenmukaisuuden arviointilaitos**

22 Arviointilaitosten pätevyyden arviointi 15

22.1 Arviointilaitoksen toiminta 15

22.2 Pätevyys 15

**Luku 8 Hyväksytyn sähköisen allekirjoituksen tai leiman luontivälineen sertifiointilaitos**

23 Sähköisen allekirjoituksen tai leiman luontivälineen sertifiointilaitos 16

**Luku 9 Siirtymäsäännökset ja allekirjoitukset**

24 Voimaantulo ja siirtymäsäännökset 16

**LUKU 1 Yleiset säännökset**

# 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.

# 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.

# 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**

# Tunnistuspalvelun tarjoajan tietoturvallisuuden hallintajärjestelmä

## 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.

## 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.

# Tunnistusjärjestelmän tietoturvavaatimukset

## 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 osapuolisten välisten tietoliikenneyhteyksin 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.

## Tietoliikenneturvallisuus

Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä

1. verkon rakenteellinen turvallisuus,
2. tietoliikenneverkon vyöhykkeistäminen,
3. suodatussäännöt vähimpien oikeuksien periaatteilla,
4. suodatuksen ja valvontajärjestelmien hallinnointi,
5. turvalliset hallintayhteydet; sekä
6. käytettävä kansainvälisesti tai kansallisesti suositeltuja salausratkaisuja.

## Tietojärjestelmäturvallisuus

Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä

1. pääsyoikeuksien hallinta vähimpien oikeuksien periaatteella,
2. järjestelmien käyttäjien yksilöity tunnistaminen,
3. järjestelmien koventaminen,
4. haittaohjelmasuojaus,
5. turvallisuuteen liittyvien tapahtumien jäljityskyky ja jäljitysprosessi,
6. poikkeamien havainnointikyky ja korjausprosessi; sekä
7. käytettävä kansainvälisesti tai kansallisesti suositeltuja salausratkaisuja.

##  Käyttöturvallisuus

Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä

1. huolellinen muutosten hallinta,
2. tiedon luokitteluun perustuva salassa pidettävän aineiston käsittely-ympäristö ja säilytys,
3. etäkäytön ja -hallinnan suojaaminen etäkäyttöympäristön uhkilta,
4. ohjelmistokehityksen ja ohjelmistohaavoittuvuuksien hallinta,
5. varmuuskopiointi; sekä
6. käytettävä kansainvälisesti tai kansallisesti suositeltuja salausratkaisuja.

##  Tunnistusjärjestelmän tuotantoverkon hallinta- ja etäyhteydet

Tuotantoverkko ja sen edellä 5.2 e) 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

1. korotetulla varmuustasolla erityisesti arvioitu ja minimoitu ja
2. korkealla varmuustasolla kokonaisuutena arvioiden estetty.

# Tunnistusmenetelmän tietoturvavaatimukset

## 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.

## Erityiset turvatoimenpiteet

6.2.1

Tunnistuspalvelun on näytettävä tunnistusvälineen käyttäjälle tunnistustapahtumassa tieto, jonka perusteella käyttäjä voi yhdistää tunnistusvälineeseen saamansa vahvistuspyynnön 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.

## 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.

## 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.

# Tunnistusjärjestelmän rajapintojen salausvaatimukset

## Tietoliikenteen salausmenetelmät

7.1.1

Tunnistuspalveluntarjoajien välisten ja tunnistuspalveluntarjoajan 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:

* 1. Liikenne- ja viestintävirastossa toimivan salaustuotteiden hyväksyntäviranomaisen *(Crypto Approval Authority)* ohje Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset turvallisuusluokat (Dnro 190/651/2015), tai
	2. 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 Shceme Agreed Cryptographic Mechanisms.

7.1.3

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

## Tietoliikenteen salausprotokolla

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

# Tietoliikenteen osapuolten varmentaminen

## 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.

## Varmenteiden ja avainten uusiminen

Edellä kohdassa 8.1 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 kohdan 8.1 mukaisesti toimitettuihin varmenteisiin tai avaimiin, tai

c) allekirjoittamalla uudet avaimet 8.1 kohdan mukaisesti toimitetulla avaimella.

# Tunnistussanomien eheys ja luottamuksellisuus

## 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 kohdan 8 mukaisesti toimitettuihin varmenteisiin tai avaimiin, tai

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

9.1.2

Tunnistusvälityspalvelun ja luottavan osapuolen välisessä tietoliikenteessä tunnistussanomat on todennettava allekirjoittamalla.

## Sanomien suojaaminen käyttäjärajapinnassa

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

## Salausalgoritmit ja menettelyt

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

# Tietoturvavaatimukset kansallisen solmupisteen rajapinnassa

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

# Tunnistuspalveluntarjoajan häiriöilmoitukset Liikenne- ja viestintävirastolle

## 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.

## 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.

## 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**

# Luottamusverkostossa välitettävät vähimmäistiedot

## 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;
3. tieto tunnistusvälineen korotetusta tai korkeasta varmuustasosta; sekä
4. tunnistusvälityspalvelun varmistama tieto luottavasta osapuolesta.

## 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
4. nykyinen osoite;
5. arvonlisäverotunniste;
6. verorekisterinumero;
7. Euroopan parlamentin ja neuvoston direktiivin 2009/101/EY[[1]](#footnote-1) 3 artiklan 1 kohdassa tarkoitettu tunniste;
8. komission täytäntöönpanoasetuksessa (EU) N:o 1247/2012[[2]](#footnote-2) tarkoitettu oikeushenkilötunnus (LEI);
9. komission täytäntöönpanoasetuksessa (EU) N:o 1352/2013[[3]](#footnote-3) tarkoitettu taloudellisen toimijan rekisteröinti- ja tunnistenumero (EORI-numero); sekä
10. neuvoston asetuksen N:o 389/2012[[4]](#footnote-4) 2 artiklan 12 kohdassa tarkoitettu valmisteveronumero.

