TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

# Määräys 72 työpajat 2020-2021

Määräys 72 A/2018 M sähköisistä tunnistus- ja luottamuspalveluista

# 10.2.2021 työpajan osallistujat

- Työpajassa oli paikalla n. 32 henkilöä seuraavista organisaatioista
  - Aktia, Danske, Handelsbanken, Nordea, OP, POP-pankit, S-Pankki Säästöpankit, Ålandsbanken
  - DNA, Elisa, Telia
  - Samlink, Ubisecure, Signicat
  - TietoEvry
  - DVV, KKV, Fiva
  - Finanssiala, FiCom
  - Puolustusvoimat

# Määräys 72 työpajat 2020-2021
# Työpaja 3/7 agenda

- Työpajat, aikataulu, työtapa
- Määräyksen yleiset linjat

- Tunnistusjärjestelmä tietoturvallisuuden hallinta (4 §)
- Tunnistusjärjestelmän tekniset tietoturvavaatimukset (5 §)
- Tunnistuspalvelun häiriöilmoitukset virastolle (11 §)
- Tunnistuspalvelun vaatimustenmukaisuuden arviointikriteerit (15 §)
- Sisäisen ja ulkoisen arviointielimen riippumattomuus ja pätevyys (18 § ja 19 §)


# Työpajat

16.12.2020-10.6.2021

# Työtapa

- Työpajat ovat avoimia sidosryhmille
- Kutsu viimeistään 1-2 viikkoa ennen työpajaa viraston sähköpostijakeluilla (luottamusverkosto, eidas-tekninen, eidas-yleinen ”tulu”)
- Kutsun kanssa samaan aikaan jaetaan/julkaistaan viraston valmistelumuistio työpajan aiheesta
- Työpajoissa käydään läpi valmistelumuistion muutosehdotukset ja niiden vaikutusten arviointi
- Viimeisessä työpajassa käydään läpi koko muutettu määräys ja perustelumuistio
- Sidosryhmät voivat koko työn ajan toimittaa kirjallisia kommentteja valmisteluun. Kommenttien julkisuus arvioidaan julkisuuslain mukaisesti.
- Virasto voi pyynnöstä järjestää kahdenvälisiä tapaamisia asioissa, joita ei voi niiden luonteen takia käsitellä julkisessa työpajassa

# Määräystyöpajojen aikataulu

| Aika | Materiaali | Aihe | Lisätyöpaja (tarvittaessa) |
|---|---|---|---|
| KE 16.12.2020<br>9-11.30 | 7.12.2020 | Tunnistus:<br>rajapinnat ja attribuutit | KE 3.2.2021<br>9-11 |
| KE 20.1.2021<br>9-11.30 | 11.1.2021 | Tunnistus:<br>Salaus, osapuolten varmentaminen ja avaintenvaihto | KE 3.2.2021<br>9-11 |
| **KE 10.2.2021<br>9-11.30** | **1.2.2021** | **Tunnistus:<br>tunnistusjärjestelmän tekniset vaatimukset ja arviointi** | KE 17.2.2021<br>9-11 |
| KE 10.3.2021<br>9-11.30 | 1.3.2021 | Tunnistus:<br>tunnistusmenetelmä, PSD2-vertailu<br>Blockchain ja SSI | KE 17.3.2021<br>9-11 |
| KE 15.4.2021<br>9-11.30 | 1.4.2021 | Luottamuspalvelut:<br>palveluiden ja arvioinnin ETSI-standardit | KE 21.4.2021<br>9-11 |
| KE 12.5.2021 | 3.5.2021 | Keskeneräiset aiheet | TO 20.5.2021<br>9-11 |
| TO 10.6.2021<br>9-11.30 | 3.6.2021 | Koko määräys ja perustelut | |

# Jatkoaikataulu – muutokset mahdollisia

- 6-8/2021 virkavalmistelu ja käännökset
- **9/2021 lausuntokierros**
- 10/2021 lausuntokooste, mahdolliset muutokset ja niiden käännökset
- **10/2021 palautetilaisuus lausuntokierroksen tuloksista**
- n. 10 – 12/2021 määräyksen EU-notifointi
- n. 1-2/2022 uusi määräys voimaan


# Määräyspäivityksen yleiset linjaukset

# Määräyspäivityksen yleiset linjaukset

- Määräyksen perusrakenne ja lukujako säilytetään
- Vaatimuksia ja perusteluja selvennetään ja ajantasaistetaan joiltain osin
- Viraston ohjeet ja suositukset pääpiirteissään samoissa asioissa kuin nyt
- Muutoksia harkitaan: attribuutit, salausvaatimukset ja luottamuspalveluiden standardiviitteiden täydennykset
  - mm. uhkat perusteena
- Operatiivisia palveluita ei ole säädetty viranomaiselle tehtäväksi (vrt. .FI)
- PSD2-vaatimuksia tarkastellaan referenssinä tunnistusmenetelmän vaatimusten kohdalla (nostoja toimijoilta tarvitaan)
- Blockchain: tilaisuus käsitellä lohkoketjuteknologian suhdetta tunnistuksen teknisiin vaatimuksiin ja arviointivaatimuksiin

# Tunnistus: tunnistuspalvelun tietoturvavaatimukset

*M72 Luku 2 Tunnistuspalvelun tietoturvavaatimukset*

*4 § Tunnistuspalvelun tarjoajan tietoturvallisuuden hallinnan vaatimukset*

*5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet*

# *4 § Tunnistuspalvelun tarjoajan tietoturvallisuuden hallinnan vaatimukset*

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

*Tietoturvallisuuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osa-alueet*

*1) tunnistuspalveluntarjoajan toimintaympäristö kokonaisuutena;*

*2) tietoturvallisuuden hallinnan johtaminen, organisointi ja ylläpito;*

*3) tunnistuspalvelun tarjontaan liittyvien tietoturvallisuusriskien hallinta;*

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

*5) tunnistuspalvelun tarjonnan suunnittelu ja ohjaus tietoturvavaatimusten täyttämiseksi; ja*

*6) tietoturvallisuuden hallinnan tehokkuuden ja toimivuuden arviointi.*

# Muutosehdotus: 4 kohta. 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.*

# Tunnistuspalvelun tarjoajan tietoturvallisuuden hallinnan vaatimukset (4 §)

- Kattaako 4 § selvästi tarpeelliset tunnistusjärjestelmän hallinnan osa-alueet? Vaatiiko määräyksen tai perustelujen selventämistä?
  - On syytä huomata, että tietoturvallisuuden ja riskien hallinta ei riitä täyttämään tunnistusjärjestelmän vaatimuksia, vaan tunnistusjärjestelmän on kaikilta osin täytettävä tekniset vaatimukset, joista säädetään tunnistuslaissa, EU:n komission varmuustasoasetuksessa ja muualla tässä määräyksessä.
- Onko vaatimusta tietoturvallisuuden hallinnan standardien noudattamisesta/käyttämisestä tarkasteltava/tarkennettava/tiukennettava?
  - Virasto harkitsee sanamuotoa tarkennettavaksi siten, että valittua tai valittuja tietoturvallisuuden hallinnan standardeja on noudatettava.
  - Olisiko tarkoituksenmukaista huomioida varmuustaso?
- Mitkä standardit ovat relevantteja tietoturvallisuuden hallinnan kannalta ISO 27001 lisäksi? (PCIDSS, …)?
  - Virasto arvioi, että edelleenkään ei ole esitetty relevantteja kokonaisvaltaisia vaihtoehtoja ISO 27001:lle