## 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.

# 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.

# Tiedonsiirrossa käytettävä protokolla ja muut vaatimukset

## Tiedonsiirrossa käytettävä protokolla

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

## 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**

# Vaatimuksenmukaisuuden arviointikriteerit

## 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)
	1. tietoturvallisuuden hallintaan
	2. tietojen säilyttämiseen ja käsittelyyn
	3. tiloihin ja henkilökuntaan
	4. teknisiin toimenpiteisiin
	5. yhteentoimivuuteen luottamusverkostossa
2. tunnistusmenetelmään eli tunnistusvälineen
	1. hakemiseen ja rekisteröintiin
	2. hakijan henkilöllisyyden todistamiseen ja varmentamiseen
	3. tunnistusmenetelmän ominaispiirteisiin ja laatimiseen
	4. myöntämiseen, toimittamiseen ja aktivointiin
	5. voimassaolon keskeyttämiseen, peruuttamiseen ja uudelleen aktivointiin
	6. uusimiseen ja korvaamiseen
	7. todentamismekanismeihin

## 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.

# Selvitys tunnistuspalvelun tarjoajan ja julkaistujen tietojen luotettavuudesta

Tunnistuspalveluntarjoajan on tunnistus- ja luottamuspalvelulain 10 §:n mukaisessa ilmoituksessa osoitettava omalla kirjallisella selvityksellään tai riippumattomalla ja pätevällä selvityksellä tai arvioinnilla seuraavien tunnistuspalveluntarjoajan 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.

# Kansallisen solmupisteen arviointiperusteet

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

**Luku 5 Tunnistuspalvelun arviointielimen pätevyys**

# Tunnistuspalvelun ulkoisen arviointielimen vaatimukset

## 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.

## 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.

# Tunnistuspalvelun sisäisen tarkastuslaitoksen vaatimukset

## 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.

## 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**

# Hyväksytyn luottamuspalvelun tarjoajan arviointikriteerit

## 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 standardin 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.

## Standardien vapaaehtoisuus

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

# Hyväksytyn luottamuspalvelun arviointikriteerit

## 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.

## Standardien vapaaehtoisuus

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

**Luku 7 Luottamuspalvelujen vaatimustenmukaisuuden arviointilaitos**

# Arviointilaitosten pätevyyden arviointi

## 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.

## 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**

# Sähköisen allekirjoituksen tai leiman luontivälineen sertifiointilaitos

Tunnistus- ja luottamuspalvelulain 36 § vaatimusten täyttymisen edellytyksenä on riittävä pätevyys ja resurssit eIDAS-asetuksessa ja komission täytäntöönpanopäätöksessä (EU) 2016/650[[6]](#footnote-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**

# Voimaantulo ja siirtymäsäännökset

24.1

Määräys tulee voimaan x.4.2022

24.2

Määräyksen kohdan 6.2.1 vaatimus on toteutettava viimeistään x.10.2022.

Määräyksen kohdan 6.2.2 ja 12.1 4) alakohdan vaatimukset on toteutettava viimeistään x.10.2022.

24.3

Määräyksen kohdan 8.1 vaatimus osapuolten tunnistamisesta on toteutettava

* 1. tunnistuspalveluiden välillä viimeistään x.10.2022,
	2. tunnistusvälityspalveluiden ja uusien luottavien osapuolten välillä viimeistään x.10.2022 ja
	3. tunnistusvälityspalveluiden ja sellaisten luottavien osapuolten välillä, joiden kanssa on tehty sopimus ennen x.10.2022, viimeistään x.4.2023

Määräyksen kohdan 8.2 vaatimus avainten ja varmenteiden päivittämisestä on otettava käyttöön viimeistään x.4.2023.

24.4

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

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

#

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

*Ratkaisija*

*Esittelijä*

**16.12.2021**

**Tietosuojavaltuutetun lausunto**

Liikenne- ja viestintävirasto Traficom on pyytänyt tietosuojavaltuutetun toimistolta lausuntoa tunnistus- ja luottamuspalvelumääräyksen luonnoksesta ja perustelumuistiosta. Tietosuojavaltuutetun toimisto kiittää tästä mahdollisuudesta.

Määräyksellä sähköisistä tunnistus- ja luottamuspalveluista (M72 B/2022) tehdään tarkennuksia lainsäädännön vaatimuksiin tunnistuspalveluiden tietoturvaa ja yhteensopivuutta koskien. Tietosuojavaltuutettu on arvioinut perustelu-muistion kohtia 1.3.3 (Henkilötiedot), 4.3.2 (Tunnistuslain ja eIDAS-asetusten määritelmät) sekä 4.6.6 (PSD2-sääntelyn yhteensopivuus). Tietosuojavaltuutettu on myös tarkastellut määräysluonnoksen 6.1.1 ja 11.3 säännöksiä.

Tietosuojavaltuutetun käsityksen mukaan aikaisempien määräyksien sisältämien mahdollisten epäselvyyksien ja aukkojen tarkentaminen on tärkeää ja tarpeellista. Tietosuojavaltuutettu pitää kannatettavina muutoksia, jotka parantavat palveluiden tietosuojan tasoa sekä käsittelyn turvallisuutta. Tunnistusjärjestelmissä ja tunnistuspalveluissa käsiteltävät henkilötiedot sekä ylipäänsä tunnistamiseen liittyvä yksityisyydensuojan tarve ovat luonteeltaan sellaisia, että on hyvin tärkeää, että tietojen ja niiden käsittelyn eheys, luottamuksellisuus ja turvallisuus on varmistettu korkeatasoisesti. Tietosuojavaltuutettu katsoo, että tietoturvallisuuden hallintaa koskevien vaatimusten täsmentäminen on tietosuojanäkökulmasta positiivinen kehityssuunta.

Suhteessa PSD2-sääntelyyn olennaista on se, että sääntelyt eivät ole keskenään ristiriidassa, kuten määräyksessä on katsottu. Kumman tahansa sääntelyn kautta tulevat täydentävät vaatimukset suhteessa toiseen sääntelyyn ovat palveluiden tietosuojan kannalta positiivinen asia.

Säännöksen 6.1.1 uusi vaatimus tehdä tunnistusmenetelmästä ”erityinen riskiarvio, jossa arvioidaan erikseen eri todentamistekijöihin ja todentamismekanismiin liittyvät uhkat ja niiltä suojaavat turvatoimenpiteet” herättää pohtimaan vaatimuksen suhdetta tietosuoja-asetuksen 35 artiklan vaatimukseen tehdä tietosuojaa koskeva vaikutustenarviointi. Tunnistuspalveluihin saattaa liittyä esimerkiksi kasvojen- ja sormenjälkitunnistusta ym. biometristen tietojen käsittelyä. On siis tärkeää, että toimijat arvioivat henkilötietojen käsittelyn riskejä myös tietosuoja-asetuksen 35 artiklan mukaisen vaikutustenarvioinnin tarpeen näkökulmasta.