# Kommentit työpajassa 10.2.2021/tietoturvallisuuden hallinta (4 §)

- Ei kommentteja 4 § esitetystä muutosehdotuksesta
- Kokonaisuutta kommentoitiin hyväksi
- Virasto toteaa, että säännökseen ei olla nostamassa ISO 27001:n lisäksi uusia tietoturvallisuuden hallinnan kannalta relevantteja standardeja
  - Tällä hetkellä perusteluissa mainittuna PCIDSS ja Katakri
- Määräykseen tulossa tarkennuksia sanavalintoihin
  - Esimerkiksi: standardeja on jatkossa *noudatettava*
  - Ei kommentteja sanavalinnoista
- Viraston yhteenveto:
  - määräykseen on tulossa lähinnä perustelujen täsmennystä, ei suuria muutoksia
  - Täydennys 26.3.2021: standardin noudattamisvaatimuksen tarkoitus korostaa tietoturvallisuuden hallinnan merkitystä

# 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet

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

*1. tietoliikenneturvallisuus*
- *a) verkon rakenteellinen turvallisuus*
- *b) tietoliikenneverkon vyöhykkeistäminen*
- *c) suodatussäännöt vähimpien oikeuksien periaatteilla*
- *d) suodatuksen ja valvontajärjestelmien hallinnointi koko elinkaaren ajan*
- *e) hallintayhteydet*

*2. tietojärjestelmäturvallisuus*
- *a) pääsyoikeuksien hallinta*
- *b) järjestelmien käyttäjien tunnistaminen*
- *c) järjestelmien koventaminen*
- *d) haittaohjelmasuojaus*
- *e) turvallisuuteen liittyvien tapahtumien jäljitys*
- *f) poikkeamien havainnointikyky ja toipuminen*
- *g) kansainvälisesti tai kansallisesti suositellut salausratkaisut muutoin kuin 7 §:ssä säädetyltä osin*

*3. käyttöturvallisuus*
- *a) muutosten hallinta*
- *b) salassa pidettävän aineiston käsittely-ympäristö*
- *c) etäkäyttö ja -hallinta*
- *d) ohjelmistohaavoittuvuuksien hallinta*
- *e) varmuuskopiointi*

*Tuotantoverkko ja sen edellä 1 momentin 1) e) ja 3) c) alakohdissa tarkoitetut hallintayhteydet ja etäkäyttö- ja etähallinta on toteutettava siten, että organisaation muiden palveluiden kuten sähköpostin tai web-selailun kautta aiheutuvat tietoturvauhat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvauhat on*
- *a) korotetulla varmuustasolla erityisesti arvioitu ja minimoitu ja*
- *b) korkealla varmuustasolla kokonaisuutena arvioiden estetty.*

# Muutosehdotus: 5 kohta. Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet

## 5.1 Tunnistusjärjestelmän turvallisuuden laatu

*Tunnistusjärjestelmän tietoliikenne, tietojärjestelmät ja niiden käyttö on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä koko elinkaaren ajan siten, että tunnistuspalvelun eheys ja luottamuksellisuus on suojattu tunnistuspalvelun varmuustason mukaista [komission varmuustasoasetuksen liitteen kohdassa 2.3 tarkoitettua] kohtuullista tai korkeaa uhkaa ja hyökkäyspotentiaalia vastaan.*

*5.2 Tietoliikenneturvallisuus*
*Tunnistusjärjestelmän tietoliikenteessä on oltava*

*a) verkon rakenteellinen turvallisuus*
*b) tietoliikenneverkon vyöhykkeistäminen*
*c) suodatussäännöt vähimpien oikeuksien periaatteilla*
*d) suodatuksen ja valvontajärjestelmien hallinnointi ~~koko elinkaaren ajan~~*
*e) hallintayhteydet*

*5.3 Tietojärjestelmäturvallisuus*
*Tunnistusjärjestelmän tietojärjestelmissä on oltava*

*a) pääsyoikeuksien hallinta vähimpien oikeuksien periaatteella*
*b) järjestelmien käyttäjien yksilöity tunnistaminen*
*c) järjestelmien koventaminen*
*d) haittaohjelmasuojaus*
*e) turvallisuuteen liittyvien tapahtumien jäljityskyky- ja ennalta määritelty prosessi*
*f) poikkeamien havainnointikyky ja ennalta määritelty prosessi poikkeamien korjaamiseen*
*g) kansainvälisesti tai kansallisesti suositellut salausratkaisut sen lisäksi, mitä määrätään 7 ja 9 kohdassa*