Säännös 11.3 sisältää tarkennuksia merkittäviä uhkia ja häiriöitä koskevaan ilmoitusmenettelyyn. Tunnistuspalveluntarjoajan on ilmoitettava palvelun merkittävästä häiriöstä tai uhkasta Traficomille. Säännös herättää pohtimaan ilmoitusmenettelyn suhdetta tietosuoja-asetuksen tietoturvaloukkauksen ilmoittamista koskeviin 33-34 artikloihin. Toimijoiden on tärkeää tunnistaa, että osa tunnistusjärjestelmien ja tunnistuspalveluiden häiriötilanteista saattaa täyttää myös tietosuoja-asetuksen mukaisen henkilötietojen tietoturvaloukkauksen määritelmän.

Tietosuojavaltuutettu Anu Talus

Ylitarkastaja Meeri Blomberg

**10.12.2021**

**Digi- ja väestötietovirasto**

Digi- ja väestötietovirasto (DVV) antaa pyynnöstä lausuntonsa Liikenne- ja viestintävirasto Traficomille tunnistus- ja luottamuspalvelumääräyksen 72 luonnoksesta ja perustelumuistiosta ja lausuu ehdotuksesta seuraavasti.

Yleisellä tasolla määräys sisältää hyviä tarkennuksia ja tärkeitä päivityksiä mm. käytettyihin algoritmeihin. Myös terminologiaa on tarkennettu ja pidämme hyvänä erityisesti muutosta, jossa ”asiointipalvelu” on korvattu termillä ”luottava osapuoli”, joka on linjassa eIDAS-asetuksen 3 artiklan määritelmän kanssa.

Kommentit säännöksestä 6 Tunnistusmenetelmän tietoturvavaatimukset

Kohdan 6.2.2. vaatimus luottavan osapuolen nimen näyttämisen pakollisuudesta on merkittävä parannus aiempaan.

Kommentit säännöksestä 8 Tietoliikenteen osapuolten varmentaminen

eIDAS-asetuksen mukaisen hyväksytyn sähköisen allekirjoituksen ja leiman huomioiminen on hyvä kehityssuunta. Perustelumuistion mukaan verkkosivujen todentamisen hyväksytyt varmenteet (ns. QWAC-varmenteet) eivät ole riittävä todentamisen tapa. Perusteluissa viitataan siihen, että linjaus tässä poikkeaa PSD2-sääntelystä, koska ”Lisävaatimuksena PSD2-sääntelyssä kuitenkin on, että kyseiset TPP-toimijat ovat finanssisektorin valvontaviranomaisen valvonnassa ja löytyvät viranomaisen rekisteristä”. Huomautamme, että tunnistuspalveluiden tarjoajat ovat finanssisektorin tapaan viranomaisen valvonnassa ja hyväksyttyjä verkkosivun todentamisen varmenteita myöntävät tahot ovat omalta osaltaan viranomaisen valvonnassa. Hyväksytyn tason varmenteiden myöntöprosessissa määritetään erittäin yksityiskohtaisesti, kuinka varmenteen hakija tulee tunnistaa varmenteen myöntämiseksi. Suoraa kahdenvälistä menettelyä pidetään riittävänä ja rinnasteisena hyväksyttyyn sähköiseen allekirjoitukseen ja leimaan, mutta tähän menettelyyn taas ei kohdisteta mitään tarkkoja vaatimuksia eikä kuvata menettelytapoja. Tämän pohjalta on epäselvää, kuinka suora kahdenvälinen menettely parantaa turvallisuutta verkkosivujen todentamiseen tarkoitettuihin hyväksyttyihin varmenteisiin verrattuna.

Perusteluissa myös todetaan: ”Virasto katsoo, että muutoin varmenne ei sinänsä osoita, että sen varmentama avainpari on oikealla haltijalla. Varmenteen haltijan avaintenhallinnan käytännöt eivät sisälly varmenteen myöntämisen vaatimuksiin.”

Edellinen perustelu kyseenalaistaa tyypistä riippumatta varmenteiden myöntöprosessit ja laajemminkin varmenteisiin tai ei-auditoiduissa ympäristöissä sijaitseviin avaimiin nojaavan turvallisuuden. Perustelu myös jättää epäselväksi, kuinka kahdenvälinen menettely parantaa tilannetta koskien avaimen haltijan avaintenhallintakäytäntöjä?

Kommentit muista säännöksistä luvussa 2 Tunnistuspalvelun tietoturvavaatimukset

Tietoliikenteen salausmenetelmiin luvussa 7.1.1. tehdyt päivitykset ovat hyviä ja tarpeellisia.

Kohdassa 5.5. ei ole riittävällä tarkkuudella määritelty tuotantoverkkoa. Määritys jättää epäselväksi, ovatko esimerkiksi asiakastietojärjestelmien käyttöön tarkoitetut työasemat osa tuotantoverkkoa vai viittaako tuotantoverkko vain tunnistusvälineen käytön yhteydessä aktiivisiin komponentteihin ja niiden hallintatyöasemiin. Jälkimmäisten tapauksessa DVV pitää vaatimuksia oikein mitoitettuna, mutta asiakastietojärjestelmien osalta korkealla tasolla ylimitoitettuina.

Kommentit luvusta 3 Tunnistuspalveluiden yhteentoimivuus

Ei lausuttavaa.

Kommentit luvusta 4 Tunnistuspalvelun arviointikriteerit

Ei lausuttavaa.

Kommentit luvusta 6 Hyväksytyt luottamuspalvelut

Ei lausuttavaa.

Kommentit siirtymäajoista, säännös 24

DVV:n osalta siirtymäajat ovat riittävät.

Kommentit muista säännöksistä (joihin ei esitetä muutoksia)

Ei lausuttavaa.

Pitkänen Mikko

Digi- ja väestötietovirasto - Digitalisaation tukipalvelut ja yhteentoimivuus -yksikkö

**10.12.2021**

**Finanssiala ry**

Kiitoksia lausuntopyynnöstä. Yleisesti ottaen määräyksen päivitys lienee paikallaan. Aiemman määräysversion puutteista on käyty paljon keskusteluita eri työryhmissä ja työpajoissa. Kuten alla olevista kommenteista käy ilmi, kaikkia huolia ei tosin olla ymmärretty tai ei olla huomioitu.