*5.4 Käyttöturvallisuus*
*Tunnistusjärjestelmän käytössä on toteutettava*

*a) muutosten suunnitelmallinen hallinta*
*b) tiedon suunnitelmalliseen luokitteluun perustuva salassa pidettävän aineiston käsittely-ympäristö ja säilytys*
*c) etäkäyttö ja -hallinta, jossa tunnistusjärjestelmä suojataan etäkäyttöympäristön uhkilta*
*d) ohjelmistokehityksen ja ohjelmistohaavoittuvuuksien suunnitelmallinen hallinta*
*e) varmuuskopiointi*

*5.5 Tunnistusjärjestelmän tuotantoverkon hallinta- ja etäyhteydet*
*Tuotantoverkko ja sen edellä 5.2.e ja 5.4.c alakohdissa tarkoitetut hallintayhteydet ja etäkäyttö- ja etähallinta on toteutettava siten, että organisaation muiden palveluiden kuten sähköpostin tai web-selailun kautta aiheutuvat tietoturvauhat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvauhat on*

*a) korotetulla varmuustasolla erityisesti arvioitu ja minimoitu ja*
*b) korkealla varmuustasolla kokonaisuutena arvioiden estetty.*

# Muutosehdotus: 5 kohta. Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet

*5.2 Tietoliikenneturvallisuus*
*Tunnistusjärjestelmän tietoliikenteessä on oltava*

*a) verkon rakenteellinen turvallisuus*
*b) tietoliikenneverkon vyöhykkeistäminen*
*c) suodatussäännöt vähimpien oikeuksien periaatteilla*
*d) suodatuksen ja valvontajärjestelmien hallinnointi ~~koko elinkaaren ajan~~*
*e) hallintayhteydet*

*5.3 Tietojärjestelmäturvallisuus*
*Tunnistusjärjestelmän tietojärjestelmissä on oltava*

*a) pääsyoikeuksien hallinta vähimpien oikeuksien periaatteella*
*b) järjestelmien käyttäjien yksilöity tunnistaminen*
*c) järjestelmien koventaminen*
*d) haittaohjelmasuojaus*
*e) turvallisuuteen liittyvien tapahtumien jäljityskyky- ja ennalta määritelty prosessi*
*f) poikkeamien havainnointikyky ja ennalta määritelty prosessi poikkeamien korjaamiseen*
*g) kansainvälisesti tai kansallisesti suositellut salausratkaisut sen lisäksi, mitä määrätään 7 ja 9 kohdassa*

*5.4 Käyttöturvallisuus*
*Tunnistusjärjestelmän käytössä on toteutettava*

*a) muutosten suunnitelmallinen hallinta*
*b) tiedon suunnitelmalliseen luokitteluun perustuva salassa pidettävän aineiston käsittely-ympäristö ja säilytys*
*c) etäkäyttö ja -hallinta, jossa tunnistusjärjestelmä suojataan etäkäyttöympäristön uhkilta*
*d) ohjelmistokehityksen ja ohjelmistohaavoittuvuuksien suunnitelmallinen hallinta*
*e) varmuuskopiointi*

*5.5 Tunnistusjärjestelmän tuotantoverkon hallinta- ja etäyhteydet*
*Tuotantoverkko ja sen edellä 5.2.e ja 5.4.c alakohdissa tarkoitetut hallintayhteydet ja etäkäyttö- ja etähallinta on toteutettava siten, että organisaation muiden palveluiden kuten sähköpostin tai web-selailun kautta aiheutuvat tietoturvauhat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvauhat on*

*a) korotetulla varmuustasolla erityisesti arvioitu ja minimoitu ja*
*b) korkealla varmuustasolla kokonaisuutena arvioiden estetty.*

# Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet (5 §)

- Säännöksen vaatimukset eivät muutu, mutta niitä selvennetään. Säännöstä on tarkennettu ja perusteluihin on lisätty esimerkkejä soveltamisesta tunnistuspalveluiden vaatimustenmukaisuuden arvioinnissa ja valvonnassa kertyneen kokemuksen ja soveltamiskäytännön perusteella.
- Korotetun ja korkean varmuustason vaatimuksia ei pääsääntöisesti ole määritelty määräyksessä erikseen. (5.2. ennallaan).
- Perustelumuistion täydentäminen ja esimerkkien lisääminen
  - esim. tunnistuspalvelun arviointiohjeen 211/2019, katakrin ja/tai pitukrin avulla
- Vaatimusten tarkentaminen
  - Tarkennettu sanamuotoa (huomioida -> huolehdittava) sekä hyökkäyspotentiaalin sietokyky ”mittariksi”
  - Suunnitelmallisuuden vaatimusta tarkennettu kautta linjan
  - Pääsyoikeuksien hallinnan ja minimoinnin tarkennuksia: yksilöity tunnistaminen, pääsyoikeuksien hallinnan vähimpien oikeuksien periaate
  - Poikkeamien korjausprosessi
  - Tietojen säilyttämisen turvallisuusvaatimukset, osin siirretty 7 §:stä
- Varmuustasot. Korotetun ja korkean varmuustason vaatimuksia ei pääsääntöisesti ole määritelty määräyksessä erikseen.
- Mitä tehdään MPS:n suositukselle tunnistusjärjestelmän kellonajan luotettavuudesta?

# Kommentit työpajassa 10.2.2021/tekniset tietoturvatoimenpiteet (5 §)

- Keskusteltiin tunnistusjärjestelmän aikalähteen suosituksen tarpeellisuudesta
- Kommentoitiin, että aikaleimat eivät ole iso haaste, jos järjestelmien keskinäinen kommunikointi on sujuvaa
  - Todettu, ettei asia vaadi suositusta virastolta
- Kommentoitiin tarkennettujen sanamuotojen soveltamista; odotetaanko esim. suunnitelmallisuutta kohdissa, joissa sitä ei ole erikseen mainittuna?
  - Suunnitelmallisuuden vaatimusta korostettu läpi säännöksen
- Kysyttiin, miten toimitaan, jos jokin salausalgoritmi todetaan heikoksi?
  - Virasto katsoo. Että haavoittuvuuksien seuranta on osa ylläpitoa ja haavoittuvista on syytä luopua. Virasto ei voi suoraan kieltää määräyksen 7 kohdassa listatun käyttöä, mutta voidaan ohjeistaa ja jakaa tietoa ennen kuin määräystä ehditään tarvittaessa muuttaa. Algoritmien haavoittuvuudet eivät yleensä ilmene nopeasti, joten tämän ei oleteta realisoituvan.
- Etäyhteyksien hallintaan liittyvät vaatimukset (5.2 §) koettiin haastaviksi, toteutus voi aiheuttaa kustannuksia
  - Voimassa olevan määräyksen perusteluissa on annettu toteutuksesta esimerkkejä, kysymys on riskienhallinnasta.
- Virasto jatkaa valmistelua muistion mukaisesti.
  - Täydennys 26.3.2021: virasto säilyttää suosituksen tunnistusjärjestelmän kellonajan tarkkuudesta osana 5 §:n perusteluja, mutta muutettuna siten, ettei aikalähteisiin oteta kantaa