Uusi määräys tuo myös uusia kustannuksia, joita on hintasäännellyssä markkinassa vaikeata tai jopa mahdotonta kattaa tunnistuspalveluiden tulovirroilla.

Kommentit säännöksestä 6 Tunnistusmenetelmän tietoturvavaatimukset

Vaatimus riskinarviosta tulee lisäämään tunnistuspalvelun tarjoamisessa vaadittavan työn määrää ja kustannuksia. Uuden sääntelyn myötä tulee aiemmin käytössä ollut riskinarviokehikko sijoittaa uusien vaatimuksien mukaiseen kehikkoon. Kuten säädöksen perustelumuistiossakin on todettu aiemmin keskustellun, voidaan pitää hyvänä, että lisääntyneet vaatimukset tulevat tasapuolisesti, samanaikaisesti ja samalla tavalla kaikkia verkoston osapuolia velvoittavaksi. Riskinarvio tarjoaa työvälineitä verkoston toimijoille arvioida omaa toimintaansa ja antaa viranomaisille tukea valvontaan. Riskinarviokehikon ollessa uudistuksessa säädellyllä tavalla avoin, vertailu toimijoiden välisten riskinarvioiden ja teknisten kontrollien välillä voi tosin olla auditoijalle ja viranomaisen valvonnalle haastavaa.

Ehdotamme määräyksen kohdan 6.2.1 muotoiluksi seuraavaa:

Tunnistuspalvelun on näytettävä tunnistusvälineen käyttäjälle tunnistustapahtumassa tieto, jonka perusteella käyttäjä voi varmistaa tunnistusvälineeseen saamansa vahvistuspyynnön liittyvän käyttäjän omaan asiointitapahtumaan. Tiedon näyttäminen on pakollista sellaisessa tunnistusmenetelmässä, jossa se on teknisesti mahdollista.

Määräyksen sanamuodon selventäminen on mielestämme tärkeää, jotta määräys kertoo olennaisen sisällön sekä tarkoituksen itsessään ilman perusteluteksteihin tutustumista. Katsomme että terminologiaa on muutettava, sillä tarkoitus on nimenomaan käyttäjän turvallisuuden lisäämisestä eikä tunnistamisen yhdistämisestä. Termi yhdistää viittaa liiaksi PSD2 -säädökseen.

Määräyksen kohdan 6.2.3. osalta olisi näkemyksemme mukaan hyvä määritellä istunnolle, jokin enimmäiskesto, jotta määräyksen kohdalla olisi merkitystä palveluita suunniteltaessa ja näin varmistetaan tunnistamisen turvallisuusvaatimuksia myös tältä osin.

Kommentit säännöksestä 8 Tietoliikenteen osapuolten varmentaminen

Yleisenä kommenttina liittyen avainten vaihtamiseen ja tietoliikenneyhteyksien varmentamiseen todetaan, että määräyksen uuden muotoilun osalta olisi hyvä selvittää tarkemmin määräyksen vaikutuksia asiointipalveluihin eli luottaviin osapuoliin. Todettakoon myös, että tällä hetkellä ei ole tarjolla sellaisia menetelmiä eikä käytäntöjä, joilla ehdotetun määräyksen vaatimukset voitaisiin täyttää ilman, että vahvan sähköisen tunnistamisen käyttäminen vaikeutuu tai jopa vaarantuu kokonaan. Näkemyksemme mukaan ennen määräyksen muuttamista näiltä osin tulisi sen vaikutukset erityisesti asiointipalveluille selvittää tarkemmin.

Luottamusverkostossa luottamus perustuu siihen, että avaimilla ja niihin liittyvillä varmenteilla todennetaan, että tietoliikenteen vastapuolet todella ovat niitä mitä ne väittävät olevansa. Tästä syystä on tärkeää ottaa huomioon, että ehdotettu kohta 8 sisältää todella mittavan muutoksen, koska yksikään Luottamusverkoston jäsen ei täytä tällä hetkellä ehdotetun määräyksen uusia vaatimuksia, asiointipalveluista puhumattakaan. Erityisen haasteen muodostaa se, että Suomessa ei ole toistaiseksi yhtäkään oikeushenkilöitä vahvasti tunnistavaa menetelmää eikä Luottamusverkostossa käytetyille protokollille ole vielä olemassa yleisesti hyväksyttyä vakiintunutta ratkaisumallia todennettuun avainten vaihtamiseen. Näin ollen ehdotettua muutosta ei tulisi tehdä näin lyhyellä aikataululla, vaan ehdotettua muutosta varten on ehdottoman tärkeää saada lisäaikaa ja muutoksen vaikutukset vahvan sähköisen tunnistamisen käyttämiseen asiointipalveluissa tulisi selvittää tarkasti.

Koska oikeushenkilöiden eli tässä tapauksessa Luottamusverkoston jäsenten tai asiointipalveluiden tunnistaminen vahvasti ei ole vielä Suomessa mahdollista, vaatisi tilapäinen ratkaisu käytännössä oikeushenkilön lukuun toimivien työntekijöiden tai alihankkijoiden työntekijöiden henkilökohtaista tunnistamista. Vielä ei ole olemassa aukotonta menetelmää todentaa onko avaintenvaihtoon osallistuva henkilö todella kyseisen toimijan valtuuttama. Sitomalla avainten vaihtoon pitkäikäinen päävarmenne tai edellisten avainten ketjutus, vaikeutettaisiin hyökkääjän tekeytymistä tunnistuspalvelun edustajaksi.