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

# Tunnistus: häiriöilmoitukset

*M72 Luku 2 Tunnistuspalvelun tietoturvavaatimukset*

*11 § Tunnistuspalveluntarjoajan häiriöilmoitukset Viestintävirastolle*

# *Muutosehdotus: 11 kohta. Tunnistuspalveluntarjoajan häiriöilmoitukset Viestintävirastolle*

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

*1) tunnistusväline tai välityspalvelu, johon häiriö vaikuttaa;*

*2) kuvaus häiriöstä ja sen tiedossa olevista syistä;*

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

*4) kuvaus korjaustoimenpiteistä; sekä*

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

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

# *11 § Tunnistuspalveluntarjoajan häiriöilmoitukset Viestintävirastolle*

*11.1 Ilmoitettavat tiedot*

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

*1) tunnistusväline tai välityspalvelu, johon häiriö vaikuttaa;*

*2) kuvaus häiriöstä ja sen tiedossa olevista syistä;*

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

*4) kuvaus korjaustoimenpiteistä; sekä*

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

*11.2 Merkittävät häiriöt*

*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.*

# Tunnistuspalveluntarjoajan häiriöilmoitukset Viestintävirastolle (11 §)

- Säännökseen on tehty valvonta- ja soveltamiskäytännön mukaisia selvennyksiä ilmoituskynnykseen.
- Ei määrätä toimivuushäiriöiden ilmoitukselle tarkkaa kynnystä
- Tunnistamisen eheyteen ja luottamuksellisuuteen liittyvissä poikkeamissa ilmoituskynnys on määräyksen mukaan matala ja esimerkkejä virastolle ilmoitettavista häiriöistä esitetään perusteluissa.
  - Onko esimerkkejä perusteluissa tarpeellista tarkentaa tai lisätä?
- Turvallisuusvaikutukset ja taloudelliset vaikutukset
  - Ilmoitusten havaintojen perusteella voidaan edistää kaikkien tunnistuspalveluiden turvallisuuden parantamista.
- Virasto arvioi, että ennakkokyselyssä saatuihin havaintoihin on vaikutettava ensisijaisesti valvonnalla ja tehostamalla edelleen luottamusverkoston keskinäistä informointia.

# Kommentit työpajassa 10.2.2021/häiriöilmoitukset (11 §)

- Ilmoitettavien tietoturvahäiriöiden esimerkeistä perusteluissa ei kommentteja
- Kommentoitiin, että ilmoituskynnys viranomaiselle koetaan korkeaksi. Tarvetta muutokselle on, mutta ratkaiseeko määräys tätä ongelmaa.
- Kommentoitiin, että EU:ssa on valmisteltavana ns. Dora-asetus, jossa mietitään finanssisektorille yhtenäisiä häiriöilmoituskynnysrajoja. Seurataan miten etenee, tullee vaikuttamaan finanssisektorin velvoitteisiin.
- Virasto jatkaa valmistelua muistion mukaisesti, tässä vaiheessa ei ole dataa toimivuushäiriöiden ilmoituskynnyksen määräämiseksi yksityiskohtaisesti (kesto, käyttäjämäärä tms.)
  - Häiriöilmoituksia voi mielellään toimittaa myös toimivuushäiriöistä myös vapaaehtoisesti.
  - Tietoturvahäiriöissä ilmoituskynnys on määräyksen mukaan matala.
  - Toimijoiden väliset ilmoitukset laissa eri asia kuin virastolle tehtävät ilmoitukset
  - Sekä virastolle että toimijoiden keskinäiset ilmoitukset myös valvonta-asia ja luottamusverkoston häiriöryhmän asia.

# Tunnistus: arviointikriteerit

*M72 Luku 3 Tunnistuspalvelun arviointikriteerit*

*15 § Arviointikriteerit*

# Nykyinen 15 § Arviointikriteerit

*Tunnistuspalvelun arvioinnin täytyy kattaa vaatimukset, jotka kohdistuvat*
*1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän)*
- *a) tietoturvallisuuden hallintaan*
- *b) tietojen säilyttämiseen*
- *c) tiloihin ja henkilökuntaan*
- *d) teknisiin toimenpiteisiin*