Avaimiin ja varmenteisiin liittyy pääasiassa kahden tyyppistä riskiä:

A. hyökkääjä varastaa käytössä olevan avaimen ja käyttää sitä sanomien allekirjoittamiseen tai salaukseen tekeytyessään oikeaksi palveluksi, ja

B. hyökkääjä luo uuden avaimen ja harhauttaa toisen palvelun luottamaan siihen oikean palvelun avaimena.

Määräysehdotus pyrkii torjumaan erityisesti vaihtoehdon B hyökkäyksiä asettamalla tiukemmat vaatimukset avainten vaihdolle. Arviomme mukaan kuitenkin, että vaihtoehto A saattaa olla hyökkääjälle houkuttelevampi keino etenkin sen vuoksi että vaihtoehto B herkästi rikkoo tunnistamisen vanhoilla avaimilla ja on siksi välittömästi havaittavissa. Sen sijaan esimerkiksi tunnistuspalvelun allekirjoitusavaimen varastaminen voi mahdollistaa sen, että hyökkääjä voi sillä allekirjoittaa väärennettyjä tunnistustapahtumia ja sitä kautta esimerkiksi tunnistautua väärällä identiteetillä julkishallinnon palveluihin ilman että kukaan välttämättä havaitsee mitään epäilyttävää. Riskejä avainten vuotoon syntyy esimerkiksi tietomurtojen tai poistuvien työntekijöiden kautta.

Perinteisesti Suomessa on ollut pankkialalla haasteita avainten vaihdossa. Perustelumuistiossa mainitaan Tupas-protokollan manuaalinen avaintenvaihto, mikä käytännössä tarkoitti salasanaa vastaavan jaetun salaisuuden toimittamista paperilla. Hyvin yleisesti Tupas-protokollaa käyttävät toimijat eivät vaihtaneet näitä avaimia koskaan, jolloin tietoturva oli hyvin kyseenalaisella tasolla. Periaatteellisella tasolla nykyiset standardit edellyttävät säännöllistä avaintenvaihtoa, mutta käytännössä Luottamusverkostossakaan kaikki toimijat eivät ole vielä vaihtaneet OIDC-protokollan sanomatasolla käytettäviä avaimia, eikä siihen ole kaikilla toimijoilla palvelukuvauksissa määriteltyä prosessia. Manuaalinen avaintenvaihtoprosessi on osoittautunut käytännössä työlääksi ja herkäksi virheille.

Kokemusten mukaan tiheä avaintenvaihto ja riittävä automaatio vähentävät oleellisesti sekä inhimillisten virheiden että hyökkäysten aiheuttamaa riskiä. Koska nykyiselläkään regulaatiolla kaikki toimijat eivät ole pystyneet vaihtamaan avaimia, tulisi avaintenvaihtoa pyrkiä nimenomaan sujuvoittamaan, vaikkakin toki tietoturvaa heikentämättä. Nykyään yleisesti luotettujen varmenteiden suurin sallittu ikä on yksi vuosi, joten TLS-varmenteet vaihdetaan nykyään pääasiassa vuosittain. Poikkeuksena ovat LetsEncryptin myöntämät varmenteet, jotka ovat voimassa vain kolme kuukautta kerrallaan. Moni luottava osapuoli käyttää viimeksi mainittuja. Huomautamme myös, että Letsencryptin varmenteita uusittaessa vaihdetaan myös niihin kytkeytyvä salainen avain, mikä tekee TLS-varmenteiden sitomisesta (certificate pinning) äärimmäisen työlästä ja häiriöaltista.

On hyvä huomata, että jo voimassa oleva määräys M72 edellytti perustellusti DHE-avaintenvaihtoa Luottamusverkostossa. Käytännössä tämä tarkoittaa, että TLS-yhteyksien sisällä siirrettävä data salataan tilapäisillä lyhytikäisillä avaimilla eikä useita vuosia voimassa olleilla sivustojen varmenteiden avaimilla, kuten aiemmin oli laajalti käytäntönä. Pyrkimällä minimoimaan sanomien allekirjoittamisessa ja salaamisessa käytettävien avainten elinkaarta kyetään oleellisesti leikkaamaan ajallisesti sitä riskiä mikä syntyy, mikäli ne vuotavat vääriin käsiin. Kannustamme viranomaista rohkaisemaan markkinoita entistä lyhytikäisempien avainten käyttöön, jotta avainten mahdollisista vuotamisista syntyviä riskejä voitaisiin minimoida.

Kohta 8.1 on monitulkintainen sen suhteen, että mihin kaikkiin avaimiin viitataan. Jos sanomatasolla viestit suojataan, TLS-varmenteen sitominen tämän kohdan mukaisiin avaimiin ei tuo lisäsuojaa ja 3-12 kuukauden välein tapahtuva manuaalinen prosessi olisi vain omiaan aiheuttamaan suuren määrän häiriötilanteita. Ehdotamme, että kohtaa tarkennetaan niin että jos käytössä on kohdan 8.1 mukaiset avaimet sanomatason salauksessa, niin TLS-varmenteiden suhteen riittäisi yleisesti hyväksytty varmenne. Lisäksi kohdassa 8.1 on monitulkintaista mitä tarkoitetaan avainten haltijoilla. Toivomme asiasta tarkennusta ensisijaisesti määräystekstiin tai toissijaisesti perustelumuistoon. Selkein merkitys haltijalle olisi se taho mikä on tehnyt sopimuksen tunnistamisesta, eli esimerkiksi Luottamusverkoston jäsen tai luottavaa osapuolta operoiva yritys, tai näiden lukuun toimiva alihankkija tai yksittäinen vastuuhenkilö. Toivomme että haltijan merkitystä ei ainakaan laajennettaisi siihen, että täytyisi tunnistaa kaikki ne henkilöt, jotka esimerkiksi palvelua operoivan tahon työntekijöinä voivat päästä käsittelemään avainta jossain sen elinkaaren vaiheessa.

Avainten vaihtoon, hallintaan ja elinkaareen on kehitteillä useita erilaisia ratkaisuja, esimerkiksi erilaiset lohkoketjuratkaisut tai SSI-menetelmät. Toivomme että tällaisia kehittyviä ratkaisuja ei suljeta pois jo etukäteen ja siksi ehdotamme, että kohtaa 8.2 c muutetaan sallimaan avainten ketjutus esimerkiksi seuraavalla muotoilulla:

c) allekirjoittamalla uudet avaimet 8.1 kohdan mukaisesti toimitetuilla avaimilla tai niistä ketjutetuilla avaimilla.