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

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

# Muutosehdotus 15 Arviointikriteerit

*15.1 Tunnistusjärjestelmän ja tunnistusmenetelmän arvioinnin osa-alueet*

*Tunnistuspalvelun arvioinnin täytyy kattaa vaatimukset, jotka kohdistuvat*

*1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän)*

- *a) tietoturvallisuuden hallintaan*
- *b) tietojen säilyttämiseen*
- *c) tiloihin ja henkilökuntaan*
- *d) teknisiin toimenpiteisiin*

*2) tunnistusmenetelmään eli tunnistusvälineen*

- *a) hakemiseen ja rekisteröintiin*
- *b) hakijan henkilöllisyyden todistamiseen ja varmentamiseen*
- *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 Arviointikriteeristöt*

*1. Edellä 15.1 kohdassa mainittujen osa-alueiden arvioinnin on katettava kaikki ~~perustuttava~~ tunnistus- ja luottamuspalvelulain ja tämän määräyksen vaatimukset.*

*2. 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.*

# Arviointikriteerit (15 §)

- Sanamuotoa tarkennettu soveltamiskäytännön mukaisesti
- 15.2.1 kohta: Arvioinnin täytyy kattaa kaikki tunnistuspalvelun tarjontaan vaikuttavan toiminnan tietoturvan ja tunnistusmenetelmän tietoturvan osa-alueille säädetyt vaatimukset.
  - On syytä huomata, että tietoturvallisuuden ja riskien hallinta ei riitä täyttämään tunnistusjärjestelmän vaatimuksia, vaan tunnistusjärjestelmän on kaikilta osin täytettävä tekniset vaatimukset, joista säädetään tunnistuslaissa ja muualla tässä määräyksessä.
- 15.2.2 kohta: Arvioinnissa voi käyttää viraston arviointiohjetta tai EU tai kv. toimielimen ohjeita tai standardeja taikka niiden yhdistelmää
  - Viraston käsitys on, että määräyksen 15 §:n ja päivitetty tunnistuspalvelun arviointiohje 211/2019 muodostavat nyt toimivan kokonaisuuden, jonka puitteissa on edelleen mahdollista hyödyntää muista syistä tehtyjä tietoturva-arviointeja.
  - Arvioinnin voi koota useamman auditoijan tai arviointielimen useisiin kriteeristöihin perustuvista auditoinneista.
  - Onko määräyksen perusteluissa oleva lista informatiivinen, hyödyllinen ja ajan tasalla?
- 16 kohta ennallaan: Arvioinnin ei tarvitse kattaa palveluntarjoajan yleistä luotettavuutta tai käyttäjille ja luottaville osapuolille tarjottavia tietoja palvelusta (tunnistusperiaatteet, sopimusehdot, hinnastot). Näistä riittää toimijan oma selvitys.

# Esimerkkilista perusteluissa

- ISO 27001
- PCI DSS, PCI/QSA
- Webtrustin Trust Services Principles and Criteria for Certification Authorities ja Webtrust for Certification Authorities - SSL Baseline Requirements Audit Criteria
- Information Security Forumin (ISF) "Standard of Good Practice"
- ISF:n IRAM-kriteeristö (Information Risk Analysis Methodology)
- ETSI TS 101456 (CA policy)
- ISRS 4400 ja ISAE 3000
- Katakri
- Vahti
- Euroopan keskuspankin tai FIVA:n määräykset tai ohjeet
- FIVA:n määräys ja ohje 2.4 "Asiakkaan tunteminen - rahanpesun ja terrorismin rahoittamisen estäminen"
- Euroopan keskuspankin Cybersecurity questionnary 2015
- BISin (Bank for International Settlements) ohje External audits of banks
- **Onko määräyksen perusteluissa oleva lista informatiivinen, hyödyllinen ja ajan tasalla?**