Perustelumuistiossa ehdotetaan, että avaimet ja varmenteet tulisi vaihtaa vähintään kahden vuoden välein. Katsomme että vaihtoväli sanomien allekirjoittamisessa ja salauksessa käytettäville avaimille ei saisi olla ainakaan kahta vuotta pidempi. Ehdotamme kuitenkin, että perustelumuistiossa hyväksyttäisiin selvästi pidempi voimassaoloaika sellaisille avaimille, joita käytetään pelkästään muiden avainten allekirjoittamiseen eli varmenteiden luomiseen. Tyypillisesti Internetin juurivarmenteet ovat voimassa 10–20 vuotta, joskus enemmänkin. Esimerkiksi www.suomi.fi nojaa Amazonin juurivarmenteeseen, joka on luotu 2015 ja on voimassa 2038 saakka. Sallimalla perustelumuistiossa tällaiset pitkäikäiset juurivarmenteet, voitaisiin Luottamusverkoston toimijoiden avaintenvaihdon luottamusta vahvistaa ja hyökkäyksiä torjua tehokkaasti suojatulla pitkäikäisemmällä avaimella.

Määräysmuutoksen riskinä on, että manuaalityötä ja kankeaa viestintää prosesseissa joudutaan uudistuksen myötä lisäämään. Lisääntyvä manuaalityö ja Luottamusverkoston jäsenten sekä asiointipalveluiden välinen kankea viestintä ei paranna tunnistuspalvelun tai verkoston turvallisuutta kokonaisuutena. On todennäköistä, että asiointipalveluilla ei ole lähellekään samanlaisia teknisiä valmiuksia saatavilla, kuin Luottamusverkoston jäsenillä. Riskinä on, että kankeammaksi muuttuva prosessi johtaa kokonaisuutena arvioiden jopa aiempaa heikompaan avaintenhallintaan, etenkin asiointipalveluissa.

Kommentit muista säännöksistä luvussa 2 Tunnistuspalvelun tietoturvavaatimukset

Säädöksessä 4.1 on hyvin hienovarainen muutos turvallisuuden hallinnan standardin osalta, kun aiempi sanamuoto "käytettävä" muuttuu muotoon "noudatettava". Määräyksen perustelujen valossa muutos vaikuttaa kuitenkin kirjaimellista tekstimuutosta merkittävämmältä. Noudatettavaa standardia ei ole tarkkaan määritelty ja määrittelemättömyys jättää varaa toteutukselle. Kuitenkin, kuten tiedetään, tulkinnanvaraisuus asettaa haasteita vaatimuksenmukaisuuden ja etenkin toimijoiden välisen turvallisuuden tason yhdenmukaisuuden arvioinnissa ja vertailussa. Uudistuksen valossa jää auki kysymys, kuinka yhdenmukaisia käytänteitä toimijat noudattavat, kun määritys on tältä osin lavea. Toisaalta herää kysymys, onko jatkossa käytännön edellytys palvelun tarjoamiselle verkostossa tietoturvallisuuden hallintajärjestelmän sertifiointi.

Finanssiala on vahvasti säännelty ja valvottu. Nyt vahvan tunnistamisen verkostoon kuulumisen edellytykseksi vaikuttaa nousevan uusi edellytys organisaation tietoturvallisuuden hallintajärjestelmälle, jonka yhteensovittaminen toimijan nykyiseen kehikkoon aiheuttaa uusia lisäkustannuksia toiminnalle.

Kommentit luvusta 3 Tunnistuspalveluiden yhteentoimivuus

-

Kommentit luvusta 4 Tunnistuspalvelun arviointikriteerit

Tunnistuslain vaatimus palveluntarjoajien tärkeimpien yhteistyökumppanien tiedoista on toistettu määräyksen luvun 4 säädöksessä 16. Laissa käytetään termiä yhteistyökumppanit, määräyksessä käytetään termiä alihankkijat. Lain ja määräyksen terminologia ei tältä osin ole yhtenevää. Sen enempää lain esitöissä, kuin määräyksessä tai määräyksen perusteluissa ei tarkenneta minkä tasoista tietoa palvelutarjoajan yhteistyökumppaneista odotetaan.

Kommentit luvusta 6 Hyväksytyt luottamuspalvelut

-

Kommentit siirtymäajoista, säännös 24

FA toivoo pidempiä siirtymäaikoja. Määräys on tarkoitus saattaa voimaan huhtikuussa 2022 ja säännöksessä ehdotetaan x.10.2022 (6 kk) ja x.4.2023 (12 kk) siirtymäaikoja.

Toimijoilla ole mahdollisuutta etukäteen varautua ja käynnistää kehitystoimia ennen kuin määräyksen lopullinen muoto on varma ja on astunut voimaan. Tarvittavia resursseja ei löydy odottamassa varaston hyllyllä. Näin ollen pieniltäkin tuntuvissa järjestelmätöissä 6 kk siirtymäaika on liian lyhyt. Ehdotamme, että siirtymäajat olisivat vähintään 12 kk.

Yllä olevissa kommenteissa määräyksen kohdasta 8 (säännöksen 8 siirtymäajat) on todettu, että ”Näin ollen ehdotettua muutosta ei tulisi tehdä näin lyhyellä aikataululla, vaan ehdotettua muutosta varten on ehdottoman tärkeää saada lisäaikaa ja muutoksen vaikutukset vahvan sähköisen tunnistamisen käyttämiseen asiointipalveluissa tulisi selvittää tarkasti.” Tähän selvitykseen ehdotetut säännöksen 24.3 alakohtien 6 kk ja jopa 12 kk siirtymäajat ovat aivan liian lyhyitä aikoja.

FA toivoo myös viranomaiselta aktiivista informointia ja ohjeistamista verkostossa, jotta määräyksen uudistamisen uudet velvoitteet selkeästi ja johdonmukaisesti saadaan kaikkien verkoston osapuolien tietoon, ml. luottavat osapuolet/asiointipalvelut. Erityisen huolisamme olemme luottavien osapuolien/asiointipalvelujen kyvykkyydestä reagoida muuttuviin vaatimuksiin.

Kommentit muista säännöksistä (joihin ei esitetä muutoksia)

Työryhmissä ja työpajoissa on esitetty tarve johdetusti operoidulle testiverkostolle. Tätä voidaan pitää eräänä keskeisenä kehityskohteena tulevaisuutta ajatellen.

Jansson Peter

Finanssiala ry

**09.12.2021**

**Nixu Certification Oy**

Vahvan sähköisen tunnistuksen sääntely on kehittynyt noin viiden vuoden ja kolmen auditointikerran aikana. Määräysluonnos jatkaa tätä kehitystyötä, mutta haluamme korostaa, että erittäin merikiitävä osa määräyksen mukaisen toiminnan varmistamisesta tehdään tukemalla vahvan sähköisen tunnistamisen vaatimuksenmukaisuutta määräyksen päivittämisen välissä. Tulkinnat yksittäisistä kohdista, auditoinneissa käytetyn kriteeristön ylläpito ja muu tuki auditoinneille sekä yhteistyö alan toimijoiden kesken on ensiarvoisen tärkeää.

Kokonaisuutena on tapahtunut merkittävää paranemista M72-auditoinneissa näiden kolmen auditointikerran välillä. Traficom on hankkinut aisantuntemusta, joka pystyy tukemaan auditointeja (ei vain lakikysymyksiä ja tietoteknisiä asioita). Myös auditointikriteeristö, raportoinnin työvälineet ja muut asiat ovat huomattavasti paremmalla tolalla kuin vesin M72 aikana.

Pidämme tärkeänä, että auditointien tekemistä kehitetään jatkossakin jo aloitetulla tavalla. Kehittämisessä on hyödynnetty auditointeja tekeviä yrityksiä, ja tämän toivomme jatkuvan.

Auditointien tulosten hyväksyntä on aiemmin kestänyt luvattoman pitkään. Vanhaan asiaan palaaminen on hankalaa kahden vuoden tauon jälkeen. Traficom voisi harkita ratkaisua, jossa auditoinnin korjausten onnistuminen todennetaan väliauditoinnilla, joka tehdään. Vuoden kuluessa varsinaisen auditoinnin päättymisestä.

Kommentit säännöksestä 6 Tunnistusmenetelmän tietoturvavaatimukset

Säännöksessä esitetään uusia tunnistuspalvelulta vaadittavia asioita, joita pidämme hyvinä. 6.1.1.1 Vaatii asioita, joiden on ilmettävä kohdan 6.1.1.2 riskiarvioista. Myös säännös 5.1.1 edellyttää arvioita.

Määräyksessä on salausratkaisua useissa säännöksissä. Osin viitataan 7§, osin “Suositeltuihin salausratkaisuihin”, joista jälkimmäinen on selvästi lievempi. Viraston on syytä olla tarkkana sanamuodoissa, jottei synny tilannetta, jossa 7§ heikompi salaus sallittaisiin säännöksen sanamuodon takia.

Säännös 6.2.1 on hyvä kiristys nykyiseen määräykseen ja vaatimus on annettu tehdyissä auditoinneissa suosituksena usean vuoden ajan. Ehdotettu sanamuoto on melko lievä, ja tapahtuman ja tunnistuksen välisen yksilöintivaatimusta voisi harkita kovennettavan niin, että yksilöintitiedon väärentäminen tai arvaaminen olisi erittäin vaikeaa. Ehdotetun sanamuodon täyttää luku 12, mutta se on paitsi arvattavissa myös väärennettävissä helposti. Pidempi luku tai visuaalinen elementti eivät olisi pakollisia ehdotetulla sanamuodolla.

Kommentit säännöksestä 8 Tietoliikenteen osapuolten varmentaminen

Ehdotettu säännös on hyvä: Avaintenhallinnan heikkoudet saattavat murentaa luottamuksen koko tunnistuspalveluun yhdellä kertaa. On huomattava, että vaatimuksen auditointi lisää hieman auditointien kokoa nykyisestä.

Kommentit muista säännöksistä luvussa 2 Tunnistuspalvelun tietoturvavaatimukset

Luvussa 2 esitetään muutoksia, joita jo tavanomaisesti auditoidaan, mutta joiden arviointi ei tiukasti tulkiten olisi pakollista. Toistaiseksi kukaan ei ole kiistänyt näiden kohtien sisällyttämistä mukana. Esimerkiksi 5.4 d tulisi kattamaan ohjelmistokehityksen. Ehdotettu muutos on hyvä, ja vie kohdat pois auditointien “harmaalta alueelta”.

Eräät esitetyt lisäykset ovat mielestämme tarpeettomia, ja kääntyvät itseään vastaa. Määräyksen mukaisessa toiminnassa ja toiminnan Auditoinnissa oletetaan, että asioita on tehtävä “hyvin” tai “huolellisesti”. Näiden sanojen lisääminen joihinkin kohtiin antaa ymmärtää, että muissa kohdissa huono tai huilimaton tekeminen kävisi. Kun muutosten hallinnan edellytetään olevan huolellista, riittääkö varmuuskopioinneissa huolimaton tekeminen, koska huolellisuusvelvoitetta ei ole esitetty kohdassa 5.4 e? Ehdotamme, että kaikkine vaatimusten täyttämisessä edellytetään huolellisuutta ja hyvää tapaa tehdä asioita, ei vain niissä, joissa se on mainittu.

Säännös 4.1 tiukentaa ISO 27001:n tai muun standardin noudattamisen velvoitetta. Nyt ei riitä niiden pelkkä käyttäminen tietoturvan johtamisessa, vaan niitä on noudatettava standardin pakollisilta osilta. Vaatimus on mielestämme hyvä ja perusteltu, mutta se lisää auditointien työmäärää. Vaatimuksen osoittamisen pitkällä aikavälillä helpoin tapa on sertifiointi, mikä useilla alan toimijoilla jo onkin. Uusien toimijoiden osalta vaatimus nostaa alalle tulon kynnystä, vaikka tämä ei ole mielestämme kovin merkittävää.

Sallittujen salausalgoritmien kirjoittaminen (”kovakoodaaminen”) suoraan määräykseen on mielestämme outo ratkaisu, mutta saamamme tiedon mukana tähän on hyvät juridiset perusteet. Nämä eivät estäneet kiusallista tilannetta vuonna 2019, jolloin ChaCha20-Poly1305 -salaus oli yleisesti vahvana pidetty, mutta joka ei ollut 7§ lueteltujen joukossa, ja näin ollen laiton vahvassa tunnistuksessa. Turvallinen mutta laiton kombinaatio siis toteutui, mutta onneksi ei laillinen, mutta turvaton

Ehdotettu muutos, jossa kryptoviranomaisten ylläpitämille listoille tulee asema vahvassa sähköisessä tunnistuksessa on mielestämme hyvä, ellei peräti välttämätön. Säännös hallitsee tilanteen, jossa turvallisten salausten listalle ilmestyy uusi, mutta ei tilannetta, jossa 7§1:ssa mainittu algoritmi poistuu 7§2:n viittaamalta listalta. Tämä tapahtuma ei ole kovin yleinen (mutta listalta on poistunut algoritmejä), mutta kvanttitietokoneiden kehitys saattaa tuoda muutoksen tilanteeseen.

Ehdotamme 7§1 ja 7§2 suhteen selkeyttämistä niin, että 7§2 tulisi ensisijaiseksi.

Kommentit luvusta 3 Tunnistuspalveluiden yhteentoimivuus

Ei kommentoitavaa

Kommentit luvusta 4 Tunnistuspalvelun arviointikriteerit

Lukuun 4 ei esitetä oleellisia muutoksia. Traficomin laatiman ohjeen mainitseminen kohdassa 15.2 on tarpeellinen lisäys, jos tosin se täyttää nykyisen 15§2 kohdan vaatimuksen.

Käsittääksemme suurin osa auditoinneista tehdään jo nyt pääosin ohjeeseen 211 perustuen. Näkisimme hyvänä, jos sen asemaa vahvistettaisiin määräyksen tasolla niin, että ohjeen mukana tehtävä auditointi olisi oletus, muiden käyttäminen sallittua perustellusta syystä. Näin edistettäisiin auditointien yhteismitallisuutta, edistettäisiin auditointia tekevien yritysten kilpailuttamista sekä vältettäisiin tilannetta, jossa auditointeja koetetaan tehdä mahdollisimman löysän ja suppean standardin mukaan.

Kommentit luvusta 6 Hyväksytyt luottamuspalvelut

Ei kommentoitavaa

Kommentit siirtymäajoista, säännös 24

Säännösten 6.2.1 ja 6.2.2 siirtymäajaksi ehdotetaan 6 kk määräyksen voimaantulosta. Vaikka tunnistustapahtuman yksilöinti tunnistusjärjestelmän toiminnallisuudella ei sinällään ole kovin vaikeaa, on mahdollista, että tämä muutos on järkevää tehdä muiden tunnistusjärjestelmään tehtävien muutosten yhteydessä. Ehdotamme, että Traficom pidättää itsellään oikeuden myöntää lisäaikaa perustelluista syistä.

Kommentit muista säännöksistä (joihin ei esitetä muutoksia)

-

Soini Olli-Pekka

Nixu Certification Oy

**16.12.2021**

**Signicat comments**

Signicat has reviewed the proposed Regulation M72B/2022. Our comments are found below.

6.2.1 states: The identification service must present the identification means user with information based on which the user is able to connect the confirmation request received in their identification means to the service event. This information must be presented in identification means that have the technical ability to do so.

6.2.2 has a similar requirement for identification of the relying party (the service provider). This is reflected in 12.1 adding as mandatory the name of the relying party to the information attributes.

Signicat welcomes the requirement for identification of the relying party. In our view, this is an important means for increased security and transparency to users.

Signicat’s interpretation of requirement 6.2.1 is that information, typically a text, shall be displayed both in the web interface for the FTN identity provider and in the identity means themselves. Meaning it is the identification provider’s responsibility to cover this requirement. Signicat however sees that there may be occasions where the broker may need to display the web interface part of the text. For this, and for other purposes, Signicat proposes that a text string parameter can be added as an optional element in 12.2 to pass on information from broker to identification provider for display to the user. This can be used for several purposes. E.g. one can pass payment information as required by PSD2, and an identification method with proper support could display the information and ensure that the authentication does the required PSD2 dynamic linking to the text message.

6.2.3 allows SSO with FTN with some cautions. Signicat supports this change as long as provisioning of SSO is not mandatory.

8.1 states for certificates and keys used to establish a trust relationship:

The authentication must be based on a qualified electronic signature or a qualified electronic seal in compliance with the eIDAS Regulation or a direct bilateral procedure. Authentication may not only be based on a generally trusted digital certificate.

While the direct bilateral procedure is likely used in most cases, the other alternative spurs a comment. Qualified seals are very seldom used in practice. Requiring this level implies that the actors must possess qualified seal creation devices, where only a few and costly products exist. The requirement should at least be reduced to qualified certificate for e-seal, meaning an advanced e-seal with qualified certificate is enough. This is in line with the requirements for PSD2 and Open Banking. Regarding the requirement for qualified signature, this mechanism is currently only available with FINeID in Finland and for the other Nordic countries only available in Iceland. Signicat plans launch of a qualified signature service mid-2022 that can mediate some of this problem but qualified signature, and even qualified certificate, based on an FTN eID is in the future if it at all will happen. A requirement for qualified signature or certificate is thus impractical and also too strict, but it is recognised that finding a right “level” for another type of generally trusted digital certificate is not easy. Perhaps reference to the NCP policy level of ETSI EN 319 411-1 can be an alternative.

Signicat is concerned that this requirement from 8.1 as well as other requirements imposed upon the relying party by clause 8 can have negative impacts. Already today our experience is that having specific Finnish requirements causes problems to relying parties that operate in many countries. Such relying parties would like one broker interface with standard security measures. Also, the requirements can be difficult to cope with for small relying parties. The security measures must be justified from risk evaluation but must also be proportionate from an economic and resource point of view by the actors.

**1.12.2021**

**S-Pankki**

Ohessa kommenttimme aiheeseen "Traficomin lausuntopyyntö määräysluonnoksesta 72B tunnistus- ja luottamuspalveluista ja määräyksen perustelumuistiosta."

12.2 Valinnaiset tiedot

Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on oltava teknisesti suunniteltu valmius välittää.

Kommentti/kysymys: Pitääkö olla teknisesti tehtynä vai riittääkö että on suunniteltu? Voitteko avata tätä?

Määräyksen kohdan 6.2.1 vaatimus on toteutettava viimeistään x.10.2022.

Toiveena lokakuun viimeinen päivä. Meillä on julkaisu lokakuun loppupuolella.

Tommy Peltonen

Tuoteomistaja

Digitaaliset palvelut ja kehitys

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). [↑](#footnote-ref-1)
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). [↑](#footnote-ref-2)
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). [↑](#footnote-ref-3)
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). [↑](#footnote-ref-4)
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 [↑](#footnote-ref-5)
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 [↑](#footnote-ref-6)