# Kommentit työpajassa 10.2.2021/Arviointikriteerit (15 §)

- Tarkasteltiin perusteluiden esimerkkilistaa arviointistandardeista
- Todettiin, että osa yleisluontoisia ja osa spesifejä. Esitettiin toiveena, ettei perusteluissa mainitusta listasta suljettaisi pois mitään, esimerkiksi operaattorispesifisiä ohjeistuksia
- Nostettiin Pitukri ehdotuksena listalle
- Nostettiin Euroopan pankkiviranomaisen guideline pilvipalveluiden ulkoistamisesta ehdotukseksi listalle.
  - Fiva lupasi käydä osaltaan listaa vielä tarkemmin läpi ja toimittaa mahdollisia ehdotuksia jälkikäteen.
- Todettiin yhteenvetona, että listassa ei ole tällä hetkellä mitään vanhentunutta
- Virasto jatkaa valmistelua muistion mukaisesti ja tekee perusteluihin ehdotettuja täydennyksiä

# Arviointielimen pätevyys

*M72 Luku 5 Tunnistuspalvelun arviointielimen pätevyys*

*18 § Tunnistuspalvelun ulkoisen arviointielimen vaatimukset*
*19 § Tunnistuspalvelun sisäisen tarkastuslaitoksen vaatimukset*

# *18 § Tunnistuspalvelun ulkoisen arviointielimen vaatimukset*

*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.*

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

# *19 § Tunnistuspalvelun sisäisen tarkastuslaitoksen vaatimukset*

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

1) *IIA:n ammattistandardien (sisäisen tarkastuksen riippumattomuus ja objektiivisuus, ml. organisatorinen riippumattomuus) noudattamisella;*
2) *ISACA:n standardien ja tietojärjestelmien valvonnan kehikoiden noudattamisella;*
3) *BIS:in (Bank for International Settlements) sisäistä tarkastusta koskevien ohjeiden noudattamisella;*
4) *Finanssivalvonnan määräys- ja ohjekokoelman sisäistä tarkastusta koskevien ohjeiden noudattamisella;*
5) *muiden ETA-alueen jäsenvaltioiden vastaavien valvontaviranomaisten antamien ohjeiden tai määräysten noudattamisella; tai*
6) *muilla edellisiin rinnastettavilla viranomaissääntelyyn tai yleiseen riippumattoman sisäi-sen tarkastuksen hallintaan liittyvien standardien noudattamisella.*

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

# Tunnistuspalvelun ulkoisen arviointielimen vaatimukset (18 §)
# Tunnistuspalvelun sisäisen tarkastuslaitoksen vaatimukset (19 §)

- Ovatko 18 § ja 19 §:n viittaukset soveltuvia ja ajan tasalla
- Onko perustelumuistion esimerkkistandardilista arvioinnille soveltuva, ajan tasalla ja hyödyllinen

- Viraston arvion mukaan esimerkkilistassa ei ole muutostarpeita.

# Kommentit työpajassa 10.2.2021/arviointielimen pätevyys (18 ja 19 §)

- Ei kommentteja näistä aihealueista
- Finanssivalvonta lupasi tarkistaa oman alansa viittausten ajantasaisuuden

# Seuraava työpaja

- Tunnistusmenetelmä, PSD2-vertailu, Blockchain ja SSI
  - ke 10.3.2021
  - PSD2-vaatimusten havainnoista toivotaan ennakkopalautetta
  - Blockchain/SSI-teemasta toivotaan alustusta
  - Muistio tulee 1.3.2021

# Kommentit 10.2.2021

- Ke 10.3.2021 seuraava työpaja, jonka aiheena tunnistusmenetelmä, PSD2-vertailu, Blockchain ja SSI.
- Traficom toivoi seuraavaan työpajaan alustusta lohkoketju /SSI teemasta suhteessa tunnistusmenetelmälle ja -järjestelmälle asetettaviin vaatimuksiin
- Keskusteltiin kaivataanko alustusta blockchainista yleensä vai käyttötapauksia. Mikä on kohderyhmä?
- Viraston mukaan kohderyhmänä kaikki, joita vaatimusten määrittely koskee
- Kommentoitiin, että SSI on blockchainia olennaisempi
- Todettiin, että pyydetään Findy-ryhmältä alustus

# Kiitos osallistumisesta, olkaa yhteydessä

eidas@traficom.fi

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus