

# **Sähköisen tunnistuspalvelun arviointiohje**

**211/2023 O**

Liikenne- ja viestintäviraston ohje

## Sisältö

|          |                                                                                                                   |           |
|----------|-------------------------------------------------------------------------------------------------------------------|-----------|
| <b>1</b> | <b>Johdanto</b>                                                                                                   | <b>4</b>  |
| 1.1      | Ohjeen tarkoitus                                                                                                  | 4         |
| 1.2      | Ohjeen voimaantulo                                                                                                | 4         |
| 1.3      | Säädös- ja standardiviittaukset ja lyhenteet                                                                      | 5         |
| 1.4      | Tunnistuspalvelun määritelmät                                                                                     | 6         |
| 1.5      | Palveluntarjoajan yleinen luotettavuus ei sisälly kriteeristöön                                                   | 7         |
| <b>2</b> | <b>Tunnistuspalvelun arviointi ja tarkastuskertomus</b>                                                           | <b>8</b>  |
| 2.1      | Tarkastuskertomuksen toimittaminen ilmoituksen liitteenä                                                          | 8         |
| 2.1.1    | Aloitusermoitus                                                                                                   | 8         |
| 2.1.2    | Muutusermoitus                                                                                                    | 8         |
| 2.1.3    | Määräaikaissarviointi                                                                                             | 9         |
| 2.2      | Tunnistuspalvelun arvioitavat osa-alueet                                                                          | 9         |
| 2.3      | Tunnistusmenetelmä, tunnistusjärjestelmä ja alihankkijat                                                          | 11        |
| 2.3.1    | Määritelmät                                                                                                       | 11        |
| 2.3.2    | Arviointi ja alihankkijat                                                                                         | 12        |
| 2.3.3    | Tarkastuskertomus: Kuvaus siitä, minkä osan tunnistusmenetelmästä ja/tai tunnistusjärjestelmästä arviointi kattaa | 13        |
| 2.3.4    | Tarkastuskertomus: Arvioitavan tunnistuspalvelun nimi/nimet                                                       | 13        |
| 2.3.5    | Tarkastuskertomus: Tunnistusmenetelmän (tunnistusvälineen) kuvaus                                                 | 13        |
| 2.3.6    | Tarkastuskertomus: Tunnistusjärjestelmän kuvaus (järjestelmäarkkitehtuuri)                                        | 14        |
| 2.4      | Tiedot arviointielimestä                                                                                          | 14        |
| 2.4.1    | Tarkastuskertomus: Arviointielimen yksilöinti- ja yhteystiedot                                                    | 15        |
| 2.4.2    | Tarkastuskertomus tai ilmoitus: Arviointielimen pätevyys ja riippumattomuus                                       | 15        |
| 2.5      | Arvioinnin toteuttaminen                                                                                          | 16        |
| 2.5.1    | Tarkastuskertomus: Arvioinnin ajankohta ja kesto henkilötyöaikana                                                 | 16        |
| 2.5.2    | Tarkastuskertomus: Arviointimenetelmät                                                                            | 16        |
| 2.5.3    | Tiedot dokumentaatiosta, jota on käytetty vaatimuksenmukaisuuden arvioinnissa                                     | 17        |
| 2.5.4    | Tunnistusmenetelmän riskiarvio                                                                                    | 17        |
| 2.6      | Arvioinnin suhteuttaminen varmuustasoon ja riskeihin                                                              | 17        |
| 2.7      | Tarkastuskertomuksen tarkkuus                                                                                     | 19        |
| 2.8      | Poikkeamien raportointi tarkastuskertomuksessa                                                                    | 20        |
| 2.9      | Poikkeamien korjaus ja korjauksista raportointi                                                                   | 20        |
| <b>3</b> | <b>Arvioitavat osa-alueet</b>                                                                                     | <b>20</b> |
| 3.1      | Tunnistusmenetelmän ominaispiirteet ja todentamismekanismi                                                        | 20        |
| 3.2      | Yhteentoimivuus                                                                                                   | 21        |
| 3.3      | Tekniset tietoturva-vaatimukset                                                                                   | 21        |
| 3.4      | Poikkeamien havainnointikyky ja hallinta sekä häiriöilmoitukset                                                   | 22        |
| 3.5      | Tietojen säilyttäminen ja käsittely                                                                               | 22        |

|      |                                                                                                       |    |
|------|-------------------------------------------------------------------------------------------------------|----|
| 3.6  | Tilaturvallisuus .....                                                                                | 23 |
| 3.7  | Riittävät ja pätevät henkilöresurssit .....                                                           | 23 |
| 3.8  | Tietoturvallisuuden hallinta .....                                                                    | 23 |
| 3.9  | Tunnistusvälineen hakijan henkilöllisyyden todistaminen ja varmentaminen<br>(ensitunnistaminen) ..... | 24 |
| 3.10 | Huomioita henkilöllisyystodistuksen perusteella ensitunnistamisesta etäyhteydellä<br>.....            | 24 |
| 3.11 | Tunnistusvälineen eli tunnistusmenetelmän elinkaari .....                                             | 30 |
| 3.12 | Testaaminen .....                                                                                     | 30 |

**LIITE A: Tarkastuskertomusohjeen muistilista .....31**

**LIITE B: Tunnistuspalvelun yleinen arviointikriteeristö .....33**

|       |                                                                                                       |     |
|-------|-------------------------------------------------------------------------------------------------------|-----|
| B 1   | Tunnistamisen menetelmän ominaispiirteet ja todentamismekanismi .....                                 | 33  |
| B 2   | Yhteentoimivuus .....                                                                                 | 52  |
| B 3   | Tekniset tietoturvavaatimukset.....                                                                   | 56  |
| B 3.1 | Tietoliikenneturvallisuus.....                                                                        | 58  |
| B 3.2 | Tietojärjestelmäturvallisuus.....                                                                     | 66  |
| B 3.3 | Käyttöturvallisuus .....                                                                              | 71  |
| B 4   | Poikkeamien havainnointikyky ja hallinta ja häiriöilmoitukset .....                                   | 74  |
| B 5   | Tietojen säilyttäminen ja käsittely.....                                                              | 80  |
| B 6   | Tilaturvallisuus .....                                                                                | 88  |
| B 7   | Riittävät ja pätevät henkilöresurssit .....                                                           | 90  |
| B 8   | Tietoturvallisuuden hallinta .....                                                                    | 91  |
| B 9   | Tunnistusvälineen hakijan henkilöllisyyden todistaminen ja varmentaminen<br>(ensitunnistaminen) ..... | 95  |
| B 10  | Tunnistusvälineen eli tunnistusmenetelmän elinkaari.....                                              | 113 |

**LIITE C Mobiilitunnistusratkaisun erityiskriteeristö .....123**

|     |                                                                             |     |
|-----|-----------------------------------------------------------------------------|-----|
| C 1 | Arkkitehtuuri, suunnittelu ja uhkakuvien mallintaminen .....                | 124 |
| C 2 | Tietojen tallennus ja tietosuojat .....                                     | 125 |
| C 3 | Salausvaatimukset.....                                                      | 127 |
| C 4 | Tunnistaminen, tunnistusmenetelmän ominaispiirteet ja istunnonhallinta..... | 128 |
| C 5 | Tietoliikenne .....                                                         | 133 |
| C 6 | Alustan ja sovelluksen yhteistyö .....                                      | 134 |
| C 7 | Ohjelmistokoodin turvallisuus, laatu ja kehitysympäristö .....              | 135 |
| C 8 | Turvakontrollit ja suojaus (EN: Resilience) .....                           | 136 |

**Viitteet .....137**

## 1 Johdanto

Tämä ohje koskee sähköisen tunnistuspalvelun vaatimustenmukaisuuden arviointia ja arvioinnista lopputuloksena laadittavaa tarkastuskertomusta.

Ohjeessa on liitteenä yleinen mallikriteeristö vahvan sähköisen tunnistuspalvelun vaatimustenmukaisuuden arvioimiseksi ja erityinen mobiilisovelluksille laadittu kriteeristö.

Ohjeessa on liitteenä muistilista tarkastuskertomuksen sisällöstä.

Ohje koskee tunnistuspalveluita, jotka ovat ilmoittautuneet tai aikovat ilmoittautua tunnistuslain 10 §:n tai 11 §:n mukaisesti vahvaksi sähköiseksi tunnistuspalveluksi. Ohje koskee sekä sähköisten tunnistusvälineiden tarjoajia että tunnistusvälityspalveluita.

### 1.1 Ohjeen tarkoitus

Ohje on tarkoitettu vahvan sähköisen tunnistuspalvelun tarjoajille ja arviointielimille, joilta tunnistuspalvelut hankkivat arviointia.

Ohjeen tarkoitus on selkeyttää, mitä seikkoja palveluun liittyvien auditointien täytyy kattaa, jotta auditoinnit kattavat kaikki vaaditut osa-alueet. Arvioinnissa voi käyttää tämän ohjeen kriteeristöjä tai muita kriteeristöjä tai niiden yhdistelmiä, jotka kattavat kaikki arvioitavaksi säädettyt osa-alueet. Mallikriteeristön noudattaminen ei siis ole pakollista, vaan se on yksi tapa varmistaa, että arviointi on riittävän kattava.

Auditoinnin lopputuloksena toimitetaan Liikenne- ja viestintävirastolle tunnistuspalvelun tarkastuskertomus. Ohjeen tarkoituksena on selkeyttää tarkastuskertomuksen vähimmäissisältöä ja esittämistapaa.

Liikenne- ja viestintäviraston tehtävänä on valvoa tunnistus- ja luottamuspalvelulain (617/2009) 42 §:n nojalla lain ja EU:n eIDAS-asetuksen<sup>1</sup> noudattamista. Tämä ohje on annettu lain 42 §:n yleisen valtuuden nojalla.

Liikenne- ja viestintävirastolle toimitettavista ilmoituksista on julkaistu erillinen ohje (214/2023 O). EU:lle notifioitavan sähköisen tunnistamisen järjestelmän vaatimustenmukaisuuden arvioinnista säädetään eIDAS-asetuksessa sekä sähköisen tunnistamisen varmuustasoasetuksessa (LoA)<sup>2</sup>.

### 1.2 Ohjeen voimaantulo

Ohje 211/2023 O tulee voimaan 13.7.2023

Ohje on voimassa toistaiseksi ja sitä täydennetään ja muutetaan tarvittaessa. Tällöin ohjeen numero säilyy, mutta päivämäärä vaihtuu ja vuosiluku vaihtuu tarvittaessa. Ohjeen muutetut versiot listataan seuraavaan taulukkoon

Voimassa oleva ohje julkaistaan Liikenne- ja viestintäviraston verkkosivulla <https://www.kyberturvallisuuskeskus.fi/fi/sahkoinen-tunnistaminen>.

<sup>1</sup> Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014 sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta.

<sup>2</sup> Komission täytäntöönpanoasetus (EU) 2015/1502 teknisten vähimmäiseritelmien ja -menettelyjen vahvistamisesta sähköisen tunnistamisen menetelmien varmuustasoja varten sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 8 artiklan 3 kohdan mukaisesti

| Versio                                                                                                                                    | Päiväys   | Kuvaus/muutos                                                                                                                                                                                                                                                                                                                                                                                                   | Tekijä                                                 |
|-------------------------------------------------------------------------------------------------------------------------------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| 211/2023 O,<br>Traficom/<br>20767/<br>09.02.00/2022                                                                                       | 13.7.2023 | <ul style="list-style-type: none"> <li>3. julkaistu versio</li> <li>lisätty etäensitunnistamiseen liittyviä kriteereitä</li> <li>lisätty lompakkoratkaisuihin soveltuvia kriteereitä</li> </ul>                                                                                                                                                                                                                 | Liikenne- ja viestintävirasto, Kyberturvallisuuskeskus |
| 211/2019 O                                                                                                                                | 9.10.2019 | 2. julkaistu yhdistetty versio <ul style="list-style-type: none"> <li>muutettu yleinen kriteeristö karsimalla kriteerejä ja listaamalla ne säädettyjen vaatimusten pohjalta</li> <li>lisätty kokonaan uusi erityiskriteeristö sähköisessä tunnistamisessa käytettäville mobiilisovelluksille</li> <li>yhdistetty päivitettyinä tunnistuspalvelun tarkastuskertomusta koskeva osa ohjeesta 215/2016 O</li> </ul> | Liikenne- ja viestintävirasto, Kyberturvallisuuskeskus |
| 211/2016 O<br>Tunnistuspalvelun auditoinnin mallikriteeristö<br><br>215/2016 O<br>Tunnistus- ja luottamuspalveluiden arviointikertomukset | 2.11.2016 | 1. julkaistut versiot                                                                                                                                                                                                                                                                                                                                                                                           | Viestintävirasto, Kyberturvallisuuskeskus              |

### 1.3 Säädös- ja standardiviittaukset ja lyhenteet

Tunnistuspalvelun yleinen arviointikriteeristö pohjautuu vahvalle sähköiselle tunnistamiselle säädettyihin vaatimuksiin.

Mobiilisovelluskriteeristö pohjautuu standardeihin ja sitä on täydennetty säädettyihin vaatimuksiin perustuvilla kriteereillä. Myös mobiilisovelluskriteeristössä yksilöidään säädetyt vaatimukset, joihin arviointikriteerit liittyvät.

Tarkastuskertomusohje perustuu säädettyihin vaatimuksiin.

Säädökset, joissa tunnistuspalvelujen vaatimuksista säädetään:

- Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009, jäljempänä *tunnistuslaki* tai *TunnL* tai *tunnistus- ja luottamuspalvelulaki*)
- Komission täytäntöönpanoasetus (EU) 2015/1502 (jäljempänä *LoA* tai *varmuustasoasetus*)
  - Tunnistuslaissa viitatu kohdat varmuustasoasetuksesta

- o LoA-guidance, varmuustasoasetuksen epävirallinen soveltamisohje<sup>3</sup>
- Liikenne- ja viestintäviraston määräys M72B/2022 (jäljempänä *M72B*)<sup>4</sup>
  - o Määräyksellä tarkennetaan eritä tunnistuslaissa säädettyjä vaatimuksia

Standardiviittaukset<sup>5</sup>:

- ISO/IEC 27001:2013/2017 Information security management
  - o Yleisen kriteeristön vaatimusten yhteydessä on viittaus relevantteihin ISO 27001 -standardin vaatimuksiin. Viittausten tarkoitus on helpottaa tunnistuspalvelun vaatimustenmukaisuuden arvioinnin yhdistäminen osaksi yleisen tietoturvallisuuden hallinnan arviointia.
- OWASP Mobile AppSec Verification v.1.4.2<sup>6</sup>
- ISO/IEC 29115
- ISO/IEC 15408-1
- ISO/IEC 18045
- ISO/IEC TS 29003:2018
- ISO/IEC 30107
- ETSI TS 102 165-1
- ETSI TS 119 461
- Common Criteria CCDB 2009 03

Varmuustason lyhenteet taulukoissa

- S=korotettu (vastaa eIDAS2, substantial)
- H=korkea (vastaa eIDAS3, high)

## 1.4 Tunnistuspalvelun määritelmät

*Vahva sähköinen tunnistus* on tunnistuspalvelua, joka täyttää tunnistuslaissa säädetyt vaatimukset ja jonka tarjoamisesta on ilmoitettu tunnistuslain mukaisesti rekisteröitäväksi Liikenne- ja viestintävirastolle.

*Tunnistuspalvelu* on säädännössä ja tässä ohjeessa yhteinen nimitys tunnistusvälineen tarjoajalle ja tunnistusvälityspalvelulle.

*Tunnistusvälineen tarjoaja* tarjoaa sähköisiä tunnistusvälineitä loppukäyttäjille.

*Tunnistusvälityspalvelu* välittää tunnistustapahtumia sähköisten asiointipalveluiden tarjoajille eli sähköiseen tunnistukseen luottaville osapuolille.

Vahvan sähköisen tunnistuspalvelun tarjoajat, jotka ovat tehneet Liikenne- ja viestintävirastoon tunnistuslain mukaisen ilmoituksen ja jotka täyttävät lain vaatimukset, muodostavat sähköisen tunnistamisen *luottamusverkoston*.

Tämä ohje on laadittu tunnistuspalvelun toimintoihin kohdistuvien vaatimusten kannalta eikä toimijoiden roolien kannalta. Ohjeen kohdassa 2.3 selvennetään, mitä tarkoitetaan tunnistusmenetelmällä ja tunnistusjärjestelmällä.

<sup>3</sup> [https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LoA\\_Guidance\\_Final\\_suomeksi.pdf](https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LoA_Guidance_Final_suomeksi.pdf)

<sup>4</sup> Määräys M72B/2022 sähköisistä tunnistus- ja luottamuspalveluista [https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/M72B\\_2022\\_M%C3%84%C3%84R%C3%84YS\\_72B\\_tunnistus-ja\\_luottamuspalvelut\\_julkaistu.pdf](https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/M72B_2022_M%C3%84%C3%84R%C3%84YS_72B_tunnistus-ja_luottamuspalvelut_julkaistu.pdf)

<sup>5</sup> Kriteeristön valmistelussa on käytetty taustamateriaalina myös seuraavaa: FIDO Security Reference: <https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-security-ref-v2.0-id-20180227.html>

<sup>6</sup> [https://www.owasp.org/index.php/OWASP\\_Mobile\\_Security\\_Testing\\_Guide](https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide)

**Määritelmät säädöksissä**

**TunnL 2 § Määritelmät**

1) vahvalla sähköisellä tunnistamisella sellaista henkilön, oikeushenkilön tai oikeushenkilöä edustavan luonnollisen henkilön yksilöimistä ja tunnisteen aitouden ja oikeellisuuden todentamista sähköistä menetelmää käyttäen, joka täyttää sähköisestä tunnistamisesta ja luottamuspalveluista annetun EU:n asetuksen 8 artiklan 2 kohdan b alakohdassa tarkoitetun korotetun varmuustason tai mainitun kohdan c alakohdassa tarkoitetun korkean varmuustason vaatimukset;

3) tunnistuspalvelun tarjoajalla tunnistusvälityspalvelun tarjoajaa tai tunnistusvälineen tarjoajaa;

4) tunnistusvälineen tarjoajalla palveluntarjoajaa, joka tarjoaa tai laskee liikkeelle vahvan sähköisen tunnistamisen tunnistusvälineitä yleisölle sekä tarjoaa tunnistusvälinettä tunnistusvälityspalvelun tarjoajalle välitettäväksi luottamusverkostossa;

5) tunnistusvälityspalvelun tarjoajalla palveluntarjoajaa, joka välittää vahvan sähköisen tunnistamisen tunnistustapahtumia sähköiseen tunnistukseen luottavalle osapuolelle;

10) luottamusverkostolla Liikenne- ja viestintäviraston ilmoituksen tehneiden tunnistuspalvelun tarjoajien verkostoa;

## 1.5 Palveluntarjoajan yleinen luotettavuus (ei sisälly kriteeristöön)

Riippumattoman arvioinnin ei tarvitse kattaa palveluntarjoajan yleistä luotettavuutta tai käyttäjille ja luottaville osapuolille tarjottavia tietoja palvelusta (tunnistuseriaatteet, sopimusehdot, hinnastot). Tätä osuutta ei siksi tarkastella kriteeristössä.

Näistä riittää **tunnistuspalvelun tarjoajan oma selvitys**, jonka palveluntarjoaja toimittaa Liikenne- ja viestintäviraston arvioitavaksi. Asiat on listattu määräyksen M72B kohdassa 16.

Liikenne- ja viestintävirastolle tunnistuspalvelun aloitus-, lopetus- ja muutositiloitusten yhteydessä toimitettavia tietoja on kuvattu tarkemmin **ohjeessa 214/2023 O Sähköisten tunnistus- ja luottamuspalveluiden ilmoitukset**.

**SÄÄNNÖKSET**

**M72B kohta 16 Selvitys tunnistuspalvelun tarjoajan ja julkaistujen tietojen luotettavuudesta**

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

- 1) tunnistuspalvelusta vastaava vakiintunut oikeushenkilö ja vastuuhenkilöiden toimintakelpoisuus ja luotettavuus;
- 2) julkaistut ilmoitukset ja käyttäjätiedot, kuten tunnistuseriaatteet, 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 siir-  
rosta, tietojen käsittelystä sekä ilmoituksista viranomaisille, luottamusverkostolle, luottaville  
osapuolille ja käyttäjille.

## 2 Tunnistuspalvelun arviointi ja tarkastuskertomus

### 2.1 Tarkastuskertomuksen toimittaminen ilmoituksen liitteenä

#### **SÄÄNNÖKSET**

##### **TunnL 10 § Tunnistuspalvelun tarjoajan velvollisuus ilmoittaa toiminnan aloittami- sesta**

Suomeen sijoittautuneen tunnistuspalvelun tarjoajan on ennen toimintansa aloittamista teh-  
tävä kirjallinen ilmoitus Liikenne- ja viestintävirastolle. Ilmoituksen voi tehdä myös sellainen  
tunnistuspalvelun tarjoajien yhteenliittymä, jonka hallinnoimaa palvelua on pidettävä yhtenä  
tunnistuspalveluna.

Ilmoituksessa on oltava:

[...]

5) vaatimustenmukaisuuden arviointilaitoksen, muun ulkoisen arviointilaitoksen taikka sisäi-  
sen tarkastuslaitoksen laatima tarkastuskertomus riippumattomasta arvioinnista 29 §:n mu-  
kaisesti;

[...]

Tunnistuspalvelun tarjoajan on viipymättä ilmoitettava 2 momentissa tarkoitetuissa tie-  
doissa tapahtuneista muutoksista kirjallisesti Liikenne- ja viestintävirastolle. Ilmoitus on teh-  
tävä myös toiminnan lopettamisesta sekä toimintojen siirtymisestä toiselle palveluntarjo-  
ajalle.

##### **TunnL 11 § Muuhun Euroopan talousalueen jäsenvaltioon sijoittautunut tunnistus- palvelun tarjoaja**

Mitä 10 §:ssä säädetään, ei estä muualle Euroopan talousalueelle sijoittautunutta tunnistus-  
palvelun tarjoajaa tekemästä mainitussa pykälässä tarkoitettua ilmoitusta.

##### **TunnL 31 § Tarkastuskertomus**

Tunnistuspalvelun tarjoajan ja Digi- ja väestötietoviraston on hankittava vaatimustenmukai-  
suuden arvioinnista tarkastuskertomus, joka toimitetaan Liikenne- ja viestintävirastolle.

Tarkastuskertomus on voimassa arvioinnissa käytetyn standardin määrittelemän ajan, kui-  
tenkin enintään 2 vuotta.

#### 2.1.1 Aloitusilmoitus

Tunnistuspalvelua koskeva tarkastuskertomus toimitetaan Liikenne- ja viestintävi-  
rastolle ilmoituksen liitteenä, kun uusi tunnistuspalvelun tarjoaja tekee virastolle  
ilmoituksen toiminnan aloittamisesta.

#### 2.1.2 Muutosilmoitus

Tunnistuspalvelua koskeva tarkastuskertomus toimitetaan Liikenne- ja viestintävi-  
rastolle ilmoituksen liitteenä, kun ilmoitetaan olennaisesta muutoksesta tunnistus-  
järjestelmässä.

Toiminnan olennaisissa muutostilanteissa täytyy tehdä arviointi ja toimittaa muu-  
tosta koskeva muutosilmoitus sekä tarkastuskertomus ennen muutoksen tuotan-  
toon viemistä.

Olennaisia muutoksia ovat esimerkiksi

- tunnistusmenetelmän eli todentamistekijöiden ja todentamismekanismin muutokset,
- tunnistusjärjestelmän tekniset muutokset eli ylläpito- ja tuotantojärjestelmän rakenteen, keskeisten ohjelmistojen tai muiden olennaisten komponenttien ja elementtien muutokset,
- ylläpitoa, laitteita, järjestelmiä tai ohjelmistoja toimittavien alihankkijoiden muutokset tai vaihtuminen,
- mobiilisovelluksen ja/tai siihen vaikuttavien käyttöjärjestelmien muutokset, jos ne edellyttävät tunnistuspalvelun oman jatkuvan riskinhallinnan ja riskiarvion perusteella tietoturvallisuuden vaatimustenmukaisuuden arviointia määräaikaisarviointien välissä.

### 2.1.3 Määräaikaisarviointi

Tunnistuspalvelua koskeva tarkastuskertomus toimitetaan Liikenne- ja viestintävirastolle, kun edellisen tarkastuskertomuksen valmistumisesta on kulunut kaksi vuotta.

Tunnistuspalvelun tarkastuskertomus on lain mukaan voimassa käytetyn standardin määrittelemän ajan, mutta kuitenkin enintään kaksi vuotta. Tarkastuskertomuksen voimassaoloaika eli enintään kaksi vuotta lasketaan päivämäärästä, jolloin edellinen tarkastuskertomus on valmistunut. Tunnistuspalveluntarjoajan on toimitettava virastolle uusi tarkastuskertomus viimeistään kahden vuoden kuluttua edellisen tarkastuskertomuksen valmistumisesta, mikäli se haluaa jatkaa vahvan sähköisen tunnistuspalvelun tarjoamista.

Tarkastuskertomus voi perustua kokonaan tai osittain standardeihin, joiden määrittelemä arviointiväli on vähemmän kuin kaksi vuotta. Tunnistuspalvelun tarjoajan vastuulla on huolehtia siitä, että arvioinnit tehdään tällaisissa tapauksissa standardin määrittelemien määräajoin. Tunnistuspalvelun tarjoajan on toimitettava virastolle vapaamuotoinen ilmoitus siitä, että jokin tarkastuskertomuksen osa-alue on arvioitu uudelleen ja on voimassa. Tämän ohjeen mukainen tarkastuskertomus on toimitettava viimeistään kahden vuoden kuluttua edellisen tarkastuskertomuksen valmistumisesta.

Liikenne- ja viestintävirasto pyrkii käsittelemään kaikkien tunnistuspalvelun tarjoajien säännöllisesti tehdyt tarkastuskertomukset samanaikaisesti ja julkaisee päivämäärän, jolloin arviointikertomukset tulee toimittaa, viimeistään 6 kuukautta ennen kyseistä ajankohtaa.

Aloitus- ja muutosilmoitusten vähimmäissisältö on kuvattu Liikenne- ja viestintäviraston ohjeessa 214/2023 O.

## 2.2 Tunnistuspalvelun arvioitavat osa-alueet

Asiat, joiden vaatimustenmukaisuus on arvioitava riippumattomasti, on säädetty tunnistuslaissa ja tarkennettu viraston määräyksessä M72B.

Arviointielin voi käyttää tämän ohjeen kriteeristöjä tai muutakin vastaavaa kriteeristöä tai menetelmää, kunhan arviointielin kykenee näyttämään tarkastuskertomuksessa, että käytetyllä menetelmällä voidaan osoittaa säädettyjen vaatimusten täyttäminen.

Ohjeen liitteessä B on yleinen tunnistuspalvelun arviointikriteeristö, joka kattaa kaikki vaatimukset tunnistusmenetelmän ja -järjestelmän toteutuksesta riippumatta.

Ohjeen liitteessä C on mobiilisovelluskriteeristö. Se täydentää yleistä kriteeristöä, jos tunnistusmenetelmässä ja -järjestelmässä on yhtenä osana mobiilisovellus.

Määräyksen 16 kohdassa tarkennetaan vaatimusalueet, joista tunnistuspalvelun tarjoaja voi esittää oman selvityksen.

**Tunnistusmenetelmän** eli tunnistusvälineen tarjoajaa koskevat kaikki kohdat.

**Tunnistusvälityspalvelua** koskevat määräyksen M72B 15 kohdan 1a-1e alakohdat ja 2g alakohta.

## **SÄÄNNÖKSET**

### ***TunnL 29 § Sähköisen tunnistuspalvelun vaatimustenmukaisuuden arviointi***

*Tunnistuspalvelun tarjoajan on määräajoin teetettävä palvelulle 28 §:ssä mainitun arviointielimen arviointi siitä, täyttääkö tunnistuspalvelu tässä laissa säädetyt yhteentoimivuutta, tietoturvaa, tietosuojaa ja muuta luotettavuutta koskevat vaatimukset.*

[...]

### ***TunnL 42 § Yleinen ohjaus sekä Liikenne- ja viestintäviraston määräykset***

[...]

*Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä:*

[...]

*5) 29, 30 ja 32 §:ssä tarkoitetuista arvioitavan tunnistus- tai luottamuspalvelun sekä kansallisen solmupisteen vaatimustenmukaisuuden arviointiperusteista;*

[...]

### ***M72B, 15 Arviointikriteerit***

#### ***15.1 Tunnistusjärjestelmän ja tunnistusmenetelmän arvioitavat toiminnot***

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

#### ***1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän):***

- a) tietoturvallisuuden hallintaan;*
- b) tietojen säilyttämiseen ja käsittelyyn;*
- c) tiloihin ja henkilökuntaan;*
- d) teknisiin toimenpiteisiin; ja*
- e) yhteentoimivuuteen luottamusverkostossa; sekä*

#### ***2) tunnistusmenetelmään eli tunnistusvälineen:***

- a) hakemiseen ja rekisteröintiin;*
- b) hakijan henkilöllisyyden todistamiseen ja varmentamiseen;*
- c) tunnistusmenetelmän ominaispiirteisiin ja laatimiseen;*
- d) myöntämiseen, toimittamiseen ja aktivointiin;*
- e) voimassaolon keskeyttämiseen, peruuttamiseen ja uudelleen aktivointiin;*
- f) uusimiseen ja korvaamiseen; ja*
- g) todentamismekanismeihin.*

## 15.2 Arviointikriteeristö

Vaatimuksenmukaisuuden arviointi voi perustua Liikenne- ja viestintäviraston arviointiohjeeseen tai EU:n tai muun kansainvälisen toimielimen antamiin säännöksiin tai ohjeisiin, julkaistuihin ja yleisesti tai alueellisesti sovellettuihin tietoturvallisuutta koskeviin ohjeisiin tai yleisesti käytettyihin tietoturvallisuusstandardeihin tai menettelyihin. Arviointi voi perustua usean edellä mainitun lähteen yhdistelmään.

## 2.3 Tunnistusmenetelmä, tunnistusjärjestelmä ja alihankkijat

### 2.3.1 Määritelmät

**Tunnistusmenetelmällä** tarkoitetaan käyttäjälle tarjottavaa tunnistusvälinettä ja tunnistustapahtumien teknistä toteutusta.

Tunnistusmenetelmään kuuluvat todentamistekijät ja todentamismekanismi.

**Tunnistusjärjestelmällä** tarkoitetaan tunnistuspalvelun teknistä ja organisatorista kokonaisuutta, jolle säädetään vaatimukset vahvan sähköisen tunnistamisen sääntelyssä.

Tunnistusjärjestelmään kuuluvat esimerkiksi tunnistuspalveluntarjoajan omat tai alihankitut tietoliikenneyhteydet ja tietojärjestelmät, ylläpito, tietojen käsittely, tietoturvallisuuden hallinta ja muut osa-alueet, jotka sisältyvät säädettyihin vaatimuksiin.

### **Määritelmät säädöksissä**

#### **TunnL 2 § Määritelmät**

2) tunnistusvälineellä sähköisestä tunnistamisesta ja luottamuspalveluista annetun EU:n asetuksen 3 artiklan 2 kohdassa tarkoitettua sähköisen tunnistamisen menetelmää;

**Vrt. TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset**

**Vrt. TunnL 8 a § Tunnistusmenetelmässä käytettävät todentamistekijät**

#### **eIDAS-asetus 3 artikla**

2) 'sähköisen tunnistamisen menetelmällä' aineellista ja/tai aineetonta kokonaisuutta, joka sisältää henkilön tunnistetietoja ja jota käytetään verkkopalveluun liittyvään todentamiseen;

4) 'sähköisen tunnistamisen järjestelmällä' sähköiseen tunnistamiseen liittyvää järjestelmää, jonka puitteissa sähköisen tunnistamisen menetelmiä myönnetään luonnollisille henkilöille, oikeushenkilöille tai oikeushenkilöä edustaville luonnollisille henkilöille;

**Vrt. eIDAS 7 artikla Edellytykset sähköisen tunnistamisen järjestelmien ilmoittamiselle**

...c) sähköisen tunnistamisen järjestelmä ja sen puitteissa myönnetty sähköisen tunnistamisen menetelmä täyttävät 8 artiklan 3 kohdassa tarkoitetussa täytäntöönpanosäädöksessä säädetyistä varmuustasoista ainakin yhden vaatimukset;

**Vrt. eIDAS 8 artikla Sähköisen tunnistamisen järjestelmien varmuustasot**

### **ALIHANKINTA SÄÄDÖKSISSÄ**

**TunnL 13 § Tunnistuspalvelun tarjoajan yleiset velvollisuudet**

[...]

*Tunnistuspalvelun tarjoaja vastaa apunaan käyttämiensä henkilöiden tuottamien palveluiden ja tuotteiden luotettavuudesta ja toimivuudesta.*

### 2.3.2 Arviointi ja alihankkijat

Tunnistuspalvelun tarjoaminen on usein vain osa yrityksen tai yhteisön toimintaa ja tunnistuspalvelussa voidaan käyttää samoja järjestelmiä kuin muussakin toiminnassa. Vaatimustenmukaisuuden arviointi täytyy tehdä tunnistuspalvelun kannalta. Vaatimusten tarkastelu täytyy kohdentaa organisaation vahvan sähköisen tunnistuspalvelun tunnistusjärjestelmään eli kaikkeen toimintaan, joka vaikuttaa vahvan sähköisen tunnistuksen säädettyjen vaatimusten täyttämiseen.

Arvioinnin täytyy kattaa myös alihankkijat (mukaan lukien nk. pilvipalvelut) siltä osin, kun ne toteuttavat jonkin osa tunnistuspalvelusta. Alihankkijoiden arvioinnin perusteellisuus voidaan suhteuttaa hankittavan toiminnon kriittisyyteen tunnistusjärjestelmässä. Myös ensitunnistamisen toteuttajat ovat osa tunnistusjärjestelmää.

Pilvipalveluita käytettäessä tunnistuspalvelun tarjoajan on varmistuttava siitä, että Liikenne- ja viestintäviraston valvontaoikeudet toteutuvat. Tässä on hyvä huomata, että myös kansainväliset pilvipalvelut voivat hyväksyä Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen tiedonsaannin.

**Tunnistusmenetelmään** liittyvistä vaatimuksista merkityksellisiä **tunnistusvälityspalvelun** toiminnassa ovat todentamismekanismit siltä osin, kun välityspalvelu välittää tunnistuksen tunnistusvälineen tarjoajan ja asiointipalvelun välillä. Todentamismekanismin vaatimukset ovat relevantteja myös tunnistusvälityspalvelun alihankkijan osalta siltä osin, kun alihankkijan järjestelmät vaikuttavat tunnistustahtumien turvallisuuteen.

Arviointikriteeristön taulukkoon ei ole erikseen merkitty ISO/IEC 27001:2013/2017 -viittauksia alihankkijoista. ISO-standardin mukaisessa tietoturvallisuuden hallinnan arvioinnissa alihankinta liittyy kautta linjan standardin kohtaan A.15.1 tietoturvallisuus toimittajasuhteissa.

Esimerkkejä tunnistusmenetelmän arvioinnista:

- Miten tunnuslukusovellus/matkapuhelin toimii toisena tunnistustekijänä ja mikä on tällöin ensimmäinen tunnistustekijä. Arvioinnissa on selvitettävä, miten tunnistaminen sovelluksella tapahtuu ja onko tähän useita tapoja (erityisesti todentamistekijöiden näkökulmasta). Onko niin, että vaaditaan aina jokin muukin tietoon perustuva tekijä/tekijöitä sovelluksen antaman kertakäyttösalasanan lisäksi. Onko mobiiliin sidottu muita todentamistekijöitä kuin tunnuslukusovellus/sovelluksen antama kertakäyttösalausana.
- Jos käytössä on mobiilitunnistussovellus, täytyy se arvioida kaikilta niiltä osin, joilla on vaikutusta tunnistamisen vaatimustenmukaisuuteen. Arvioinnissa on selvitettävä, miten varmistetaan sovelluksen sitominen oikeaan henkilöön päätelaitteessa ja taustajärjestelmässä. Jos sovellukseen on yhdistetty myös muita toimintoja, näitä muita toimintoja ei tarvitse sisällyttää arviointiin siltä osin, kun ne eivät voi vaikuttaa tunnistamisen luotettavuuteen.
- Jos tunnistautuminen asiointipalveluun voidaan tehdä pelkällä mobiilisovelluksella, on myös varmistuttava siitä, että todentamistekijät ovat riittävän erilliset. Toisin sanoen arvioinnissa on selvitettävä, miten menetelmässä varmistutaan siitä, että tietoon tai ominaisuuteen perustuva todentamistekijä ei joudu väärin käsiin, jos puhelin on toisen hallussa fyysisesti tai tietoturvaloukkauksen takia. Miten on estetty se, että matkapuhelimeen ei tallennu esimerkiksi kopiota tai murrettavissa olevaa tiivistettyä PIN-koodista, jolloin pelkän matkapuhelimen varastaminen vaarantaa tunnistautumisen.

Esimerkkejä tunnistusjärjestelmän arvioinnissa huomioitavista asioista:

- Konesali
- Sovelluspalvelimet ja palvelinalustat (virtuaalialusta)
- Pääsynhallinta palvelinalustalle
- Toimistoverkko (tunnistuspalvelun hallintajärjestelmän turvallisuus suhteessa muuhun toimistoverkkoon)
- Tietoliikenneyhteys palvelimeen (hallintayhteys)
- Virtuaalipalvelimen tietoturvallisuus (pääsynhallinta, päivitykset)
- Tunnistussovelluksen tietoturvallisuus (pääsynhallinta, päivitykset)
- Hallinta- ja tuotantoympäristön erottaminen
- Tuotanto/palveluympäristön tietoturvallisuus (sovellusliikennöinnin tietoturvallisuus/asiakasrajapinnat)
- Edellisiin liittyvä tila-, henkilöstö-, käyttö-, tietoliikenne-, ohjelmistoturvallisuus

**Pilvipalvelut**

- Tunnistuspalvelussa voi käyttää sellaisia pilvipalveluita, joiden vaatimustenmukaisuudesta pystyy arvioinnissa varmistumaan joko omalla arvioinnilla tai arvioimalla huolellisesti toisen riippumattoman ja pätevän arvioijan tekemän arvioinnin tuloksia. Siten esimerkiksi pilvipalvelusta hyödynnettävät palvelut/toiminnot/tuotteet on tarpeen yksilöidä tarkasti ja niiden sertifikaatteihin tai muuhun näyttöön on perehdyttävä.

**2.3.3 Tarkastuskertomus: Kuvaus siitä, minkä osan tunnistusmenetelmästä ja/tai tunnistusjärjestelmästä arviointi kattaa**

Tarkastuksen tulee kohdistua siihen osaan tunnistuspalveluntarjoajan järjestelmää, jossa tunnistuspalvelua tuotetaan. Tunnistuspalveluntarjoaja voi tilata arvioinnin osissa myös kahdelta tai usealta arviointielimeltä siten, että kukin arvioi osaa tunnistusjärjestelmästä. On tärkeää, että tarkastuskertomuksesta ilmenee yksiselitteisesti, kattaako arviointielimen laatima tarkastuskertomus vain osan tunnistusjärjestelmästä vai sen kokonaan. Arviointielimen on kuvattava selkeästi, mitkä osat tunnistusjärjestelmästä sen suorittama arviointi kattaa. Samoin tarkastuskertomuksesta tulee käydä ilmi se, että tunnistuspalveluntarjoajan järjestelmästä on tarkastettu ne kaikki osat, joissa tunnistuspalvelua tuotetaan.

**2.3.4 Tarkastuskertomus: Arvioitavan tunnistuspalvelun nimi/nimet**

Tarkastuskertomuksesta täytyy ilmetä tuote- tai palvelunimet, joilla käyttäjät ja asiointipalvelut tunnistavat, mistä palvelusta on kysymys.

Myös tunnistuspalvelun sisäisesti käyttämät nimitykset on hyvä kertoa, jos ne esiintyvät tarkastuskertomuksessa tai tunnistuspalvelun dokumentaatiossa.

**2.3.5 Tarkastuskertomus: Tunnistusmenetelmän (tunnistusvälineen) kuvaus**

Tarkastuskertomuksen on liitettävä kuvaus ja/tai dokumentaatio tunnistusmenetelmästä ja todentamismekanismista.

Kuvausten täytyy olla teknisesti niin tarkkoja, että niiden perusteella pystyy päätelemään, että kaikki vaatimusten kannalta relevantit asiat on huomioitu arvioinnissa.

- ✓ Mitkä ovat menetelmässä käytetyt todentamistekijät (vähintään kaksi eri luokista)
- ✓ Miten niiden riippumattomuus toisistaan on varmistettu
- ✓ Miten todentamistekijät on kytketty tunnistusvälineen haltijaan
- ✓ Todentamismekanismi eli tekninen kuvaus tunnistustapahtumien toteuttamisesta

Kuvausten täytyy kattaa alihankkijat.

### 2.3.6 Tarkastuskertomus: Tunnistusjärjestelmän kuvaus (järjestelmäarkkitehtuuri)

Tarkastuskertomukseen täytyy liittää tunnistusjärjestelmän kokonaisarkkitehtuurista kuva, kaavio tai muu selkeä esitys. Arkkitehtuuriselvityksen ja tarkastuskertomuksen perusteella on voitava varmistua siitä, että kaikki relevantit järjestelmän turvallisuuteen vaikuttavat tekijät on huomioitu arvioinnissa ja että järjestelmän arkkitehtuuri on turvallinen. Kuvausten täytyy kattaa alihankkijat.

- ✓ Järjestelmän arkkitehtuurikuvauksessa tulee olla nähtävillä tunnistamiseen liittyvät järjestelmäkomponentit.
- ✓ Selvityksen perusteella täytyy pystyä hahmottamaan tunnistusjärjestelmän osat ja niiden toimittajat, osien väliset yhteydet/yhdyskäytävät, yhteyksien suojauskäytännöt, järjestelmän osien väliset rajapinnat ja muut seikat.
- ✓ Arkkitehtuurikuvauksesta täytyy käydä ilmi koko tunnistusjärjestelmän komponenttien toiminnalliset suhteet kokonaisuudessaan, mm. tietovarantojen eriyttäminen, esityskerroksen ja liiketoimintalogiikan eriyttäminen, yhdyskäytävät/ympäristöjen väliset kytkennät ja näiden suojaus sekä ulkoisten toimijoiden väliset turvallisuuskontrollit.
- ✓ Kuvauksesta pitäisi selvittää verkkotopologia, L3-tason komponentit kuten palomuurit, palvelimet ja yhteenkytkennät muihin ympäristöihin sekä hallintayhteydet, mikäli ne on eriytetty.
- ✓ Lisäksi tulisi kuvata tunnistusprosessiin liittyvät tietovuot.
- ✓ Jos järjestelmä käyttää hyväkseen pilvipalveluiden tuotteistettuja komponentteja tai tuotteita (Amazon Web Services, Google, Microsoft Azure jne.), tulee tuotekomponentit nimetä ja sisällyttää nämä ulkoiset komponentit alihankkijoihin kohdistuvan arvioinnin piiriin.

## 2.4 Tiedot arviointielimestä

### **SÄÄNNÖKSET**

#### **TunnL 28 § Vaatimustenmukaisuuden arviointielimet**

*Tämän luvun mukaisen palvelun vaatimustenmukaisuuden voivat arvioida seuraavat arviointielimet siten kuin jäljempänä säädetään:*

- 1) vaatimustenmukaisuuden arviointilaitos;*
- 2) muu yleisesti käytetyn menetelmän mukaisesti toimiva ulkoinen arviointielin (muu ulkoinen arviointilaitos); tai*
- 3) palveluntarjoajan sisäinen yleisesti käytetyn standardin mukainen riippumaton arvioija (sisäinen tarkastuslaitos).*

Tarkastuskertomuksen täytyy perustua tunnistus- ja luottamuspalvelulain 4 luvun mukaisen arviointielimen tekemään arviointiin. Tunnistuspalvelun arvioija voi olla korotetulla varmuustasolla ulkoinen arviointilaitos tai sisäinen tarkastuslaitos. Korkealla varmuustasolla arviointielimen on oltava ulkoinen arviointilaitos.

Tunnistusjärjestelmän vaatimustenmukaisuuden arviointi voi koostua monen arviointielimen tekemästä arvioinnista. Näistä voidaan toimittaa erilliset tai yhdistetty tarkastuskertomus. Kaikkien arviointielinten tiedot täytyy selvittää.

Tunnistuspalvelun tarkastuskertomuksesta täytyy käydä ilmi vähintään seuraavat perustiedot.

2.4.1 Tarkastuskertomus: Arviointielimen yksilöinti- ja yhteystiedot

- ✓ Yrityksen tai yhteisön nimi ja yksilöivä rekisterinumero tai -tunnus;
- ✓ jos yritys tai yhteisö on sijoittunut muuhun ETA-alueen valtion kuin Suomeen, rekisteri, johon ulkomainen yhteisö tai yritys on merkitty;
- ✓ postiosoite ja yhteyshenkilöt; ja
- ✓ sähköpostiosoitteet Liikenne- ja viestintäviraston tiedusteluja varten.

2.4.2 Tarkastuskertomus tai ilmoitus: Arviointielimen pätevyys ja riippumattomuus

Selvityksen voi antaa tarkastuskertomuksessa tai muutoin ilmoituksen yhteydessä.

Selvityksestä täytyy käydä ilmi arviointielimen riippumattomuuden ja pätevyyden peruste (noudatettava standardi tai muu määräyksen M72B 18 tai 19 kohdan mukainen peruste)

**TunnL 42 § Yleinen ohjaus sekä Liikenne- ja viestintäviraston määräykset**

[...]

*Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä:*

[...]

*6) 33 §:ssä säädettyistä vaatimustenmukaisuuden arviointielimen pätevyysvaatimuksista ottaen huomioon, mitä sähköisestä tunnistamisesta ja luottamuspalveluista annetussa EU:n asetuksessa säädetään;*

[...]

**Määräys M72B, 18 Tunnistuspalvelun ulkoisen arviointielimen vaatimukset**

**18.1 Osoittamismenettelyt**

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

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

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

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

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

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

**18.2 Pätevyys**

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

**Määräys M72B, 19 Tunnistuspalvelun sisäisen tarkastuslaitoksen vaatimukset**

**19.1 Riippumattomuus**

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

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

**19.2 Pätevyys**

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

**2.5 Arvioinnin toteuttaminen**

**2.5.1 Tarkastuskertomus: Arvioinnin ajankohta ja kesto henkilötyöaikana**

Arvioinnin ajankohta kerrotaan päivämäärinä ja kesto henkilötyöpäivinä tai tunteina. Tarkoitus on selvittää yleisellä tasolla arvioinnin ajantasaisuus ja perusteellisuus.

Arvioinnin kestolle ei aseteta vähimmäiskestoja. Arviointiin vaikuttavat monet eri seikat, jotka voivat pidentää tai lyhentää arviointiin käytettyä aikaa. Jos palvelun arvioinnissa voidaan hyväksilukea useita aiempia tai voimassa olevia arviointeja tai sertifikaatteja, arviointiin käytetty aika lyhenee. Arvioinnin tulee kattaa koko tunnustusjärjestelmä, ja kaikki tässä ohjeessa luetellut osa-alueet, ja mukana tulee olla myös tekniset näytteenotot tai arvioinnit.

**2.5.2 Tarkastuskertomus: Arviointimenetelmät**

Tarkastuskertomuksessa on kuvattava, mitä menetelmiä kunkin osa-alueen arvioinnissa on käytetty. Arvioinnissa käytettävien lähteiden määrälle ei ole tarkkoja vaatimuksia.

Arvioija ja tunnistuspalvelun tarjoaja harkitsevat itse, mistä lähteistä arviointi teetetään ja mitä osa-alueita verifioidaan useista lähteistä.

Kaikkien osa-alueiden arviointia ainoastaan kirjallisen dokumentaation perusteella ei voida pitää riittävänä. **Liikenne- ja viestintävirasto ei katso tarkastusmenetelmiä riittäväksi, jos tarkastuksessa ei ole miltään osin tehty teknistä havainnointia järjestelmän ulkopuolelta tai muutoin.**

Myöskään pelkkiä standardilistauksia tai -viittauksia ei voida pitää riittävänä.

**Jos arviointi perustuu toisen arviointielimen tekemään arviointiin, kyseiseen arviointiin ja sen tuloksiin täytyy perehtyä ja tarkastuskertomuksesta tulee ilmetä, minkä konkreettisten seikkojen perusteella palvelun vaatimustenmukaisuus on arvioitu** eli miten arvioija on perehtynyt näiden muiden arviointien materiaaliin ja arvioinut niiden laatua, kattavuutta ja niiden perusteella tehtyjä korjauksia ja korjausten aikataulua.

2.5.3 Tiedot dokumentaatiosta, jota on käytetty vaatimuksenmukaisuuden arvioinnissa

Tarkastuskertomuksessa on listattava, mitä palveluntarjoajan dokumentaatiota on arvioitu.

Kaikkea arviointiin liittyvää materiaalia ei ole tarpeen liittää Liikenne- ja viestintävirastolle toimitettavaan tarkastuskertomukseen. Virasto voi tarvittaessa pyytää toimittamaan tarkemman dokumentaation. Tiedonsaantioikeus perustuu tunnistus- ja luottamuspalvelulain 43 §:ään, jonka mukaan Liikenne- ja viestintävirastolla on oikeus salassapitosäynnösten estämättä saada tehtäviensä suorittamiseksi tarvittavat tiedot niiltä, joiden oikeuksista ja velvollisuuksista ko. laissa säädetään ja jotka toimivat näiden lukuun.

Arvioinnin yhteydessä laadittava dokumentaatio on säilytettävä vähintään tarkastuskertomuksen voimassaolon ajan. Lisäksi on otettava huomioon se, että sovellettavat menetelmät saattavat myös asettaa edellytyksiä dokumentaation säilyttämiselle ja säilytysajalle.

2.5.4 Tunnistusmenetelmän riskiarvio

Määräyksen M72B 6.1.1 kohdan mukaan suojautumiskyvyn on perustuttava riskiarvioon, jossa arvioidaan erikseen hallussapitoon, tietoon ja ominaisuuteen perustuviin todentamistekijöihin ja todentamismekanismiin kohdistuvat uhkat sekä uhkilta suojaavat turvatoimenpiteet.

Riskiarvion kohdalla voi käyttää hyväksi hyökkäyspotentiaalin laskemista esim. Common Criteria CCDB 2009 03 kappaleen 3 tai ETSI 102 165-1 kappaleen 6.6 ja 6.7 mukaisesti.

## 2.6 Arvioinnin suhteuttaminen varmuustasoon ja riskeihin

Vahvan sähköisen tunnistamisen luotettavuudelle on säädetty kaksi varmuustasoa, korotettu ja korkea.<sup>7</sup> Arviointikriteerien taulukoissa käytetään lyhenteitä S=korotettu (vastaa eIDAS2, substantial) ja H=korkea (vastaa eIDAS3, high).

Vaatimuksia on sääntelyssä monessa kohdassa eroteltu eri varmuustasoilla, mutta kaikissa vaatimuksissa näin ei ole tehty.

Yleinen varmuustasoja erottava vaatimus on se, miten hyvin tunnistusmenetelmä ja -järjestelmä suojaa tunnistusta erilaisia tietoturvariskejä ja uhkia vastaan. Koko

<sup>7</sup> EU:n varmuustasoasetuksessa määritellään vaatimukset myös matalalle varmuustasolle, mutta Suomen tunnistuslaissa sitä ei huomioida. eIDAS-asetuksen vastavuoroisuusvaatimukset eivät myöskään koske matalan varmuustason tunnistusmenetelmiä, vaan niiden huomioiminen on vapaaehtoista.

tunnistuspalvelun tarjoamisen ja tunnistusmenetelmän elinkaaren riskit ja uhkat on huomioitava. Korkealla varmuustasolla täytyy olla kaikilta osin kyky suojautua jo varsin edistynyttä hyökkäyspotentiaalia vastaan. Korotetullakin varmuustasolla hyökkäysten sietokyvyn täytyy olla erinomaisella tasolla.

Kriteeristöissä varmuustasoja käsitellään pääosin yhdessä. Jos korkean tason vaatimusta tai kriteeriä ei ole eritelty, yleinen arviointiohje korkealla varmuustasolla on arvioida tunnistuspalvelun suojautumiskykyä ja toimenpiteitä suhteessa korkeaan hyökkäyspotentiaaliin.

Kriteeristöjä voidaan tulevaisuudessa päivittää ja huomioida tarkemmin myös korkea varmuustaso, kun soveltamisesta saadaan kokemusta Suomessa ja kun eIDAS-sääntelyn vaatimusten tulkinnasta syntyy yhtenäisiä käytäntöjä Euroopassa.

Riskien ja uhkien tunnistaminen, niiden suunnitelmallinen hallinta, niihin valmistautuminen ja niiltä suojautuminen teknisillä ja organisatorisilla toimenpiteillä on turvallisuuden perusta.

**VRT.**

**LoA 2.3 Todentaminen**

*Tässä jaksossa käsitellään todentamismekanismin käyttöön liittyviä uhkia ja luetellaan vaatimukset kullekin varmuustasolle. Tässä jaksossa turvatoimenpiteet on ymmärrettävä suhteutettuina riskeihin kulloisellakin tasolla.*

**LoA guidance, kohta 2.3**

Todentamisvaiheessa käytetyillä todentamismekanismeilla ei voi estää täysin kaikkia hyökkäyksiä, vaan niillä voidaan vain vastustaa hyökkäyksiä tietyllä turvallisuus- tai varmuustasolla. Tavanomainen tapa mitata eri mekanismien tuottamaa sietokykyä on asettaa mekanismit järjestykseen sen mukaan, miten hyvin ne kestävät tietyn vakavuusasteen hyökkäyksiä (eli hyökkääjän voimaa).

Varmuustasossa eri vakavuusasteista käytettävät termit ovat "korkeampi perustaso" (enhanced-basic), "kohtuullinen" (moderate) ja "korkea" (high). Nämä termit on lainattu standardeista ISO/IEC 15408 "Information technology – Security techniques – Evaluation criteria for IT security" ja ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation". Standardien teksti on vapaasti luettavissa osoitteessa [www.commoncriteriaportal.org/cc](http://www.commoncriteriaportal.org/cc) (CCPART1-3 vastaa standardia ISO/IEC 15408 ja CEM standardia ISO/IEC 18045).

Standardissa ISO/IEC 15408-1 hyökkäyksen vakavuusaste määritellään sen työn määräksi, jota [mekanismia] vastaan hyökkääminen edellyttää, ilmaistuna hyökkääjän asiantuntemuksena, resursseina ja motivaationa.

Standardin ISO/IEC 18045 / CEM:n liitteessä B.4 ohjeistetaan, miten lasketaan todentamismekanismin tietyn heikkouden hyväksikäyttämisen edellyttämä hyökkäyksen vakavuusaste.

Täytäntöönpanoasetuksessa säädettyjen vaatimusten täyttäminen edellyttää mahdollisten hyökkäysten sietokyvyn arviointia.

Arvioinnissa olisi otettava huomioon asiaankuuluvat uhat. Standardissa ISO 29115 mainitaan esimerkiksi seuraavat: verkossa ja verkon ulkopuolella tapahtuva arvaaminen, tunnistetietojen toisintaminen, tietojen kalastelu, salakuuntelu, replay-hyökkäys, istuntokaappaus, mies välissä -hyökkäys, tunnistetietojen varastaminen, spoofing-hyökkäys ja toisena esiintyminen.

Hyökkäysten sietokyvyn arvioinnissa on syytä ottaa huomioon koko todentamismekanismi, myös sähköisen tunnistamisen menetelmän hallussapidon varmentamisesta aiheutuvat riskit.

[...]

Riskinarvioinnissa on otettava huomioon kohtuulliset oletukset sellaisten komponenttien turvallisuustasosta, joita todentamisjärjestelmä hyödyntää, mutta jotka eivät ole sen osia (esimerkiksi käyttäjän ympäristö, selain ja älypuhelin).

Komponentteja voidaan käyttää eri kokoonpanoissa ja eri suojausasetuksilla.

[...]

#### **LoA 2.4 Hallinto ja organisointi**

*Kaikilla osallistujilla, jotka tarjoavat sähköiseen tunnistamiseen liittyvää...palvelua (jäljempänä tässä liitteessä "palveluntarjoajat"), on oltava käytössä dokumentoidut tietoturvallisuuden hallintakäytännöt, toimintaperiaatteet, lähestymistavat riskien hallintaan ja muut hyväksytyt turvatoimenpiteet siten, että asiaankuuluvilla sähköisen tunnistamisen järjestelmien hallintoelimillä on kyseeseen tulevilla jäsenvaltioissa varmuus siitä, että tehokkaat menettelyt ovat käytössä. Kaikki 2.4 jakson vaatimukset/osatekijät on ymmärrettävä suhteutettuina riskeihin kulloisellakin tasolla.*

#### **LoA guidance, kohta 2.4**

[...]

Riskienhallinnassa yleisenä periaatteena on, että organisaation on itsensä valittava, minkä tasoista riskiä se pitää hyväksyttävänä. Kohdan 2.4 vaatimuksella muutetaan tätä yleistä periaatetta, sillä sen mukaan organisaation turvatoimenpiteiden on oltava suhteutettuja riskeihin kulloisellakin tasolla.

[...]

## **2.7 Tarkastuskertomuksen tarkkuus**

Tarkastuskertomuksesta tulee käydä ilmi, miten vaatimusten täytyminen on arvioitu.

**Tarkastuskertomuksessa tulee olla sanallinen kuvaus siitä, minkä käytännön seikkojen ja havaintojen perusteella kunkin vaatimuksen täytyminen on arvioitu ja todettu.**

Tarkastuskertomuksessa täytyy listata, mitä palveluntarjoajan dokumentaatiota on arvioitu kussakin kohdassa ja mitä menetelmiä on käytetty.

Tarkkoja tietoja edellytetään tarvittaessa erityisesti

- ✓ tietojen säilyttämisen/käsittelyn,
- ✓ teknisten toimenpiteiden,
- ✓ todentamismekanismin,
- ✓ tietoturvallisuuden hallintajärjestelmän ja
- ✓ tilaturvallisuuden arvioinnista.

Korkealla varmuustasolla edellytetään tarkempia tietoja kuin korotetulla varmuustasolla.

**Selvityksen täytyy kattaa myös alihankkijat.**

## 2.8 Poikkeamien raportointi tarkastuskertomuksessa

Vaatimuksenmukaisuuden arvioinnin yhteydessä löytyy tyypillisesti poikkeamia, joita korjataan arvioinnin aikana tai pian sen jälkeen.

Poikkeamien havaitseminen ja korjaaminen on olennainen osa tietoturvallisuuden ylläpidon ja hallinnan kyvykkyyttä, joten tarkastuskertomuksessa on hyvä antaa selvitystä poikkeamien havaitsemisesta ja korjaamisesta. Ne voi kuvata kunkin vaatimuksen kohdalla tai kootusti.

**Tämän ohjeen liitteenä on excel-muotoinen raportointitaulukko, jota on hyvä käyttää arvioinnin työkaluna ja havaintojen raportointivälineenä Liikenne- ja viestintävirastolle. Taulukossa on tarvittavat kohdat havainnoista raportoinnille ja korjaustoimenpiteistä ilmoittamiselle.**

**Jokaisen havaitun poikkeaman kohdalle kirjataan arvioijan toimenpideehdotus sekä tunnistuspalvelun tarjoajan suunnitelma korjauksesta ja korjaavista toimenpiteistä taikka kompensoivista toimenpiteistä.** Myös jo korjatuista poikkeamista tulee ilmoittaa, miten ne on korjattu.

Liikenne- ja viestintävirasto ei laadi poikkeamien vakavuusasteikkoa, vaan niiden arviointi jää tunnistuspalveluntarjoajan ja arvioijan välisen harkinnan varaan. Virasto tekee lopullisen arvion siitä, voidaanko poikkeamia hyväksyä niiden vähäisyyden, riittävän korjaussuunnitelman tai kompensoivien toimenpiteiden perusteella. Tarvittaessa virasto edellyttää korjaamaan havaitut poikkeamat.

## 2.9 Poikkeamien korjaus ja korjauksista raportointi

Kriittiset poikkeamat tulee korjata välittömästi ja korjaavat toimenpiteet tulee suorittaa 6 kuukauden kuluessa poikkeaman havaitsemisesta. Myös muista havaituista poikkeamista tulee ilmoittaa korjauksen aikataulu sekä korjaavat toimenpiteet.

**Korjaavat toimenpiteet tulee arvioida seuraavan arvioinnin yhteydessä, taikka jos kyse on kriittisestä poikkeamasta, viimeistään 6 kuukauden kuluessa** poikkeaman havaitsemisesta. Uusi arviointi toimitetaan Liikenne- ja viestintävirastolle sen valmistuttua.

## 3 Arvioitavat osa-alueet

Tässä kohdassa listataan arvioitavien osa-alueiden vaatimukset ja mahdolliset ohjeet arvioinnista ja raportoinnista tarkastuskertomuksessa.

Tunnistuspalvelun yleisessä arviointikriteeristössä noudatetaan tätä jaottelua. Tunnistuspalvelun yleinen arviointikriteeristö on ohjeen liitteenä B.

### 3.1 Tunnistusmenetelmän ominaispiirteet ja todentamismekanismi

Vaatimukset säädetään seuraavissa säännöksissä:

- TunnL 8 a § Tunnistusmenetelmässä käytettävät todentamistekijät
- LoA Liite 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu
- TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset. 1 mom. 3 kohta
- LoA Liite, 2.3.1 Todentamismekanismi
- LoA Liite, 2.4.6 Tekniset tarkastukset (controls), kohta 2
- M72B, 6 Tunnistusmenetelmän tietoturva-vaatimukset
- M72B, 7 Tunnistusjärjestelmän rajapintojen salausvaatimukset
- M72B, 8 Tietoliikenteen osapuolten varmentaminen
- M72B, 9 Tunnistussanomien eheys ja luottamuksellisuus

- LoA Liite, 1. Sovellettavat määritelmät
- 2) 'todentamistekijällä' tarkoitetaan tekijää, joka on vahvistettu henkilöön kytkeytyväksi ja joka kuuluu johonkin seuraavista luokista [...]
- 3) 'dynaamisella todentamisella' tarkoitetaan sähköistä prosessia, jossa käytetään salausta tai muita tekniikoita, joiden avulla voidaan pyynnöstä luoda sähköinen todiste siitä, että henkilöllä on hallinnassaan tai hallussaan tunnistetiedot, sekä muuttaa sitä jokaisessa uudessa henkilön ja hänen henkilöllisyytensä varmentavan järjestelmän välillä tapahtuvassa todentamisessa;

Tarkastuskertomuksesta täytyy ilmetä, miten on arvioitu tunnistusmenetelmän ominaispiirteitä ja todentamismekanismeja ja menetelmän kykyä suojata varmuustason edellyttämällä tasolla tietoturvaohjeilta ja -loukkauksilta.

Tunnistusmenetelmän ominaispiirteiden vaatimustenmukaisuus on tunnistusvälineen tarjoajan vastuulla.

Todentamismekanismin vaatimustenmukaisuus on myös tunnistusvälityspalvelun vastuulla, koska sen järjestelmä on mukana tunnistustapahtumien välittämisessä.

Määräyksen M72B 7 kohdan arvioinnista tulee toimittaa tarkastuskertomuksen lisäksi skannausraportti, josta näkyvät tunnistusjärjestelmän ulospäin tarjotun rajapinnan TLS- ja salausprofiilit.

### 3.2 Yhteentoimivuus

Vaatimukset säädetään seuraavissa säännöksissä:

- TunnL 12 a § Tunnistuspalvelun tarjoajien luottamusverkosto
- VNA 169/2016 Valtioneuvoston asetus vahvan sähköisen tunnistuspalvelun tarjoajien luottamusverkostosta, 1 § Luottamusverkoston tekniset rajapinnat
- M72B, 12 Luottamusverkostossa välitettävät vähimmäistiedot
- M72B, 14 Tiedonsiirrossa käytettävä protokolla ja muut vaatimukset

Tarkastuskertomuksesta täytyy ilmetä luottamusverkostossa tarjottavien rajapintojen ja tunnistusmenetelmällä tarjottavien attribuuttien (tunnistetietojen) arviointi. Tarkastuskertomuksesta täytyy ilmetä myös, miten on arvioitu valmiutta optionaalisten attribuuttien tarjoamiseen.

Attribuuttien arviointi koskee vain tunnistusmenetelmän tarjoajaa.

### 3.3 Tekniset tietoturva-vaatimukset

Vaatimuksia tarkastellaan tietoliikenne-, tietojärjestelmä- ja käyttöturvallisuuden kannalta.

Vaatimukset säädetään seuraavissa säännöksissä:

- TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset, 1 mom. 4 kohta
- LoA Liite, 2.3.1 Todentamismekanismi
- LoA Liite, 2.4.6 Tekniset tarkastukset (controls), kohdat 1, 2 ja 3
- M72B, 5 Tunnistusjärjestelmän tietoturva-vaatimukset

Tarkastuskertomuksesta täytyy ilmetä, miten on arvioitu tunnistusjärjestelmän suunnittelun, toteutuksen ja ylläpidon tietoliikenne-, tietojärjestelmä- ja käyttöturvallisuutta ja järjestelmän suojaamista teknisillä toimenpiteillä varmuustason edellyttämiltä kohtuullisten tai korkean tason tietoturvaohjeiden ja -loukkausten vaikutuksilta.

Tarkastuskertomuksesta täytyy ilmetä, millä perusteella on arvioitu, että alihankkijoiden toteuttamat osat tunnistusjärjestelmästä täyttävät vaatimukset.

Arvioinnissa ja tarkastuskertomuksessa on hyvä huomioida soveltuvin osin

- Tietoliikenneyhteydet
- Hallintayhteydet
- Tietoliikenneyhteysien vyöhykkeistäminen
- Tietoliikennelaitteet- ja järjestelmät
- Tuotanto-, ylläpito- ja hallinnointiverkkojen sekä kehitysympäristön eriyttäminen
- Suodattukset
- Yhteydet julkiseen verkkoon
- Tietojärjestelmien luokittelu
- Pääsyoikeudet ja käyttäjien tunnistus
- Vaaralliset työyhdistelmät
- Koverit
- Salauksratkaisut
- Kryptografisen materiaalin turvallisuus
- Etätyöasemien erityiset vaatimukset
- Haittaohjelmat
- Muutostenhallinta
- Ohjelmistohaavoittuvuudet
- Varmuuskopiointi

### 3.4 Poikkeamien havainnointikyky ja hallinta sekä häiriöilmoitukset

Vaatimukset säädetään seuraavissa säännöksissä:

- TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset, 1 mom. 4 kohta
- LoA Liite, 2.4.6 Tekniset tarkastukset (controls), kohdat 1 ja 4
- TunnL 16 § Tunnistuspalvelun tarjoajan velvollisuus ilmoittaa toimintaan ja tietojen suojaamiseen kohdistuvista uhkista tai häiriöistä
- M72B, 5 Tunnistusjärjestelmän tietoturva-vaatimukset
- M72B, 11 Tunnistuspalveluntarjoajan häiriöilmoitukset Liikenne- ja viestintävirastolle

Tarkastuskertomuksesta täytyy ilmetä, millä perusteella seuraavien asioiden on arvioitu täyttävän vaatimukset:

- ✓ poikkeamien havainnointikyky
- ✓ tapahtumalokien ja hallintalokien kerääminen
- ✓ monitorointi poikkeamien havaitsemiseksi
- ✓ poikkeamien vakavuusluokittelu ja suunnitelmallinen käsittely
- ✓ korjaustoimenpiteiden suunnitelmallisuus
- ✓ valmius täyttää häiriöilmoitusvelvollisuudet eri tahoille

### 3.5 Tietojen säilyttäminen ja käsittely

Vaatimukset säädetään seuraavissa säännöksissä:

- TunnL 13 § Tunnistuspalvelun tarjoajan yleiset velvollisuudet
- LoA Liite, 2.4.4 Tietojen säilyttäminen, kohdat 1 ja 2
- TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset, 1 mom. 4)
- LoA Liite, 2.4.6 Tekniset tarkastukset (controls), kohta 1 (huomaa korotetun ja korkean tason vaatimus arkaluonteinen salaustekninen aineiston suojaamisesta) ja kohta 5
- M72B, 5 Tunnistusjärjestelmän tietoturva-vaatimukset
- M72B, 7 Tunnistusjärjestelmän rajapintojen salausvaatimukset
- TunnL 24 § Tunnistustapahtumaa ja tunnistusvälinettä koskevien tietojen tallentaminen ja käyttö

Tarkastuskertomuksesta täytyy ilmetä, millä perusteella seuraavat asiat on arvioitu vaatimustenmukaiseksi:

- ✓ tunnistusjärjestelmään ja tunnistamiseen liittyvien tietojen luokittelu

- ✓ tietoon pääsyn hallinta
- ✓ tiedon keskittymisestä johtuva riski
- ✓ tietojen käsittelyn ja säilyttämisen turvallisuus (ml. salaukset)
- ✓ tietojen jäljitettävyyden ja palautettavuus
- ✓ tiedon elinkaaren hallinta mukaan lukien tiedon säilytysajat ja hävittäminen

### 3.6 Tilaturvallisuus

Vaatimukset säädetään seuraavissa säännöksissä:

- TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset, 1 mom. 4 kohta
- LoA Liite, 2.4.5 Tilat ja henkilökunta, kohdat 3 ja 4

Tarkastuskertomuksesta täytyy ilmetä havainnot, joiden perusteella tunnistusjärjestelmän turvallisuuteen vaikuttavien tilojen fyysinen turvallisuus ja valvonta on arvioitu vaatimustenmukaiseksi.

Arvioinnissa ja tarkastuskertomuksessa on hyvä huomioida soveltuvin osin:

- ✓ Suojautuminen ympäristötapauksilta (palo, lämpö, kaasu, pöly, värinä, vesi)
- ✓ Suojautuminen luvattomalta pääsylvä (murto)
- ✓ Sähkösaannin katkokset
- ✓ Suojautuminen ilkivallalta
- ✓ Vyöhykkeistäminen
- ✓ Rakenteellinen suojaus
- ✓ Kulunvalvonta
- ✓ Turvallisuusjärjestelmien laatu
- ✓ Luvattomat laitteet ja yhteydet

### 3.7 Riittävät ja pätevät henkilöresurssit

Vaatimukset säädetään seuraavissa säännöksissä:

- TunnL 13 § Tunnistuspäalvelun tarjoajan yleiset velvollisuudet
- LoA Liite, 2.4.5 Tilat ja henkilökunta, kohdat 1 ja 2

Tarkastuskertomuksesta täytyy ilmetä havainnot, joiden perusteella on arvioitu:

- ✓ henkilöresurssien operatiivinen riittävyys sähköisen tunnistuspäalvelun toiminnan luonteeseen nähden (24/7/365)
- ✓ tarpeellisten osa-alueiden osaamisesta (tekninen, oikeudellinen mm. henkilötietojen käsittelyn takia)
- ✓ alihankittujen palveluiden ja toimintojen (toimistojärjestelmät, käyttöpalvelut, ohjelmistot, infra...) riittävyys ja pätevyys

### 3.8 Tietoturvallisuuden hallinta

Vaatimukset säädetään seuraavissa säännöksissä:

- TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset, 1 mom. 5 kohta
- LoA Liite, 2.4 Hallinto ja organisointi, johdanto
- LoA Liite, 2.4.3 Tietoturvallisuuden hallinta
- LoA Liite, 2.4.7 Noudattaminen ja tarkastus
- M72B, 4 Tunnistuspäalvelun tarjoajan tietoturvallisuuden hallintajärjestelmä
- LoA Liite, 1. Sovellettavat määritelmät  
4. 'tietoturvallisuuden hallintajärjestelmällä' tarkoitetaan prosesseja ja menettelyjä, joiden tarkoituksena on pitää tietoturvaluuteen liittyvät riskit hyväksyttävällä tasolla.

Tarkastuskertomuksesta täytyy ilmetä, millä perusteella seuraavat asiat on arvioitu vaatimustenmukaiseksi:

- ✓ tunnistuspalvelun tarjoajan tietoturvallisuuden hallinta on kattavaa, johdonmukaista, organisoitua, suunnitelmallista ja jatkuvasti seurattua
- ✓ tunnistuspalvelun vaatimukset (TunnL, eIDAS LoA-asetus ja viraston määräys M72B) on huomioitu hallintajärjestelmässä
- ✓ alihankkijoiden tietoturvallisuuden hallinta täyttää vaatimukset

### 3.9 Tunnistusvälineen hakijan henkilöllisyyden todistaminen ja varmentaminen (ensitunnistaminen)

Vaatimukset säädetään seuraavissa säännöksissä:

- TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset, 1 mom. 1 ja 2 kohta
- TunnL 17 § Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen
- LoA Liite, 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)
- TunnL 7 b § Tieto passin tai henkilökortin voimassaolosta
- M72B, 6 Tunnistusmenetelmän tietoturvavaatimukset

Vaatimukset oikeushenkilön henkilöllisyyden todistamiselle ja varmentamiselle:

- TunnL 7 a § Yritys- ja yhteisörekisterien tietojen käyttäminen
- TunnL 17 a § Tunnistusvälineen hakijana olevan oikeushenkilön tunnistaminen
- LoA Liite, 2.1.3 Henkilöllisyyden todistaminen ja varmentaminen (oikeushenkilö)
- LoA, Liite 2.1.4 Luonnollisten ja oikeushenkilöiden sähköisen tunnistamisen menetelmien välinen kytkös
- LoA Liite, 1. Sovellettavat määritelmät  
1. 'luotettavalla lähteellä' tarkoitetaan mitä tahansa sellaista lähdettä muodosta riippumatta, josta voidaan luotettavasti saada paikkansapitäviä tietoja ja/tai todisteita, joita voidaan käyttää henkilöllisyyden todistamiseen;

Tarkastuskertomuksesta täytyy ilmetä, miten ja millä perusteella henkilön ensitunnistamismenettely tai -menettelyt on arvioitu vaatimustenmukaiseksi.

Mahdolliset ensitunnistusmenettelyt

- 1) Ensitunnistus perustuu Suomessa hyväksytyn henkilöllisyystodistuksen esittämiseen
- 2) Ensitunnistus sähköisellä tunnistusvälineellä
- 3) Ensitunnistus muuhun tarkoitukseen tehdyn tunnistamisen perusteella
- 4) Poliisin tekemä ensitunnistus
- 5) Etä[ensi]tunnistus esimerkiksi videoyhteyden tai valokuvasarjan sekä henkilöllisyystodistuksen etäluvun avulla

### 3.10 Huomioita henkilöllisyystodistuksen perusteella ensitunnistamisesta etäyhteydellä

**HUOM. Ohjeen valmisteluhetkellä ei ole vielä vakiintuneita tulkintoja siitä, millä edellytyksillä henkilöllisyystodistuksen esittäminen etäyhteydellä voi täyttää korotetun tai korkean varmuustason vaatimukset.**

Siksi ohjeeseen on koottu näkökohtia, joita toteutuksen riski- ja uhka-arvioissa ja suunnittelussa on syytä ottaa huomioon. Vahvalla sähköisellä tunnistusvälineellä voidaan asioida sähköisesti monenlaisissa palveluissa ja siksi tunnistusvälineiden myöntämiseen vain oikeille henkilöille on suhtauduttava tiukasti korotetulla varmuustasolla. Korkealla varmuustasolla on huomioitava suojautumiskyky korkean tason hyökkäyksiltä.

Oheen kootut huomiot eivät ole tyhjentävä luettelo, vaan esimerkkejä asioista, joita on ohjeen laatimisen hetkellä pohdittu.

Henkilöllisyystodistuksen (passin tai henkilökortin) esittämiseen perustuvassa ensitunnistamisessa on otettava huomioon mm.

- Henkilöllisyystodistusten aitouden varmistaminen
- Henkilöllisyystodistuksen esittäjän (ominaisuuksien) vertailu henkilöllisyystodistuksen tietoihin
  - o Todistuksessa olevan kasvokuvan ja todistuksen esittäjän kasvojen vertailu. Voidaan myös verrata allekirjoituksia; todistuksessa saattaa olla kuva allekirjoituksesta, pyydetään henkilöä kirjoittamaan nimensä.
- **Väestötietojärjestelmän käyttö**
- **Henkilöllisyystodistusten aitouden tai voimassaolon tarkistus käytävissä olevista tietokannoista**
- Jos henkilöllisyystodistuksen voi esittää etäyhteydellä, arvioinnissa on huomioitava perusteellisesti riskit ja suojakeinot, joilla suojaudutaan väärän henkilön esittämän tai väärennetyn henkilöllisyystodistuksen uhalta. Huomioon on otettava
  - o henkilöllisyystodistuksen aitoustekijöiden havainnointi ja
  - o henkilön itsestään toimittaman kuvan tai videon aitouden varmistaminen ja havainnointi.

#### **Näkökohtia etäensitunnistamisesta**

- Jos henkilöllisyystodistuksen voi esittää etäyhteydellä, arvioinnissa on huomioitava perusteellisesti riskit ja suojakeinot, joilla suojaudutaan väärän henkilön esittämän tai väärennetyn henkilöllisyystodistuksen uhalta.
- Huomioon on otettava henkilöllisyystodistuksen aitoustekijöiden havainnointi ja henkilön itsestään toimittaman kuvan tai videon aitouden varmistaminen ja havainnointi.
- Vain sirullista henkilöllisyystodistusta voidaan käyttää etäensitunnistamiseen myönnettäessä vahvaa sähköistä tunnistusvälinettä.
  - Henkilöllisyystodistusten aitoustekijät on suunniteltu tarkasteltavaksi paikan päällä ja esimerkiksi ultraviolettivalon avulla. Henkilöllisyyttä osoittavan asiakirjan aitoutta ei välttämättä olekaan mahdollista tarkastaa pelkän siitä lähetetyn kuvan perusteella riittävän luotettavasti, koska turvatekijät eivät välity kuvassa. Kuvasta pystyy lähinnä tarkistamaan, että kuvan asiakirjan asettelu on oikeanlainen.
  - Henkilöllisyystodistuksen sirun käyttäminen muuttaa tilannetta olennaisesti. Passiivinen todennus (Passive Authentication) eli allekirjoituksen tarkistaminen kertoo sen, että kyseinen tieto on peräisin aidolta asiakirjalta eikä tietoja ole muutettu. Kaikissa sirullisissa passeissa on olemassa tämä allekirjoitusominaisuus.
- Tiedot on kuitenkin voitu kopioida sirulta koska tahansa. Tietojen kopiointi ei vaadi erityistä hyökkäyspotentiaalia, koska lähtökohtaisesti sirulta saa lukea tiedot vapaasti lukuun ottamatta sormenjälkiä.
- Passeissa ja henkilökorteissa on myös mahdollisuus tehdä aktiivinen todennus tai siruntodennus, jonka avulla voidaan varmistua siitä, että siru on aito eikä tietoja ole kopioitu, eli aito asiakirja on etäyhteyden päässä juuri sillä hetkellä.

- Kun on varmistettu sirun ja sen sisältämien tietojen aitous ja kopioimattomuus, voidaan luottaa sirulta luettuun kasvokuvaan. Se on lähtökohtaisesti hyvälaatuinen ja huomattavasti isompi kuin pinnassa oleva kuva. Näin kuvatietaan voidaan luottaa ja parempilaatuisena se soveltuu paljon paremmin kasvovertailun tekemiseen etätunnistustapahtumassa välitettyyn kuvaan ja/tai videoon nähden.
- Sähköisen henkilöllisyystodistuksen sirulle ei välttämättä ole talletettu todistuksessa olevaa kasvokuvaa, jolloin sitä ei voida lukea sirulta ja hyödyntää henkilöä tunnistettaessa. Biometrisessä passissa kuva on talletettu sirulle.
- Tunnistuslain 7 §:n mukaan tunnistusvälineen tarjoajan on hankittava ja päivitettävä luonnollisen henkilön tunnistuspalvelun tarjoamiseksi tarvittavat tiedot väestötietojärjestelmästä. Tämän lisäksi tunnistuspalvelun tarjoajan on varmistettava, että sen tunnistuspalvelun tarjoamiseksi tarvittavat tiedot ovat ajan tasalla väestötietojärjestelmän tietojen kanssa.
- Tunnistuslain 7 b §:n mukaan tunnistuspalvelun tarjoajalla on oikeus saada sähköisesti poliisin tietojärjestelmässä oleva tieto ensitunnistamisessa käytettävän passin tai henkilökortin voimassaolosta.
- Jos on mahdollisuus käyttää myös muun maan vastaavia rekistereitä tai palveluita, joissa voi tarkistaa henkilöllisyystodistusten ja passien voimassaolon sekä henkilöllisyyden olemassaolon ja että henkilöllisyyden ilmoittaneella henkilöllä on tämä sama henkilöllisyys, voidaan niitä hyödyntää.
  - (Vrt. Varmuustasoaasetus 2.1.2 matala, kohta 3: luotettavan lähteen tiedossa on, että ilmoitettu henkilöllisyys on olemassa, ja voidaan olettaa, että henkilöllisyyden ilmoittaneella henkilöllä on tämä sama henkilöllisyys;
  - ja korotettu, kohta 2: henkilöllisyystodistus esitetään rekisteröintiprosessin aikana siinä jäsenvaltiossa, jossa todistus on myönnetty, ja todistus näyttää liittyvän sen esittäneeseen henkilöön ja on ryhdytty toimiin sen riskin minimoimiseksi, että henkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, että todistus on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt).
- Tilanne, jossa henkilöllisyyttä osoittavan asiakirjan tiedot eivät vastaa Väestötietojärjestelmän tietoja (esimerkiksi nimi tai hetu vaihtunut, tai esitettävä asiakirja on esimerkiksi toisen EU-maan myöntämä), tulee muin keinoin varmistua hakijan henkilöllisyydestä ja asiakirjan voimassaolosta.
- On tarpeen varmistaa se, että etäyhteydellä saatava tieto henkilöllisyystodistuksen esittäjästä on aitoa ja tulee henkilöllisyystodistuksen esittäjältä. Huomioon on otettava tietoliikenteen ja järjestelmän luotettavuus, riski lähetteen väärentämisestä tai henkilön ulkonäön muokkaamisesta tavalla, joka on vaikeasti havaittavissa etäyhteydellä. Lähtökohtaisesti vaatimuksena on, että videoyhteyttä käytetään mobiilisovelluksen kautta, sillä tietokoneen selaimen kautta tapahtuva videoyhteys voidaan helposti murtaa.
- Valaistusolosuhteet ja videon laatuvaatimukset tulee olla määritelty. Valaistuksen tulee olla hyvä ja mahdolliset artefaktit tulee havaita, sillä nämä ovat viitteitä mahdollisesta videomanipulaatiosta. Resoluution tulee olla

hyvä koko etäensitunnistustapahtuman ajan. Mikäli videossa esiintyy häiriöitä, on tunnistustapahtuma keskeytettävä ja aloitettava tarvittaessa uudestaan.

- Etätunnistustapahtumassa henkilöllisyystodistuksen esittävän henkilön elävyyden havainnointi edesauttaa mahdollisuutta varmistua siitä, että henkilöllisyystodistuksen esittäjä on paikalla esittämishetkellä eikä kysymyksessä ole väärennetty tallenne. Esimerkiksi henkilö tekee pyydetyt sattumanvaraiset eleet reaaliaikaisesti. Elävyyden havainnointiin voi käyttää eri tapoja, kuten sattumanvaraiset syötteet videoanalyysissä tai kuvasta havaitut biosignaalit. Elävyyden havainnointia varten tulee olla henkilöstölle riittävä koulutus ja kattavat ohjeet. Elävyyden havainnointi koneellisesti tulee perustua sattumanvaraisiin tapahtumiin tai pyyntöihin, jotka on kohdennettu etäensitunnista tekeväälle asiakkaalle.
- Etäyhteyden päässä olevan henkilön videolla havainnoitavien tai kuvana lähettämien ominaisuuksien vertaamisen henkilöllisyystodistuksesta saatuun vertailutietoon on pystyttävä tekemään luotettavasti (FAR-arvo).
- Siitä, miten tämä on luotettavasti mahdollista ei ole määrittelyjä. Etäyhteydellä tämä voi tarkoittaa periaatteessa joko ihmisen tekemää vertailua tai automaattista vertailua sähköisesti taustajärjestelmässä, johon on lähetetty molemmat kasvokuvat. Vertailukohtana luotettavuuden arvioinnissa voidaan pitää sitä, että tunnistuspalvelun työntekijä havainnoi paikan päällä henkilön ja henkilöllisyystodistuksen tietojen vastaavuuden ja pystyy havainnoimaan myös henkilöllisyystodistuksen esittäjän käyttäytymistä.
- On huomattava, että tietokoneen tekemä havainnointi on lähtökohtaisesti paljon luotettavampaa kuin ihmisen. Siten pelkkä virkailijan käyttö etätunnistaessa ei ole riittävää.

**Vrt. myös LoA guidance:**

*Luontaisissa todentamistekijöissä on syytä olla vaihtelua myös ominaisuuksiltaan samanlaisten ihmisten välillä, jotta henkilön yksilöinti on mahdollista; esimerkkejä ovat sormenjälki, kämmenjälki, kämmenen verisuonisto, kasvot, käden geometria ja silmän iiris.*

*Biometrisiä tekijöitä käytettäessä on tärkeää varmistaa, että henkilö, johon todentamistekijä liittyy, on varmentamispaikassa fyysisesti läsnä. Näin vähennetään huijausten tai toisintamisen vaaraa.*

**Näkökohtia sirun lukemista koskevasta lainsäädännöstä**

- Passilain 671/2006 5 a §:n mukaan passissa on jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijöitä ja biometriikkaa koskevista vaatimuksista annetussa neuvoston asetuksessa (EY) N:o 2252/2004 (EU:n passiasetus) tarkoitettu tekninen osa.

Tekniseen osaan talletetaan passinhaltijan kasvokuva sekä 6 a §:ssä tarkoitettut sormenjäljet tarvittavine lisätietoineen siten kuin EU:n passiasetuksessa säädetään. Tekniseen osaan voidaan tallettaa myös 5 §:n 1 momentissa tarkoitettut tiedot. Passinhaltijan oikeudesta tarkastaa passin tekniseen osaan hänestä talletetut tiedot säädetään EU:n passiasetuksessa.

Passin turvatekijöistä ja biometrisistä tunnisteista säädetään EU:n passiasetuksessa. Biometrisen tunnisteiden sisältävän passin kannessa on tätä osoittava tunnuskuva.

- Passilain 5 b §:n mukaan passin tekniseen osaan talletettuja sormenjälkiä saa lukea vain EU:n passiasetuksessa säädetyllä tavalla. Sormenjälkiä saavat lukea 10 §:ssä tarkoitettu passiviranomainen sekä poliisi- tai rajatarkastusviranomainen. [...]

Sormenjälkiä luettaessa passinhaltijan tietoja ei saa käsitellä muulla kuin EU:n passiasetuksessa ja tässä laissa säädetyllä tavalla.

Sen lisäksi, mitä tässä laissa säädetään sormenjälkien lukemisesta, noudatetaan yhteisön lainsäädäntöä ja Suomea sitovia kansainvälisiä sopimuksia.

- Passilaissa on samoin rajattu sormenjälkien lukeminen nimetyille viranomaisille, mutta kasvokuvan lukemista ei ole rajattu.
- Henkilökorttilain (663/2016) 5 a §:n mukaan henkilökortin tekniseen osaan talletetut sormenjäljet ja kasvokuvan saa lukea vain EU:n ID-asetuksessa säädetyllä tavalla. Sormenjälkiä saavat lukea 18 §:ssä tarkoitettu henkilökorttiviranomainen, poliisi ja Rajavartiolaitos. Lisäksi sormenjälkiä saa lukea Tulli silloin, kun se toimii esitutkintaviranomaisena tai hoitaa rajatarkastusviranomaisen tehtäviä. [...]
- Sormenjälkien luku on siis rajoitettu vain tietyille viranomaisille, mutta kasvokuvan lukemista ei laissa ole rajoitettu.
- EU:n ID-asetuksen (EU) 2019/1157 11 artiklan 6 kohdan mukaan henkilökorttien tallennusvälineeseen tallennettuja biometrisiä tietoja saa käyttää ainoastaan toimivaltaisten kansallisten viranomaisten ja unionin virastojen asianmukaisesti valtuutettu henkilöstö unionin oikeuden ja kansallisen lainsäädännön mukaisesti.

Asetuksen 22 resitaalin mukaan biometriset tunnisteet olisi kerättävä ja tallennettava henkilökorttien ja oleskeluasiakirjojen tallennusvälineeseen asiakirjan aitouden ja haltijan henkilöllisyyden todentamiseksi. Vain asianmukaisesti valtuutetun henkilöstön olisi tehtävä tällainen todentaminen, ja se olisi tehtävä ainoastaan, kun asiakirja on lain mukaan esitettävä. 19 resitaalin mukaan jäsenvaltioiden olisi yleisenä käytäntönä asiakirjan aitouden ja haltijan henkilöllisyyden todentamiseksi tarkastettava ensisijaisesti kasvokuva, ja kun se on tarpeen aitouden ja henkilöllisyyden varmistamiseksi, tarvittaessa myös sormenjäljet. 17 resitaalin mukaan turvaominaisuudet ovat tarpeen asiakirjan aitouden todentamiseksi ja henkilön henkilöllisyyden toteamiseksi. Turvallisuutta koskevien vähimmäisvaatimusten vahvistaminen ja biometrinen tietojen sisällyttäminen henkilökortteihin [...] ovat tärkeitä askelia tehtäessä niiden käytöstä unionissa turvallisempaa. Tällaisten **biometrinen tunnisteiden lisäämisen pitäisi mahdollistaa se, että unionin kansalaiset voivat täysimääräisesti hyödyntää oikeuttaan vapaaseen liikkuvuuteen.** Lisäksi erityisesti 15 resitaalin mukaan "Tämä **asetus ei vaikuta siihen, että jäsenvaltiot voivat käyttää muihin tarkoituksiin henkilökortteja** ja oleskeluasiakirjoja, jotka voidaan tunnistaa sähköisesti (eID), **eikä se vaikuta sääntöihin, jotka on vahvistettu Euroopan parlamentin ja neuvoston asetuksessa (EU) N:o 910/2014,** jossa säädetään unionin laajuisesta sähköisen tunnistamisen vastavuoroisesta tunnustamisesta, **kun on kyse julkisiin palveluihin pääsystä,** ja helpotetaan kansalaisten siirtymistä toiseen jäsenvaltioon edellyttämällä sähköisten tunnistamisen menetelmien vastavuoroista tunnustamista tietyin edellytyksin. **Parempien henkilökorttien avulla olisi parannettava henkilöllisyyden selvittämistä ja palvelujen saatavuutta.**"

- eIDAS asetuksen nojalla annetun komission täytäntöönpanoasetuksen (EU) 2015/1502 (LoA, varmuustasoasetus) liitteessä kohdassa 2.1.2 edellytetään varmuustasolla korkea, että **jos henkilöllä on** varmennettu olevan hallussaan sen jäsenvaltion hyväksymä valokuva tai **biometrinen tunnistus**, jossa sähköisen tunnistamisen menetelmää haetaan, ja kyseinen todiste edustaa ilmoitettua henkilöllisyyttä, **todiste tarkistetaan** sen määrittämiseksi, onko se luotettavan lähteen mukaan voimassa.
- Suurin osa henkilökorttien tiedoista on vapaasti luettavissa, mutta osa on estetty ilman oikeaa varmennetta. Estettyjä ovat erityisesti sormenjäljet, joiden lukeminen laissa on rajattu vain nimetyille viranomaisille. Kasvokuvan lukeminen ei yleensä ole estetty ja markkinoilla onkin paljon ilmaisia sovelluksia, joilla kasvokuvan voi lukea. (HUOM! Nämä eivät lähtökohtaisesti ole sellaisenaan käytettävissä tietoturvallisina menetelminä)
- Tietosuoja-asetuksen 9 artiklan 1 kohdan mukaan [...] biometrinen tietojen käsittely henkilön yksiselitteistä tunnistamista varten [...] on kiellettyä. Artiklan 2 kohdan g) alakohdan mukaan 1 kohdassa mainittujen tietojen käsittely on kuitenkin sallittua jäsenvaltion lainsäädännön nojalla, edellyttäen että se on oikeasuhteinen tavoitteeseen nähden, siinä noudatetaan keskeisiltä osin oikeutta henkilötietojen suojaan ja siinä säädetään asianmukaisista ja erityisistä toimenpiteistä rekisteröidyn perusoikeuksien ja etujen suojaamiseksi.
- Lähtökohtaisesti tilanteissa, joissa kasvokuva luettaisiin, voisi asiakas siitä kieltäytyä ja mennä sen sijaan tunnistautumaan henkilökohtaisesti. Asiakas voi myös hyväksyä kasvokuvan lukemisen niin halutessaan, ja hoitaa tunnistamisen silloin etäyhteydellä.
- European Banking Authority (EBA) on julkaissut ohjeen asiakkaan etätunnistamisesta (<https://www.eba.europa.eu/eba-publishes-guidelines-remote-customer-onboarding>).
  - Paragraph 35:  
"In situations where the device the customers use to prove their identity allows the collection of relevant data, for example because the data is contained in the chip of a national identity card, and it is technically feasible for the credit and financial institutions to access this data, credit and financial institutions should consider using this information to verify its consistency with the information obtained through other sources, such as the submitted data or other documents submitted by the customer. "
  - Paragraph 39:  
"Where the remote customer onboarding solution involves the use of biometric data to verify the customer's identity, credit and financial institutions should make sure that the biometric data is sufficiently unique to be unequivocally linked to a single natural person. [...]"
- EBA tulkitsee, että henkilöllisyystodistuksista voi ja kannattaa lukea mm. kasvokuva asiakkaan etätunnistustilanteessa.
- Liikenne- ja viestintävirasto nojautuu tulkinassaan EBA:n ohjeen suuntaan ja lisäksi siihen, että esimerkiksi EU:n ID-asetuksessa ei ole eIDAS-asetuksen soveltamista rajoitettu ja eIDAS-asetuksen nojalla annetussa varmuustasoasetuksessa biometrinen tietojen lukeminen mahdollistetaan. Näiden perusteella virasto toteaa, että kasvokuvan lukeminen henkilökortilta tai passista ei näyttäisi olevan lain mukaan kiellettyä ja varmuustasoasetuksen

perusteella olisi varmuustasolla korkea jopa edellytetty. Siten se on hyvä tapa mahdollistaa asiakkaan etätunnistaminen.

### 3.11 Tunnistusvälineen eli tunnistusmenetelmän elinkaari

Vaatimukset säädetään seuraavissa säännöksissä:

- Hakeminen ja rekisteröinti TunnL 7 § ja 20 §; M72B, 6.3
- Myöntäminen, toimittaminen, aktivointi TunnL 20 § ja 21 §; LoA Liite, 2.2.2
- Voimassaolon keskeyttäminen, peruuttaminen ja uudelleen aktivointi TunnL 25 § ja 26 § (LoA Liite, 2.2.3)
- Uusiminen ja korvaaminen, TunnL 22 §; LoA Liite, 2.2.4

Tarkastuskertomuksesta täytyy ilmetä, miten ja millä perusteella on arvioitu, että

- ✓ tunnistusvälineeseen liittyvät henkilötiedot ovat oikeat
- ✓ tunnistusvälineen toimittaminen, keskeyttäminen, peruuttaminen, uudelleen aktivointi, uusiminen ja korvaaminen on kokonaisuutena toteutettu niin, että tunnistusvälineen pysyminen oikealla haltijalla on varmistettu.

Liikenne- ja viestintävirasto on julkaissut joulukuussa 2018 neuvontamuiston<sup>8</sup>, jossa käsitellään henkilöllisyyden todentamista ylläpitotilanteissa.

### 3.12 Testaaminen

Tunnistusjärjestelmää ja sen komponentteja tulee testata kattavasti ja säännöllisesti. Jokainen muutos on testattava ennen tuotantoon viemistä. Erityisesti tulee testata myös negatiiviset testitapaukset, jolla pyritään estämään virheellisten tapahtumien syntyminen.

<sup>8</sup> Ks. Tulkintakannanotto Dnro: Traficom/106/09.02.00/2019 (25.3.2019) Liikenne- ja viestintäviraston tulkintamuistio ajokortin käyttämisestä henkilöllisyyden todentamisessa tunnistusvälineen lukkiutuessa tai uusittaessa tunnistusväline tai todentamistekijä. Kannanotto löytyy viraston verkkosivuilta <https://www.kyberturvallisuuskeskus.fi/fi/sahkoinen-tunnistaminen>

## **LIITE A: Tarkastuskertomusohjeen muistilista**

Tähän liitteeseen on koottu muistilista tarkastuskertomusohjeen sisällöstä. Suluissa on viittaus kohtaan, jossa asiaa käsitellään ohjeessa.

1. Arviointielimen yksilöinti- ja yhteystiedot (2.4.1)
  - 1) Yrityksen tai yhteisön nimi ja yksilöivä rekisterinumero tai -tunnus
  - 2) jos yritys tai yhteisö on sijoittunut muuhun ETA-alueen valtion kuin Suomeen, rekisteri, johon ulkomainen yhteisö tai yritys on merkitty
  - 3) postiosoite ja yhteyshenkilöt
  - 4) sähköpostiosoitteet Liikenne- ja viestintäviraston tiedusteluja varten
2. Arviointielimen pätevyys ja riippumattomuus (2.4.2)
  - Selvityksen voi antaa tarkastuskertomuksessa tai muutoin ilmoituksen yhteydessä
3. Arvioinnin ajankohta ja kesto henkilötyöaikana (2.5.1)
4. Arviointimenetelmät (2.5.2)
5. Tiedot dokumentaatiosta, jota on käytetty arvioinnissa (2.5.3)
6. Kuvaus siitä, minkä osan tunnistusmenetelmästä ja/tai tunnistusjärjestelmästä arviointi kattaa (2.3.3)
7. Arvioitavan tunnistuspalvelun nimi/nimet (2.3.4)
8. Tunnistusmenetelmän (tunnistusvälineen) kuvaus (2.3.5)
9. Tunnistusjärjestelmän kuvaus (järjestelmäarkkitehtuuri) (2.3.6)
10. Poikkeamat (2.8-2.9)
11. Tulokset osa-alueiden arvioinnista (3.1-3.12 soveltuvien osien)

## **Sähköisen tunnistuspalvelun arviointiohje**

Liikenne- ja viestintäviraston ohje

211/2023 O Liite C Mobiilikriteeristö

## LIITE B: Tunnistuspalvelun yleinen arviointikriteeristö

### B 1 Tunnistamisen menetelmän ominaispiirteet ja todentamismekanismi

#### KESKEISET SÄÄNNÖKSET

##### **M72B 15.1 Tunnistusjärjestelmän ja tunnistusmenetelmän arvioitavat toiminnot**

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

[...]

2) tunnistusmenetelmään eli tunnistusvälineen:

[...]

c) tunnistusmenetelmän ominaispiirteisiin ja laitimiseen;

[...]

g) todentamismekanismeihin.

##### **M72B 6 Tunnistusmenetelmän tietoturva-vaatimukset**

##### **6.1 Tunnistusjärjestelmän ominaispiirteet ja suojautumiskyky**

###### **6.1.1**

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

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

###### **6.1.2**

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

###### **6.1.3**

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

##### **6.2 Erityiset turvatoimenpiteet**

###### **6.2.1**

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

#### 6.2.2

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

#### 6.2.3

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

Tunnistuspalvelun on kertakirjautumisen suunnittelussa, toteutuksessa ja ylläpidossa huolehdittava kertakirjautumiseen liittyvien istuntojen keston, siirtämisen ja lopettamisen hallintaan perustuvista turvatoimenpiteistä sekä

### 6.3 Tunnistusvälineen kytkeminen henkilöön

#### 6.3.1

Tunnistusmenetelmän todentamistekijät on kytkettävä tunnistusjärjestelmässä tunnistusvälineen haltijaan.

#### 6.3.2

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

### 6.4 Tunnistusmenetelmän haltijakohtaisten tietojen käsittely

#### 6.4.1

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

#### 6.4.2

Tunnistuspalvelun tarjoaja ei saa kopioida tunnistusvälineeseen liittyviä salaisia tietoja.

| NRO | VARMUUS-TASO | TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ                                       | SÄÄNNÖKSET                                                                                                                                                                                                                                                                                                                                                         | STANDARDI-VIITTAUS                                             | HUOMIOITA                                                                                                                                                             |
|-----|--------------|---------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.  | S, H         | Tunnistusmenetelmästä on olemassa riskiarvio (hyökkäyspotentiaalin laskeminen). | <b>TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset</b><br>8.1 § 3) tunnistusmenetelmällä voidaan varmistua, että ainoastaan tunnistusvälineen haltija voi käyttää välinettä siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdissa 2.2.1 ja 2.3 vähintään korotetulle varmuustasolle säädetyt edellytykset täyttyvät; | ISO 29115<br><br>ISO/IEC 15408-1<br><br>ISO/IEC 18045, liite B | Esim. Common Criteria CCDB 2009 03, kappale 3, tai ETSI TS 102 165-1, kappale 6.6 ja 6.7 miten laskea hyökkäyspotentiaali. Riskiarvion asianmukainen toteuttaminen on |

|    |      |                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                           |                                                           |
|----|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|-----------------------------------------------------------|
|    |      |                                                                                       | <p><b>LoA Liite 2.3.1 Todentamismekanismi</b><br/>Todentamismekanismissa toteutetaan turvatoimenpiteitä sähköisen tunnistamisen menetelmän varmentamiseksi siten, että on erittäin epätodennäköistä, että viestin arvaaminen, salakuuntelu, toisto tai manipulointi hyökkäyksessä, jonka vakavuusaste on kohtuullinen ("moderate"), voi heikentää todentamismekanismeja.</p> <p><b>M72B 6.1.1</b><br/>Tunnistusmenetelmän todentamistekijät, todentamismekanismi ja turvatoimenpiteet on suunniteltava, toteutettava ja ylläpidettävä siten, että ne suojaavat tunnistusmenetelmän eheyden ja luotamuksellisuuden. 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 <b>riskiarvioon</b>, jossa arvioidaan erikseen hallussapitoon, tietoon ja ominaisuuteen perustuviin todentamistekijöihin ja todentamismekanismiin kohdistuvat uhkat sekä uhkilta suojaavat turvatoimenpiteet.</p> | <p>Common Criteria CCDB 2009 03, kapale 3</p> <p>ETSI TS 102 165-1, kapale 6.6 ja 6.7</p> | <p>peruslähtökohta hyökkäyspotentiaalin laskemiselle.</p> |
| 2. | S, H | <p>Tunnistusmenetelmässä käytetään vähintään kahta todentamistekijää eri luokista</p> | <p><b>TunnL 8 a § Tunnistusmenetelmässä käytettävät todentamistekijät</b><br/>[...]<br/>1) tiedossa oloon perustuvaa todentamistekijää, jonka henkilön on osoitettava olevan tiedossaan;<br/>2) hallussapitoon perustuvaa todentamistekijää, jonka henkilön on osoitettava olevan hallussaan;<br/>3) luontaista todentamistekijää, joka perustuu johonkin luonnollisen henkilön fyysiseen ominaisuuteen.<br/>[...]</p> <p><b>LoA Liite 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                           |                                                           |

|    |      |                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |                                                                                                                                                  |
|----|------|--------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--------------------------------------------------------------------------------------------------------------------------------------------------|
|    |      |                                                                                                                                | Sähköisen tunnistamisen menetelmässä käytetään vähintään kahta todentamistekijää eri luokista.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |  |                                                                                                                                                  |
| 3. | S, H | Todentamistekijät ovat toisistaan riippumattomia                                                                               | <p><b>LoA Liite 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu</b><br/>Sähköisen tunnistamisen menetelmä on suunniteltu siten, että sitä voidaan olettaa käytettävän vain, jos se on sen henkilön hallinnassa tai hallussa, jolle se kuuluu.</p> <p><b>M72B 6.1.2</b><br/>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.</p> |  | Todentamistekijöiden riippumattomuuteen toisistaan on syytä kiinnittää erityistä huomiota mobiililaitteella käytettävissä tunnistusmenetelmissä. |
| 4. | S, H | Tunnistusmenetelmän suunnittelussa on otettu huomioon se, että eri todentamistekijöihin kohdistuu erityyppisiä uhkia           | <p><b>LoA Liite 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu</b><br/>Sähköisen tunnistamisen menetelmä on suunniteltu siten, että sitä voidaan olettaa käytettävän vain, jos se on sen henkilön hallinnassa tai hallussa, jolle se kuuluu.</p> <p><b>M72B 6.1.2</b><br/>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.</p> |  |                                                                                                                                                  |
| 5. | S, H | Tunnistusmenetelmään liittyvät salaiset tiedot eivät tule tunnistuspalveluntarjoajan henkilökunnan tai alihankkijoiden tietoon | <p><b>M72B 6.4 Tunnistusmenetelmän haltijakohtaisten tietojen käsittely</b><br/>6.4.1<br/>Tunnistuspalvelun tarjoajan on varmistettava, etteivät tunnistusvälineeseen liittyvät salaiset tiedot paljastu sen henkilöstölle missään tilanteessa.</p>                                                                                                                                                                                                                                                                                                                                                                                       |  | Salaisia tietoja ovat tyypillisesti esimerkiksi PIN-koodit tai muut tietoon perustuvat todentamistekijät.                                        |

|    |      |                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |  |                                                                                                                                                                                                                                      |
|----|------|-------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |      |                                                                                                                   | 6.4.2<br>Tunnistuspalvelun tarjoaja ei saa kopioida tunnistusvälineeseen liittyviä salaisia tietoja.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |  | Vaatimuksen tarkoitus on huomioida tunnistuspalvelun vilpillisen henkilökunnan riski.                                                                                                                                                |
| 6. | S, H | Todentamistekijät on vahvistettu henkilöön liittyväksi                                                            | <p><b>LoA Liite 1 Sovellettavat määritelmät</b></p> <p>2) 'todentamistekijällä' tarkoitetaan tekijää, joka on vahvistettu henkilöön kytkettyväksi ja joka kuuluu johonkin seuraavista luokista [...]</p> <p><b>LoA Liite 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu</b></p> <p>Sähköisen tunnistamisen menetelmä on suunniteltu siten, että sitä voidaan olettaa käytettävän vain, jos se on sen henkilön hallinnassa tai hallussa, jolle se kuuluu.</p> <p><b>M72B 6.3 Tunnistusvälineen kytkeminen henkilöön</b></p> <p>6.3.1<br/>Tunnistusmenetelmän todentamistekijät on kytkettävä tunnistusjärjestelmässä tunnistusvälineen haltijaan.</p> <p>6.3.2<br/>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.</p> |  | Esimerkiksi tunnistussoveluksen kytkeminen henkilöön, sirun personointi, tunnuslukulistan tai laitteen kytkeminen henkilöön.                                                                                                         |
| 7. | S, H | Todentamismekanismi on suunniteltu siten, että jokaisella tunnistustapahtumalla on yksilöllinen sähköinen todiste | <p><b>TunnL 8 a § Tunnistusmenetelmässä käytettävät todentamistekijät</b></p> <p>[...] Jokaisessa tunnistusmenetelmässä on käytettävä sähköisen tunnistamisen varmuustasoa-<br/>tuksen liitteen kohdassa 2.3.1 tarkoitettua sel-<br/>laista dynaamista todentamista, joka <u>muuttuu jo-</u><br/><u>kaisessa</u> uudessa henkilön ja hänen henkilöllisyy-<br/>tensä varmentavan järjestelmän välillä tapahtu-<br/>vassa todentamistapahtumassa.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |  | <p>Myös tunnistusvälityspalvelu</p> <p>LoA guidance (otteita):<br/>Dynaamisen todentamisen ensisijainen tarkoitus on vähentää esimerkiksi mies välissä (Man in the Middle) -tyyppisten hyökkäysten vaaraa tai riskiä siitä, että</p> |

|    |      |                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----|------|--------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |      |                                                                                            | <p><b>LoA Liite 1 Sovellettavat määritelmät</b></p> <p>3) 'dynaamisella todentamisella' tarkoitetaan sähköistä prosessia, jossa käytetään salausta tai muita tekniikoita, joiden avulla voidaan pyynnöstä luoda sähköinen todiste siitä, että henkilöllä on hallinnassaan tai hallussaan tunnistetiedot, sekä muuttaa sitä jokaisessa uudessa henkilön ja hänen henkilöllisyytensä varmentavan järjestelmän välillä tapahtuvassa todentamisessa;</p> <p><b>LoA Liite 2.3.1 Todentamismekanismi</b></p> <p>Henkilön tunnistetietojen luovutusta edeltää sähköisen tunnistamisen menetelmän ja sen voimasaolon luotettava varmentaminen käyttämällä dynaamista todentamista.</p> |  | <p>aiemmin tallennetun todentamiskerran varmentamistietoja käytetään uudelleen.</p> <p>[...]</p> <p>On syytä muistaa, että useaan tekijään perustuva ja dynaaminen todentaminen eivät tarkoita samaa asiaa. Useaan tekijään perustuvassa todentamisessa ei edellytetä, että todentaminen tapahtuu dynaamisesti (esimerkkejä ovat PIN-koodi ja sormenjälkitiedot), joten tällainen todentamistapa voi olla alttiimpi replay-hyökkäykselle kuin dynaaminen todentaminen.</p> <p>[...]</p> <p>Jos henkilön yksityinen avain on tallennettu etäpalveluna (keskitetysti esimerkiksi tunnistustietojen tarjoajan käyttämälle HSM-laitteelle), yksityisen avaimen käyttämiseen vaadittavan todentamistavan on myös oltava dynaaminen.</p> |
| 8. | S, H | Tunnistustapahtuman sähköinen todiste perustuu henkilöön liitettyihin todentamistekijöihin | <p><b>LoA Liite 1 Sovellettavat määritelmät</b></p> <p>3) 'dynaamisella todentamisella' tarkoitetaan sähköistä prosessia, jossa käytetään salausta tai muita tekniikoita, joiden avulla voidaan pyynnöstä luoda sähköinen todiste siitä, että henkilöllä on hallinnassaan tai hallussaan tunnistetiedot, sekä muuttaa sitä jokaisessa uudessa henkilön ja hänen henkilöllisyytensä varmentavan järjestelmän välillä tapahtuvassa todentamisessa;</p>                                                                                                                                                                                                                           |  | Todentamistekijät eivät saa olla kopioitavissa.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|    |   |                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----|---|--------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |   |                                                                                                  | <p><b>M72B 6.3 Tunnistusvälineen kytkeminen henkilöön</b><br/>6.3.1<br/>Tunnistusmenetelmän todentamistekijät on kytkettävä tunnistusjärjestelmässä tunnistusvälineen haltijaan.</p> <p><b>LoA liite 2.3.1 Todentamismekanismi</b><br/>Korotettu:<br/>1. Henkilön tunnistetietojen luovutusta edeltää sähköisen tunnistamisen menetelmän ja sen voimassaolon luotettava varmentaminen käyttämällä dynaamista todentamista.<br/>2. Todentamismekanismeissa toteutetaan turvatoimenpiteitä sähköisen tunnistamisen menetelmän varmentamiseksi siten, että on erittäin epätodennäköistä, että viestin arvaaminen, salakuuntelu, toisto tai manipulointi hyökkäyksessä, jonka vakavuusaste on kohtuullinen ("moderate"), voi heikentää todentamismekanismeja.</p> |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 9. | H | Käyttäjä voi suojata menetelmän (välineen) ja todentamistekijänsä luotettavasti muiden käytöltä. | <p><b>LoA Liite 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu</b><br/>Sähköisen tunnistamisen menetelmä on suunniteltu niin, että henkilö, jolle se kuuluu, voi suojata sen luotettavasti muiden käytöltä.</p> <p>Myös <b>LoA Liite 2.2.2 Myöntäminen, toimittaminen ja aktivointi</b><br/>Aktivointiprosessi varmistaa, että sähköisen tunnistamisen menetelmä on toimitettu vain sen henkilön haltuun, jolle se kuuluu.</p> <p><b>M72B 6.1 Tunnistusmenetelmän ominaispiirteet ja suojautumiskyky</b><br/>6.1.1<br/>Tunnistusmenetelmän todentamistekijät, todentamismekanismi ja turvatoimenpiteet on suunniteltava, toteutettava ja ylläpidettävä siten, että ne</p>                                                           |  | <p>Esimerkkejä LoA-guidance:<br/>"Luotettava suojaaminen" tarkoittaa toimenpiteitä, joiden avulla sähköisen tunnistamisen menetelmä voidaan suojata niin, ettei sitä voi käyttää henkilön tietämättä ja ilman hänen aktiivista suostumustaan. Esimerkiksi salausavaintunnisteen yksityinen avain ei voi olla sellainen, jota voidaan käyttää koneellisissa prosesseissa ilman käyttäjän aktiivista suostumusta (kuten PIN-koodin antamista).</p> |

|  |  |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--|--|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  |  | <p>suojaavat tunnistusmenetelmän eheyden ja luotamuksellisuuden. Tunnistusmenetelmällä on oltava suojautumiskyky vähintään tunnistuspalvelun varmuustason mukaista sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.3 tarkoitettua kohtuullisen tai korkean vakavuustason uhkaa ja hyökkäyspotentiaalia vastaan. [...]</p> <p>6.1.2<br/>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.</p> <p><b>M72B 6.4 Tunnistusmenetelmän haltijakoh-<br/>taisten tietojen käsittely</b></p> <p>6.4.1<br/>Tunnistuspalvelun tarjoajan on varmistettava, etteivät tunnistusvälineeseen liittyvät salaiset tiedot paljastu sen henkilöstölle missään tilanteessa.</p> <p>6.4.2<br/>Tunnistuspalvelun tarjoaja ei saa kopioida tunnistusvälineeseen liittyviä salaisia tietoja.</p> |  | <p>Tällä vaatimuksella suojaudutaan toisintamisen, arvaamisen, toiston ja viestinnän väärentämisen muodostamilta uhilta.</p> <p>Edellä mainittujen teknikkoiden lisäksi (ks. Myös LoA-guidance kohta 2.2.1 korkea 1) voidaan käyttää myös seuraavia:</p> <ul style="list-style-type: none"> <li>- Vahvat staattiset salasana-</li> <li>- Käyttäjän biometrinen varmentaminen,</li> <li>- Ympäristön tarkistaminen haitallisen koodin varalta,</li> <li>- Kaistan ulkopuolella tapahtuva varmentaminen,</li> <li>- Kaikkien salassa pitämi-</li> </ul> <p>seen perustuvien todentamistekijöiden (staattiset salasanat, laitteiston kertakäyttöiset salasanat) osalta arvaaminen muodostaa uhan, jota on syytä lieventää korkean varmuustason saavuttamiseksi esimerkiksi rajaamalla yritysten määrää tai käyttämällä hidastusmekanismeja sekä huolehtimalla riittävästä entropiasta.</p> <p>LoA-guidance kohta 2.2.2 korkea: Tasolla "korkea" aktivointiprosessilla on varmistettava, että vain</p> |
|--|--|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|  |  |  |  |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--|--|--|--|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  |  |  |  | <p>laillinen omistaja voi akti-voida sähköisen tunnistamisen menetelmän ja että aktivointiprosessi on suojattu vahingossa tapahtuvasta häviämiseltä sekä sisäpiiriuhilta, kuten vilpilliseltä yhteistyöltä.</p> <p>HUOM! Käyttäjän tulee voida varmistua, etteivät turvatekijät, tai esimerkiksi tunnistusvälineeseen liittyvä resetointikoodi voi olla muiden saatavilla. Mahdollinen aktivointi- tai resetointikoodi ovat kertakäyttöisiä.</p> <p>Tällä varmistetaan, ettei uudelleen käytettävällä aktivointikoodilla voida mitätöidä eli ylikirjoittaa vain käyttäjän tiedossa olevaa todentamistekijää (PIN) tämän tietämättä. Tunnistusraissa ei ole viittausta LoA kohtaan 2.2.3 ("Käytössä ovat toimenpiteet, joilla estetään voimassaolon luvaton keskeyttäminen, peruuttaminen ja/tai uudelleenaktivointi.") Koodin kertakäyttöisyys on kuitenkin hyvä käytäntö, jollei muin tavoin voida suojata tunnistusvälineen luvaton uudelleenaktivointia.</p> |
|--|--|--|--|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|     |      |                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                          |                                                                                                                                                  |
|-----|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| 10. | S, H | Tunnistetietoja ei luovuteta luotavalle osapuolelle eli tunnistustapahtumaa ei toteuteta ennen kuin tunnistusväline/metelmä on varmennettu dynaamisella todentamisella | <b>LoA Liite 2.3.1 Todentamismekanismi</b><br>Henkilön tunnistetietojen luovutusta edeltää sähköisen tunnistamisen menetelmän ja sen voimaolon luotettava varmentaminen käyttämällä dynaamista todentamista.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | A.14.1 Järjestelmien hankkiminen, kehittäminen ja ylläpito/Tietojärjestelmiä koskevat turvallisuusvaatimukset<br>A.14.1.2 sovelluspalvelutapahtumien suojaaminen julkisissa verkoissa<br>A.14.1.3 sovelluspalvelutapahtumien suojaaminen | Myös tunnistusvälityspalvelu                                                                                                                     |
| 11. | S, H | Tunnistustapahtumassa tallentuvat tunnistetiedot (henkilötiedot) suojataan                                                                                             | <b>LoA Liite 2.3.1 Todentamismekanismi</b><br>Jos henkilön tunnistetiedot tallennetaan osana todentamismekanismia, nämä tiedot on suojattu niiden menetykseltä ja vaarantamiselta, mukaan lukien analyysi verkkoympäristön ulkopuolella.<br><br><b>M72B 7.1 Tietoliikenteen salausmenetelmät</b><br>7.1.1<br>Tunnistuspalvelun tarjoajien välisten ja tunnistuspalvelun tarjoajan ja luottavan osapuolen välisten rajapintojen liikenne on salattava. [kts. menetelmät määräyksestä tai jäljempänä]<br><br><b>M72B 9.1 Sanomien suojaaminen tunnistuspalveluiden ja luottavan osapuolen välillä</b><br>9.1.1<br>Tunnistuspalveluiden välisessä ja tunnistuspalvelun ja luottavan osapuolen välisessä tietoliikenteessä on <b>suojattava henkilötietoja sisältävien tunnistussanomien eheys ja luottamuksellisuus</b> joko: |                                                                                                                                                                                                                                          | Myös tunnistusvälityspalvelu<br><br>Huomioitava kaikki tunnistustapahtumaan osallistuvien tekniset ympäristöt, joissa tunnistetietoja tallentuu. |

|     |   |                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----|---|--------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |   |                                                                                                  | <p>a) varmistamalla tietoliikenneyhteyden eheys ja luottamuksellisuus sitomalla osapuolten tietoliikenne 8 kohdan mukaisesti toimittuihin varmenteisiin tai avaimiin; tai</p> <p>b) salaamalla ja allekirjoittamalla sanomat 8 kohdan mukaisella menettelyllä toimitettulla avaimella.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 12. | S | Todentamismekanismin turvatoimenpiteet suojaavat vakavuusasteeltaan kohtuulliselta hyökkäykseltä | <p><b>TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset</b></p> <p>8.1 § 3) tunnistusmenetelmällä voidaan varmistua, että ainoastaan tunnistusvälineen haltija voi käyttää välinettä siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdissa 2.2.1 ja 2.3 vähintään korotetulle varmuustasolle säädetyt edellytykset täyttyvät;</p> <p><b>LoA Liite 2.3.1 Todentamismekanismi</b></p> <p>Todentamismekanismissa toteutetaan turvatoimenpiteitä sähköisen tunnistamisen menetelmän varmentamiseksi siten, että on erittäin epätodennäköistä, että viestin arvaaminen, salakuuntelu, toisto tai manipulointi hyökkäyksessä, jonka vakavuusaste on kohtuullinen ("moderate"), voi heikentää todentamismekanismeja.</p> | <p>ISO 29115</p> <p>ISO/IEC 15408-1</p> <p>ISO/IEC 18045, liite B</p> <p>Common Criteria CCDB 2009 03, kapale 3</p> <p>ETSI TS 102 165-1, kapale 6.6 ja 6.7</p> | <p>Vrt. kriteeri 1 riskiarvio ja hyökkäyspotentiaalin laskeminen</p> <p>Arvioinnissa olisi otettava huomioon asiaankuuluvat uhat. Standardissa ISO 29115 mainitaan esimerkiksi seuraavat: verkossa ja verkon ulkopuolella tapahtuva arvaaminen, tunnistetietojen toisintaminen, tietojen kalastelu, salakuuntelu, replay-hyökkäys, istuntokaappaus, mies välissä -hyökkäys, tunnistetietojen varastaminen, spoofing-hyökkäys ja toisena esiintyminen.</p> <p>Standardissa ISO/IEC 15408-1 hyökkäyksen vakavuusaste määritellään sen työn määräksi, jota [mekanismia] vastaan hyökkääminen edellyttää, ilmaistuna hyökkääjän asiantuntemuksena, resursseina ja motivaationa.</p> <p>Standardin ISO/IEC 18045 / CEM:n liitteessä B.4 ohjeistetaan, miten lasketaan</p> |

|     |   |                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |          |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----|---|-------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |   |                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |          | <p>todentamismekanismin tietyn heikkouden hyväksikäyttämisen edellyttämä hyökkäyksen vakavuusaste.</p> <p>Common Criteria ja ETSI 102 165-1 sisältävät ohjeita hyökkäyspotentiaalin laskemiselle.</p> <p>Todentamismekanismissa on huomioitava myös uhka väärän asiointipalvelun käynnistämästä tunnistuspyynnöstä tai kaappamasta tunnistusistunnosta (phishing).</p> <p>Ks. LoA guidance kohdan 2.3.1 kuvaus</p> <p>Myös tunnistusvälityspalvelu</p> |
| 13. | H | Todentamismekanismin turvatoimenpiteet suojaavat vakavuusasteeltaan korkean tason hyökkäykseltä | <p><b>TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset</b></p> <p>8.1 § 3) tunnistusmenetelmällä voidaan varmistua, että ainoastaan tunnistusvälineen haltija voi käyttää välinettä siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdissa 2.2.1 ja 2.3 vähintään korotetulle varmuustasolle säädetyt edellytykset täyttyvät;</p> <p><b>LoA Liite 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu</b></p> <p>Sähköisen tunnistamisen menetelmä on suojattu toisintamiselta ja väärentämiseltä sekä hyökkäyksiltä, joiden vakavuusaste on korkea ("high").</p> <p><b>LoA Liite 2.3.1 Todentamismekanismi</b></p> | ks. yllä | <p>Myös tunnistusvälityspalvelu</p> <p>Kaikki todentamismekanismiin liittyvät turvallisuusseikat suhteutettuna korkean vakavuustason hyökkäyspotentiaaliin.</p>                                                                                                                                                                                                                                                                                        |

|     |      |                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                              |                              |
|-----|------|---------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|------------------------------|
|     |      |                                                                                                                                                   | Todentamismekanismeissa toteutetaan turvatoimenpiteitä sähköisen tunnistamisen menetelmän varmentamiseksi siten, että on erittäin epätodennäköistä, että viestin arvaaminen, salakuuntelu, toisto tai manipulointi hyökkäyksessä, jonka vakavuusaste on korkea ("high"), voi heikentää todentamismekanismeja.                                                                                                                                                                                                         |                                                                                                                              |                              |
| 14. | S, H | Todentamismekanismi näyttää asiointipalvelun nimen niissä välineissä ja tunnistusprosessin vaiheissa, missä se on mahdollista                     | <p><b>M72B 6.2.2</b> Tunnistuspalvelun on näytettävä tunnistusvälineen käyttäjälle tunnistustapahtumassa tieto luottavasta osapuolesta, jolle tunnistus välitetään. Tiedon näyttäminen on pakollista sellaisessa tunnistusmenetelmässä, jossa se on teknisesti mahdollista.</p> <p><b>M72B 12.1 Pakolliset tiedot</b><br/>Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on välitettävä:<br/>[...]4) tunnistusvälityspalvelun varmistama tieto luottavasta osapuolesta.</p> |                                                                                                                              | Myös tunnistusvälityspalvelu |
| 15. | S, H | Todentamismekanismi näyttää istuntotunnisteen niissä välineissä ja tunnistusprosessin vaiheissa, missä se on mahdollista                          | <b>M72B 6.2.1</b> Tunnistuspalvelun on näytettävä tunnistusvälineen käyttäjälle tunnistustapahtumassa tieto, jonka perusteella käyttäjä voi varmistaa, että tunnistusvälineeseen käyttäjän saama tunnistuspyyntö liittyy käyttäjän omaan asiointitapahtumaan. Tiedon näyttäminen on pakollista sellaisessa tunnistusmenetelmässä, jossa se on teknisesti mahdollista.                                                                                                                                                 |                                                                                                                              | Myös tunnistusvälityspalvelu |
| 16. | S, H | Todentamismekanismeissa noudatetaan pakollisia salausvaatimuksia <b>tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välillä</b> | <p><b>LoA Liite 2.4.6 Tekniset tarkastukset</b> (controls)<br/>2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät <u>sähköisen viestinnän kanavat on suojattu</u> salakuuntelulta, manipuloinnilta ja toistolta.</p> <p><b>M72B 7.1 Tunnistusjärjestelmän rajapintojen salausvaatimukset</b><br/><u>7.1.1</u><br/><u>Tunnistuspalvelun tarjoajien välisten ja tunnistuspalvelun tarjoajan ja luottavan osapuolen välisten</u></p>                                                           | <p>A.10.1.1 salauksen käytön periaatteet</p> <p>A.13.2.3 viestintäturvallisuus/tietojen siirtäminen: sähköinen viestintä</p> | Myös tunnistusvälityspalvelu |

|  |  |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |  |  |
|--|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
|  |  |  | <p><u>raajapintojen liikenne on salattava.</u> Salauksessa, avaintenvaihdossa, varmenteissa sekä salaukseen liittyvässä allekirjoituksessa on noudatettava seuraavia menetelmiä:</p> <ol style="list-style-type: none"> <li>1) Avaintenvaihto: Avaintenvaihdossa on käytettävä DHE-menetelmiä tai elliptisiä käyriä käyttäviä ECDHE-menetelmiä. Las-kutoimituksissa käytetyn äärellisen kunnan (finite field) koon tulee olla DHE-menetelmässä vähintään 2048 bittiä ja ECDHE-menetelmässä vähintään 224 bittiä.</li> <li>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.</li> <li>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.</li> <li>4) Tiivistefunktiot: Tiivistefunktion tai autentikaatiokoodin on oltava SHA-2, SHA-3, Whirlpool tai Poly1305.</li> </ol> <p>7.1.2<br/>Kohdassa 7.1.1 mainittujen lisäksi voidaan noudattaa menetelmiä ja arvoja, jotka on arvioitu turvallisiksi 1-4 alakohdissa tarkoitettuun käyttöön seuraavien asiakirjojen ajantasaisissa versioissa:</p> <ol style="list-style-type: none"> <li>a) Liikenne- ja viestintävirastossa toimivan salaustuotteiden hyväksyntäviranomaisen (Crypto Approval Authority) ohje Kryptografiset vahvuusvaatimukset luottamuk-sellisuuden suojaamiseen - kansalliset turvallisuuksluokat (Dnro 190/651/2015); tai</li> </ol> |  |  |
|--|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|

|  |  |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |  |  |
|--|--|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
|  |  |  | <p>b) eräiden Euroopan unionin tai ETA-alueen jäsenvaltioissa toimivien sertifiointielinten välisen SOGIS-MRA (Senior Officers Group for Information Systems, Mutual Recognition Agreement) asiakirja SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms.</p> <p>7.1.3<br/><u>Salausasetukset tulee teknisesti pakottaa edellä luoteltuihin vähimmäistasoihin, jotta yhteyskäte-lyissä ei päädyttäisi vähimmäistasoja heikompiin asetuksiin.</u></p> <p><b>7.2 Tietoliikenteen salausprotokolla</b><br/>Mikäli yhteyskäytännössä käytetään TLS-protokol-<br/>laa, tulee käyttää vähintään TLS versiota 1.2.<br/><u>Henkilötietoja sisältävien sanomien eheys ja luot-<br/>tamuksellisuus on suojattava edellä 1 momentissa<br/>tarkoitettun liikenteen salauksen lisäksi sanomata-<br/>solla 1 momentin mukaisesti.</u></p> <p><b>M72B 8 Tietoliikenteen osapuolten varmen-<br/>taminen</b><br/><b>8.1 Tietoliikenneyhteyden osapuolten tunnis-<br/>taminen</b><br/>Tunnistuspalveluiden välisessä sekä tunnistuspal-<br/>velun ja luottavan osapuolen välisessä tietoliiken-<br/>neyhteyden perustamisessa on todennettava tie-<br/>toliikenteen tai sanomien salaamisessa käytettä-<br/>vien varmenteiden ja avainten aitous ja eheys<br/>sekä niiden haltijat.<br/>Todentamisen on perustuttava eIDAS-asetuksen<br/>mukaiseen hyväksytyyn sähköiseen allekirjoituk-<br/>seen tai hyväksytyyn sähköiseen leimaan taikka<br/>suoraan kahdenväliseen menettelyyn. Todentami-<br/>nen ei voi perustua pelkästään yleisesti luotettuun<br/>varmenteeseen.</p> <p><b>8.2 Varmenteiden ja avainten uusiminen</b></p> |  |  |
|--|--|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|

|  |  |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |  |
|--|--|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
|  |  |  | <p>Edellä 8.1 kohdassa tarkoitetut varmenteet ja avaimet on uusittava säännöllisesti. Uusien varmenteiden ja avainten aitouden ja eheyden varmistamiseksi uusiminen on tehtävä joko:</p> <ul style="list-style-type: none"> <li>a) 8.1 kohdan mukaisella menettelyllä;</li> <li>b) toimittamalla uudet avaimet tietoliikenneyhteydellä, jonka eheys ja luottamuksellisuus on varmistettu sitomalla osapuolten tietoliikenne 8.1 kohdan mukaisesti toimitettuihin varmenteisiin tai avaimiin; tai</li> <li>c) allekirjoittamalla uusi avain 8.1 kohdan mukaisesti toimitetulla avaimella tai sellaisesta ketjutetulla avaimella.</li> </ul> <p><b>M72B 9 Tunnistussanomien eheys ja luottamuksellisuus</b></p> <p><b>9.1 Sanomien suojaaminen tunnistuspalveluiden ja luottavan osapuolen välillä</b></p> <p>9.1.1<br/>Tunnistuspalveluiden välisessä ja tunnistuspalvelun ja luottavan osapuolen välisessä tietoliikenteessä on suojattava henkilötietoja sisältävien tunnistussanomien eheys ja luottamuksellisuus joko:</p> <ul style="list-style-type: none"> <li>a) varmistamalla tietoliikenneyhteyden eheys ja luottamuksellisuus sitomalla osapuolten tietoliikenne 8 kohdan mukaisesti toimitettuihin varmenteisiin tai avaimiin; tai</li> <li>b) salaamalla ja allekirjoittamalla sanomat 8 kohdan mukaisella menettelyllä toimitetulla avaimella.</li> </ul> <p>9.1.2<br/>Tunnistusvälityspalvelun ja luottavan osapuolen välisessä tietoliikenteessä tunnistussanomien on todennettava allekirjoittamalla.</p> |  |  |
|--|--|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|

|     |      |                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                     |                                    |
|-----|------|----------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
|     |      |                                                                                                                      | <p><b>9.2 Sanomien suojaaminen käyttäjärajapinnassa</b><br/>Jos tunnistussanomien välitetään käyttäjän selaimen tai päätelaitteen kautta, sanomat on salattava ja allekirjoitettava 9.1.1.b) alakohdan mukaisesti.</p> <p><b>9.3 Salausalgoritmit ja menettelyt</b><br/>Sanomien salaamisessa ja allekirjoittamisessa on käytettävä soveltuvin osin 7.1 kohdan mukaisia menettelyjä.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                     |                                    |
| 17. | S, H | Todentamismekanismissa noudatetaan pakollisia salausvaatimuksia <b>tunnistuspalvelun ja asiointipalvelun välillä</b> | <p><b>LoA Liite 2.4.6 Tekniset tarkastukset</b> (controls)<br/>2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät <u>sähköisen viestinnän kanavat on suojattu</u> salakuuntelulta, manipuloinnilta ja toistolta.</p> <p><b>M72B 7-8 (yllä)</b></p> <p><b>M72B 9 Tunnistussanomien eheys ja luottamuksellisuus</b><br/><b>9.1 Sanomien suojaaminen tunnistuspalveluiden ja luottavan osapuolen välillä</b><br/>9.1.1<br/>Tunnistuspalveluiden välisessä ja tunnistuspalvelun ja luottavan osapuolen välisessä tietoliikenteessä on suojattava henkilötietoja sisältävien tunnistussanomien eheys ja luottamuksellisuus joko:<br/>a) varmistamalla tietoliikenneyhteyden eheys ja luottamuksellisuus sitomalla osapuolten tietoliikenne 8 kohdan mukaisesti toimittuihin varmenteisiin tai avaimiin; tai<br/>b) salaamalla ja allekirjoittamalla sanomat 8 kohdan mukaisella menettelyllä toimitulla avaimella.</p> <p><b>9.2 Sanomien suojaaminen käyttäjärajapinnassa</b></p> | <p>A.10.1.1 salauksen käytön periaatteet</p> <p>A.13.2.3 viestintäturvallisuus/tietojen siirtäminen: sähköinen viestintä</p> <p>A 14.1.1. Tietoturva vaatimusten analysointi ja määrittely</p> <p>A 14.1.2 Sovelluspalveluiden suojaaminen julkisissa verkoissa</p> | Huom. myös tunnistusvälytyspalvelu |

|     |      |                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                     |                                    |
|-----|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
|     |      |                                                                                                                                                                                                                               | <p>Jos tunnistussanomat välitetään käyttäjän selaimen tai päätelaitteen kautta, sanomat on salattava ja allekirjoitettava 9.1.1.b) alakohdan mukaisesti.</p> <p><b>9.3 Salausalgoritmit ja menettelyt</b><br/>Sanomien salaamisessa ja allekirjoittamisessa on käytettävä soveltuvin osin 7.1 kohdan mukaisia menettelyjä.</p>                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                     |                                    |
| 18. | S, H | Todentamismekanismissa noudatetaan pakollisia salausvaatimuksia <b>käyttäjäraajapinnassa (selain, mobiili)</b>                                                                                                                | <p><b>LoA Liite 2.4.6 Tekniset tarkastukset</b> (controls)<br/>2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät <u>sähköisen viestinnän kanavat on suojattu</u> salakuuntelulta, manipuloinnilta ja toistolta.</p> <p><b>M72B 7 (yllä)</b></p> <p><b>M72B 9.2 Sanomien suojaaminen käyttäjäraajapinnassa</b><br/>Jos tunnistussanomat välitetään käyttäjän selaimen tai päätelaitteen kautta, sanomat on salattava ja allekirjoitettava 9.1.1.b alakohdan mukaisesti.</p> <p><b>M72B 9.3 Salausalgoritmit ja menettelyt</b><br/>Sanomien salaamisessa ja allekirjoittamisessa on käytettävä soveltuvin osin 7.1 kohdan mukaisia menettelyjä.</p> | <p>A.10.1.1 salauksen käytön periaatteet</p> <p>A.13.2.3 viestintäturvallisuus/tietojen siirtäminen: sähköinen viestintä</p> <p>A 14.1.1. Tietoturva vaatimusten analysointi ja määrittely</p> <p>A 14.1.2 Sovelluspalveluiden suojaaminen julkisissa verkoissa</p> | Huom. myös tunnistusvälityspalvelu |
| 19. | H    | Todentamismekanismissa noudatetaan <b>suosituksen</b> mukaisia tiukennettuja/korkean tason salausvaatimuksia tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välillä, tunnistuspalvelun ja asiointipalvelun | <p><b>MPS M72B kohta 4.7.1.3 (20.5.2022) suositus</b></p> <p>Korkealla varmuustasolla tunnistusjärjestelmässä suositellaan sovellettavaksi määräyksessä säännöksessä 7.1 edellytettyjen korotetun varmuusta-</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <p>A.10.1.1 salauksen käytön periaatteet</p> <p>A.13.2.3 viestintäturvallisuus/tietojen</p>                                                                                                                                                                         | Huom. myös tunnistusvälityspalvelu |

|  |  |                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                 |  |
|--|--|----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|--|
|  |  | <p>välillä ja käyttäjärajapinnassa (selain, mobiili)</p> | <p>son vaatimusten sijaan seuraavassa esitettyjä su-<br/>luissa olevia arvoja, <b>joilla saavutetaan vähin-<br/>tään 128 bitin vahvuustaso:</b></p> <p>1) <b>Avaintenvaihto:</b> Avaintenvaihdossa on käy-<br/>tettävä DHE-menetelmiä tai elliptisiä käyriä käyt-<br/>täviä ECDHE-menetelmiä. Laskutoimituksissa käy-<br/>tetyn äärellisen kunnan (<i>finite field</i>) koon tulee<br/>olla DHE-menetelmässä vähintään 2048 (<b><u>korke-<br/>alla varmuustasolla 4096</u></b>) bittiä ja ECDHE-me-<br/>netelmässä vähintään 224 (<b><u>korkealla varmuus-<br/>tasolla 256</u></b>) bittiä.</p> <p>IANA:n IKEv2-määritysten mukaiset DH-ryh-<br/>mät 14 - <b>21</b>, 23, 24 ja 26 (<b><u>korkealla var-<br/>muustasolla 16 - 21</u></b>) toteuttavat edellä mai-<br/>nitut edellytykset.</p> <p>2) Allekirjoitus tai epäsymmetrinen salaus: Käy-<br/>tettäessä RSA:ta sähköiseen allekirjoitukseen tai<br/>salaukseen, avaimen pituuden tulee olla vähin-<br/>tään 2048 (<b><u>korkealla varmuustasolla 3072</u></b>)<br/>bittiä. Käytettäessä elliptisen käyrän menetelmää<br/>ECDSA:ta tai EdDSA:ta, alla olevan kunnan koon<br/>tulee olla vähintään 224 (<b><u>korkealla varmuusta-<br/>solla 256</u></b>) bittiä.</p> <p>3) Symmetrinen salaus: Salausalgoritmin on ol-<br/>tava AES, Serpent tai ChaCha20 (<b><u>korkealla var-<br/>muustasolla AES tai Serpent</u></b>). Avaimen pituu-<br/>den tulee olla vähintään 128 (<b><u>korkealla var-<br/>muustasolla 128</u></b>) bittiä. Salausmoodin on oltava<br/>CBC, CCM, GCM tai CTR.</p> <p>4) Tiivistefunktiot: Tiivistefunktion tai autentikaa-<br/>tiokoodin on oltava SHA-2, SHA-3, Whirlpool tai<br/>Poly1305. SHA-2:lla tarkoitetaan funktioita<br/>SHA224, SHA256, SHA384 ja SHA512 (<b><u>korkealla<br/>varmuustasolla SHA-3-256, SHA-3-384, SHA-<br/>3-512</u></b>)</p> | <p>siirtäminen:<br/>sähköinen<br/>viestintä</p> |  |
|--|--|----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|--|

## B 2 Yhteentoimivuus

### KESKEISET SÄÄNNÖKSET

#### **TunnL 29 § Sähköisen tunnistuspalvelun vaatimustenmukaisuuden arviointi**

Tunnistuspalvelun tarjoajan on määrajoin teetettävä palvelulleen 28 §:ssä mainitun arviointielimen arviointi siitä, täyttääkö tunnistuspalvelu tässä laissa säädetyt yhteentoimivuutta, tietoturvaa, tietosuojaa ja muuta luotettavuutta koskevat vaatimukset.

[...]

#### **M72B 15 Vaatimuksenmukaisuuden arviointikriteerit**

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):
  - d) teknisiin toimenpiteisiin
  - e) yhteentoimivuuteen luottamusverkostossa

#### **TunnL 12 a § Tunnistuspalvelun tarjoajien luottamusverkosto**

[...]

Tunnistuspalvelun tarjoajien on tehtävä yhteistyötä sen varmistamiseksi, että luottamusverkoston jäsenten väliset tekniset rajapinnat ovat yhteen toimivia ja että ne mahdollistavat yleisesti tunnettujen standardien mukaisten rajapintojen tarjoamisen luottaville osapuolille.

[...]

#### **M72B 12 Luottamusverkostossa välitettävät vähimmäistiedot**

##### **12.1 Pakolliset tiedot**

Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on välitettävä:

- 1) luonnollista henkilöä koskevassa tunnistustapahtumassa ainakin tunnistusvälineen tarjoajan varmistama henkilön yksilöivä tunniste, henkilön etunimi, henkilön suku-nimi ja henkilön syntymäaika;
- 2) oikeushenkilöä koskevassa tunnistustapahtumassa ainakin tunnistusvälineen tarjoajan varmistama oikeushenkilöä edustavan luonnollisen henkilön yksilöivä tunniste, henkilön etunimi, henkilön sukunimi ja organisaation yksilöivä tunniste;
- 3) tieto tunnistusvälineen korotetusta tai korkeasta varmuustasosta; sekä
- 4) tunnistusvälityspalvelun varmistama tieto luottavasta osapuolesta.

##### **12.2 Valinnaiset tiedot**

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

- 1) tieto siitä, koskeeko tunnistustapahtuma julkisen hallinnon asiointipalvelua vai yksityistä asiointipalvelua;
- 2) luonnollista henkilöä koskevassa tunnistustapahtumassa etunimi (-nimet) ja sukunimi (-nimet) syntymähetkellä, syntymäpaikka, nykyinen osoite ja sukupuoli; ja
- 3) oikeushenkilöä koskevassa tunnistustapahtumassa:
  - a) nykyinen osoite;

- b) arvonlisäverotunniste;
- c) verorekisterinumero;
- d) Euroopan parlamentin ja neuvoston direktiivin 2009/101/EY 3 artiklan 1 kohdassa tarkoitettu tunniste;
- e) komission täytäntöönpanoasetuksessa (EU) N:o 1247/20122 tarkoitettu oikeushenkilötunnus (LEI);
- f) komission täytäntöönpanoasetuksessa (EU) N:o 1352/20133 tarkoitettu taloudellisen toimijan rekisteröinti- ja tunnistenumero (EORI-numero); sekä
- g) neuvoston asetuksen N:o 389/20124 2 artiklan 12 kohdassa tarkoitettu valmisteveronumero.

### 12.3 Tunnistuksen pseudonymisointi

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

### 14 Tiedonsiirrossa käytettävä protokolla ja muut vaatimukset

#### 14.1 Tiedonsiirrossa käytettävä protokolla

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

#### 14.2 Rajapinnan muut ominaisuudet

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

| NRO | VARMUUS-TASO | TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ                                                                                 | SÄÄNNÖKSET                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | STANDARDI-VIITTAUS | HUOMIOITA                                                                                                                                                                                                                                                                                       |
|-----|--------------|---------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 20. | S, H         | Tunnistuspalvelun tarjoaja tarjoaa luottamusverkostossa vähintään yhtä yleisesti käytetyn standardin mukaista rajapintaa. | <p><b>VNA 169/2016 Valtioneuvoston asetus vahvan sähköisen tunnistuspalvelun tarjoajien luottamusverkostosta</b></p> <p><b>1 § Luottamusverkoston tekniset rajapinnat</b></p> <p>Vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain (617/2009), jäljempänä tunnistuslaki, 12 a §:n 2 momentissa tarkoitettuja teknisiä rajapintoja ovat:</p> <ol style="list-style-type: none"> <li>1) <u>tunnistusvälineen tarjoajien välinen rajapinta;</u></li> <li>2) <u>tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välinen rajapinta;</u></li> </ol> |                    | <p><b>Soveltaminen: M72B kohta 14.1 tiukentunut vaatimus "vähintään OpenID Connect tai SAML-protokollan mukaisella rajapinnalla"</b></p> <p>Liikenne- ja viestintävirasto on laatinut luottamusverkoston yhteistointiryhmää kuullen suositusprofiilit SAML ja OpenIDConnect -protokollille.</p> |

|     |      |                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |  |                                                                                                                                                                                                                                                                                                                                             |
|-----|------|---------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |      |                                                                                                                           | <p>3) tunnistusvälityspalvelun tarjoajan ja tunnistuspalveluun luottavan osapuolen välinen rajapinta.</p> <p>Luottamusverkostoon kuuluvat tunnistuspalvelun tarjoajat voivat sopia tunnistuslain 12 a §:n 3 momentissa tarkoitetun tunnistetiedon veloituksen välittämiseen tarvittavasta tai muusta luottamusverkoston toiminnassa tarpeellisesta rajapinnasta. <u>Luottamusverkostoon kuuluvan tunnistuspalvelun tarjoajan on tarjottava 1 momentin 1 ja 2 kohdassa tarkoitetuissa rajapinnoissa kummassakin vähintään yhtä yleisesti käytetyn standardin mukaista teknistä rajapintaa.</u></p> <p><b>M72B 14 Tiedonsiirrossa käytettävä protokolla ja muut vaatimukset</b><br/><b>14.1 Tiedonsiirrossa käytettävä protokolla</b><br/>Tunnistuspalvelun tarjoajan on osaltaan mahdollistettava tunnistuslain 17 §:n mukainen ensitunnistamisen ketjuttaminen ja tunnistuslain 12 a §:n mukainen tunnistustapahtumien välitys luottamusverkostossa vähintään OpenID Connect- tai SAML-protokollan mukaisella rajapinnalla.</p> |  | <p>Suositus 212/2023 S (SAML) Luottamusverkoston rajapinnasta</p> <p>Suositus 213/2023 S (OIDC) Luottamusverkoston rajapinnasta</p> <p>Suosituksien löytyvät viraston verkkosivulta <a href="https://www.kyberturvallisuuskeskus.fi/fi/sahkoisten-tunnistaminen">https://www.kyberturvallisuuskeskus.fi/fi/sahkoisten-tunnistaminen</a></p> |
| 21. | S, H | Tunnistusvälineen tarjoaja tarjoaa vaatimusten mukaiset tiedot (attribuutit) <b>luonnollisen henkilön</b> tunnistamisessa | <p><b>M72B 12 Luottamusverkostossa välitettävät vähimmäistiedot</b><br/><b>12.1 Pakolliset tiedot</b><br/>Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on välitettävä:</p> <p>1) luonnollista henkilöä koskevassa tunnistustapahtumassa ainakin tunnistusvälineen tarjoajan varmistama henkilön yksilöivä tunniste, henkilön etunimi, henkilön sukunimi ja henkilön syntymäaika; [...]</p> <p>3) tieto tunnistusvälineen korotetusta tai korkeasta varmuustasosta; [...]</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |  | Välityspalvelu voi tarvittaessa rikastaa tai köyhyttää tunnistusvälineen tarjoajalta saatuja tietoja (kts. M72B 12.3 kohta). Tunnistusvälineen tarjoajan on joka tapauksessa välitettävä M72B:n 12.1 kohdan mukaiset tiedot.                                                                                                                |
| 22. | S, H | Tunnistusvälineen tarjoajalla on vaadittu <b>suunniteltu valmius</b> välittää optionaaliset tiedot                        | <p><b>M72B 12 Luottamusverkostossa välitettävät vähimmäistiedot</b><br/><b>12.2 Valinnaiset tiedot</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |  | MPS72 12.1 § perustelut, s. 56:                                                                                                                                                                                                                                                                                                             |

|     |      |                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----|------|--------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |      | <b>luonnollisen henkilön</b> tunnistamisessa                                                                       | <p>Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on oltava teknisesti suunniteltu valmius välittää:</p> <ol style="list-style-type: none"> <li>1) tieto siitä, koskeeko tunnistustapahtuma julkisen hallinnon asiointipalvelua vai yksityistä asiointipalvelua;</li> <li>2) luonnollista henkilöä koskevassa tunnistustapahtumassa etunimi (-nimet) ja sukunimi (-nimet) syntymähetkellä, syntymäpaikka, nykyinen osoite ja sukupuoli;</li> </ol> <p>[...]</p>                                                                                                                            |  | <p>Valmius välittää valinnaisia attribuutteja tarkoittaa, että valinnaisten attribuutien käsittely täytyy suunnitella rajapinnassa ja tunnistusjärjestelmässä siten, että tunnistuspalvelun tarjoajalla on käsitys käytönotossa tarvittavista teknisistä toimenpiteistä. Teknistä toteutusta järjestelmiin ei vaadita valinnaisille attribuuteille. Teknisissä konfiguroinneissa tulee kuitenkin huomioida, etteivät tunnistussanomiiin sisältyvät valinnaiset attribuutit haittaa tunnistustapahtumia silloinkaan, kun niiden käytöstä ei ole sovittu. Valvontaa varten <u>suunnitelma</u> täytyy käytännössä dokumentoida.</p> |
| 23. | S, H | Tunnistusvälineen tarjoaja tarjoaa vaatimusten mukaiset tiedot (attribuutit) <b>oikeushenkilön</b> tunnistamisessa | <p><b>M72B 12 Luottamusverkostossa välitettävät vähimmäistiedot</b></p> <p><b>12.1 Pakolliset tiedot</b></p> <p>Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on välitettävä:</p> <p>[...]</p> <ol style="list-style-type: none"> <li>2) oikeushenkilöä koskevassa tunnistustapahtumassa ainakin tunnistusvälineen tarjoajan varmistama oikeushenkilöä edustavan luonnollisen henkilön yksilöivä tunniste, henkilön etunimi, henkilön sukunimi ja organisaation yksilöivä tunniste;</li> <li>3) tieto tunnistusvälineen korotetusta tai korkeasta varmuustasosta;</li> </ol> <p>[...]</p> |  | <p>Vain, jos ryhdytään tarjoamaan oikeushenkilön vahvaa sähköistä tunnistusta</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

|     |      |                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |  |  |
|-----|------|-----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
| 24. | S, H | Tunnistusvälineen tarjoajalla on vaadittu suunniteltu valmius välittää optionaaliset tiedot <b>oikeushenkilön</b> tunnistamisessa | <p><b>M72B 12 Luottamusverkostossa välitettävät vähimmäistiedot</b><br/> <b>12.2 Valinnaiset tiedot</b><br/> Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on <u>oltava teknisesti suunniteltu valmius välittää</u>:</p> <ol style="list-style-type: none"> <li>1) tieto siitä, koskeeko tunnistustapahtuma julkisen hallinnon asiointipalvelua vai yksityistä asiointipalvelua;</li> <li>2) [...]</li> <li>3) oikeushenkilöä koskevassa tunnistustapahtumassa <ol style="list-style-type: none"> <li>a) nykyinen osoite;</li> <li>b) arvonlisäverotunniste;</li> <li>c) verorekisterinumero;</li> <li>d) Euroopan parlamentin ja neuvoston direktiivin 2009/101/EY 3 artiklan 1 kohdassa tarkoitettu tunniste;</li> <li>e) komission täytäntöönpanoasetuksessa (EU) N:o 1247/2012 tarkoitettu oikeushenkilötunnus (LEI);</li> <li>f) komission täytäntöönpanoasetuksessa (EU) N:o 1352/2013 tarkoitettu taloudellisen toimijan rekisteröinti- ja tunnustenumero (EORI-numero); sekä</li> <li>g) neuvoston asetuksen N:o 389/2012 2 artiklan 12 kohdassa tarkoitettu valmisteveronumero.</li> </ol> </li> </ol> |  |  |
|-----|------|-----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|

### B 3 Tekniset tietoturva-vaatimukset

#### KESKEISET SÄÄNNÖKSET

##### **M72B 15 Vaatimuksenmukaisuuden arviointikriteerit**

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):
  - d) teknisiin toimenpiteisiin

**TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset**

4) tunnistusjärjestelmä on turvallinen ja luotettava siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdissa...2.4.6 vähintään korotetulle varmuustasolle säädetty edellytykset täyttyvät ottaen huomioon kulloinkin käytettävissä olevaan tekniikkaan liittyvät tietoturvaluottamukset

**LoA Liite 2.4.6 Tekniset tarkastukset (controls)**

1) Käytössä on oikeasuhteiset tekniset tarkastukset palvelujen turvallisuuteen kohdistuvien riskien hallitsemiseksi ja käsiteltävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi.

**M72B 5 Tunnistusjärjestelmän tietoturva-vaatimukset**

**5.1 Tunnistusjärjestelmän suojautumiskyky**

**5.1.1**

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

**5.1.2**

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

**5.2 Tietoliikenneturvallisuus**

Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:

- a) verkon rakenteellinen turvallisuus;
- b) tietoliikenneverkon vyöhykkeistäminen;
- c) suodatussäännöt vähimpien oikeuksien periaatteilla;
- d) suodatuksen ja valvontajärjestelmien hallinnointi;
- e) turvalliset hallintayhteydet; sekä
- f) käytettävä kansainvälisesti tai kansallisesti suositeltuja salausratkaisuja.

**5.3 Tietojärjestelmäturvallisuus**

Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:

- a) pääsyoikeuksien hallinta vähimpien oikeuksien periaatteilla;
- b) järjestelmien käyttäjien yksilöity tunnistaminen;
- c) järjestelmien koventaminen;
- d) haittaohjelmasuojaus;
- e) turvallisuuteen liittyvien tapahtumien jäljitys- ja jäljitysprosessi;
- f) poikkeamien havainnointikyky ja korjausprosessi; sekä
- g) käytettävä kansainvälisesti tai kansallisesti suositeltuja salausratkaisuja.

#### 5.4 Käyttöturvallisuus

Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:

- muutosten hallinta;
- tiedon luokitteluun perustuva salassa pidettävän aineiston käsittely-ympäristö ja säilytys;
- etäkäytön ja -hallinnan suojaaminen etäkäyttöympäristön uhkilta;
- ohjelmistokehityksen ja ohjelmistohaavoittuvuuksien hallinta;
- varmuuskopiointi; sekä
- käytettävä kansainvälisesti tai kansallisesti suositeltuja salausratkaisuja.

#### 5.5 Tunnistusjärjestelmän tuotantoverkon hallinta- ja etäyhteydet

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

- korotetulla varmuustasolla erityisesti arvioitu ja minimoitu ja
- korkealla varmuustasolla kokonaisuutena arvioiden estetty.

### B 3.1 Tietoliikenneturvallisuus

#### 3.1 Tietoliikenneturvallisuus

| NRO | VARMUUSTASO | TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ                                                                                                                                                                                                                                                                                                                                                                                                                             | SÄÄNNÖKSET                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | STANDARDI-VIITTAUS                                                                                                                                     | HUOMIOITA                                                                                                                                                                                                                                                                                                                                    |
|-----|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 25. | S, H        | <p>Tietoliikenneturvallisuus:</p> <p>Tunnistusjärjestelmän <b>tietoliikenneyhteydet, hallintayhteydet, prosessit</b> (tunnistuspalvelun tuotantoon ml. hallintaan liittyvien osaprosessien tietoliikenne) ja niiden <b>suojauskäytännöt</b> on <b>tunnistettu, dokumentoitu ja ylläpidetty</b>.</p> <p>Tunnistusjärjestelmän tietoliikenneyhteyksien vyöhykkeistäminen ja suodatussäännöt on toteutettava ja ylläpidettävä vähimpien oikeuksien (least privilege)</p> | <p><b>M72B 5.2 Tietoliikenneturvallisuus</b></p> <p>Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:</p> <ol style="list-style-type: none"> <li>verkon rakenteellinen turvallisuus;</li> <li>tietoliikenneverkon vyöhykkeistäminen;</li> <li>suodatussäännöt vähimpien oikeuksien periaatteilla;</li> <li>suodatuksen ja valvontajärjestelmien hallinnointi;</li> <li>turvalliset hallintayhteydet; sekä</li> <li>käytettävä kansainvälisesti tai kansallisesti suositeltuja salausratkaisuja.</li> </ol> <p><b>LoA Liite 2.4.6 Tekniset tarkastukset</b> (controls)</p> | <p>A.8.1.1 Suojattavan omaisuuden luettelointi</p> <p>A.13.1 viestintäturvallisuus/verkon turvallisuuden hallinta:</p> <p>A.13.1.1 verkon hallinta</p> | <p>Tunnistusjärjestelmän kokonaisarkkitehtuurissa huolehditaan tietoliikenneturvallisuudesta.</p> <p>Huom. suunnittelussa on huolehdittava myös kaikista relevanteista tietoliikenneyhteyksistä alihankkijoihin (infra, ohjelmistot, käyttöpalvelut, korttitehdas jne. jne.)</p> <p>Ilmoitukseen/<b>tarkastuskertomukseen</b> on liitet-</p> |

|     |      |                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                  |                                                                                                                                                                                                                                                                                                                          |
|-----|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |      | ja monitasoisen suojaamisen (defence in depth) periaatteiden mukaisesti.                                                                                                                                                                                                   | 2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät <u>sähköisen viestinnän kanavat on suojattu</u> salakuuntelulta, manipuloinnilta ja toistolta.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | A.13.1.3 ryhmien eriyttäminen verkossa                                                                                           | tävä arkkitehtuurista kuvaus, josta ilmenevät tunnistusjärjestelmän osien väliset tietoliikenneyhteydet ja niiden suojauskäytännöt. Dokumentaatioon tulee selkeästi kuvata eri turvatason verkkoalueet, sekä niiden välissä toimivat suodatus- ja valvontajärjestelmät.                                                  |
| 26. | S, H | Tietoliikenneturvallisuus:<br><br>Tunnistusjärjestelmän <b>tietoliikennelaitteet ja -järjestelmät</b> on tunnistettu ja dokumentoitu.                                                                                                                                      | <b>M72B 5.2 Tietoliikenneturvallisuus</b><br>Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:<br>a) verkon rakenteellinen turvallisuus;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | A.8.1.1 Suojattavan omaisuuden luetteloiminen                                                                                    |                                                                                                                                                                                                                                                                                                                          |
| 27. | S, H | Tietoliikenneturvallisuus:<br><br><b>Tuotantoverkko</b> tulee olla <b>eriytettynä</b> ylläpito- ja hallinnointiverkosta.<br><br>Ylläpito- ja hallinnointiverkon tulee olla eriytettynä muusta toimistoverkosta.<br><br>Käytössä on tuotannosta eriytetty kehitysympäristö. | <b>M72B 5.2 Tietoliikenneturvallisuus</b><br>Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:<br>a) verkon rakenteellinen turvallisuus;<br>b) tietoliikenneverkon vyöhykkeistäminen; [...]<br><br><b>5.5 Tunnistusjärjestelmän tuotantoverkon hallinta- ja etäyhteydet</b><br>Tuotantoverkko ja sen edellä 5.2.e) ja 5.4.c) alakohtissa tarkoitetut hallintayhteydet ja etäkäyttö ja etähallinta on toteutettava siten, että organisaation muiden palveluiden kuten sähköpostin tai web-selailun kautta aiheutuvat tietoturvaohat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvaohat on:<br>a) <u>korotetulla varmuustasolla erityisesti arvioitu ja minimoitu ja</u><br>b) <u>b) korkealla varmuustasolla kokonaisuutena arvioiden estetty.</u> | A.12.1.4 Käytöturvallisuus: Kehitys-, testaus- ja tuotantoympäristöjen erottaminen<br><br>A.13.1.3 Ryhmien eriyttäminen verkossa | Eriyttäminen voidaan tehdä loogisesti tai fyysisesti. Eriyttämiseltä vaadittavaan tasoon vaikuttavat kokonaisuutena verkon kriittisyys ja siinä käsiteltävät tiedot. Vaatimuksen tarkoitus on vähentää tietoliikenneyhteyksien kautta aiheutuvia riskejä verkkojen eheydelle, luotamuksellisuudelle ja käytettävyydelle. |
| 28. | S, H | Tietoliikenneturvallisuus:                                                                                                                                                                                                                                                 | <b>M72B 5.2 Tietoliikenneturvallisuus</b><br>Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | A.13.1.1-3 viestintätur-                                                                                                         |                                                                                                                                                                                                                                                                                                                          |

|     |      |                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                     |                                                                                              |
|-----|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
|     |      | Tunnistusjärjestelmän tietoliikenneyhteyksillä <b>huolehditaan suodatuksista</b> vähimpien oikeuksien periaatteilla.                                                         | [...]<br>c) suodatussäännöt vähimpien oikeuksien periaatteilla;<br>d) suodatuksen ja valvontajärjestelmien hallinnointi;<br>[...]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | vallisuus/verkon turvallisuuden hallinta:<br>A.13.1.1 verkon hallinta<br>A.13.1.2 Verkkopalvelujen turvaaminen<br>A.13.1.3 Ryhmien eriyttäminen verkossa<br>Ks. myös pääsynhallinta |                                                                                              |
| 29. | S, H | Tietoliikenneturvallisuus:<br><br>Tuotantoverkon <b>yhteyksien julkiseen verkkoon</b> tulee olla riskiperusteisia, vain palvelun toiminnallisuudet mahdollistavia yhteyksiä. | <b>M72B 5.2 Tietoliikenneturvallisuus</b><br>Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:<br>a) verkon rakenteellinen turvallisuus;<br>b) [...]<br>c) suodatussäännöt vähimpien oikeuksien periaatteilla;<br>d) suodatuksen ja valvontajärjestelmien hallinnointi;<br>e) turvalliset hallintayhteydet; sekä<br>f) [...]<br><br><b>5.5 Tunnistusjärjestelmän tuotantoverkon hallinta- ja etäyhteydet</b><br>Tuotantoverkko ja sen edellä 5.2.e) ja 5.4.c) alakohtissa tarkoitetut hallintayhteydet ja etäkäyttö ja etähallinta on toteutettava siten, että organisaation muiden palveluiden kuten sähköpostin tai web-selailun kautta aiheutuvat tietoturvausuhat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvausuhat on:<br>a) <u>korotetulla varmuustasolla erityisesti arvioitu ja minimoitu ja</u> | Ks. ed. rivi                                                                                                                                                                        | Kaikki muut kuin toiminnalle tarpeelliset yhteydet on nimenomaisesti kielletty tai suljettu. |

|     |      |                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |      |                                                                                                                                                                     | b) <u>b) korkealla varmuustasolla kokonaisuutena arvioiden estetty.</u>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 30. | S, H | Tietoliikenneturvallisuus:<br><br>Tunnistuspalveluiden ja luottavien osapuolten <b>kryptografisen avainmateriaali</b> tai <b>metadata</b> vaihdetaan turvallisesti. | <p><b>M72B 8 Tietoliikenteen osapuolten varmentaminen</b></p> <p><b>8.1 Tietoliikenneyhteyden osapuolten tunnistaminen</b></p> <p>Tunnistuspalveluiden välisessä sekä tunnistuspalvelun ja luottavan osapuolen välisessä tietoliikenteen tai sanomien salaamisessa käytettävien varmenteiden ja avainten aitous ja eheys sekä niiden haltijat.</p> <p>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.</p> <p><b>8.2 Varmenteiden ja avainten uusiminen</b></p> <p>Edellä 8.1 kohdassa tarkoitetut varmenteet ja avaimet on uusittava säännöllisesti.</p> <p>Uusien varmenteiden ja avainten aitouden ja eheyden varmistamiseksi uusiminen on tehtävä joko:</p> <ul style="list-style-type: none"> <li>a) 8.1 kohdan mukaisella menettelyllä;</li> <li>b) toimittamalla uudet avaimet tietoliikenneyhteydellä, jonka eheys ja luottamuksellisuus on varmistettu sitomalla osapuolten tietoliikenne 8.1 kohdan mukaisesti toimitettuihin varmenteisiin tai avaimiin; tai</li> <li>c) allekirjoittamalla uusi avain 8.1 kohdan mukaisesti toimitetulla avaimella tai sellaisesta ketjutetulla avaimella.</li> </ul> <p><b>LoA Liite 2.4.6 Tekniset tarkastukset</b></p> <p>1. Käytössä on oikeasuhteiset tekniset tarkastukset palvelujen turvallisuuteen kohdistuvien riskien hallitsemiseksi ja käsiteltävien tietojen <u>luottamuksellisuuden</u>, eheyden ja käytettävyyden suojaamiseksi.</p> | A.10.1.2 Salauksenhallinta: salausavainten hallinta | <p>vrt. PSD2/RTS eIDAS art45 tai eSeal varmennevaatimus osapuolen tunnistamiselle</p> <p>Osapuolten välille on määriteltä prosessi turvalliseen luottosuhteen perustamiseen ja osapuolten todentamiseen ja pitkäikäisten avainten/salaisuuksien vaihtamiseen.</p> <p>Salausavaintenhallinnan prosessit ja käytännöt ovat dokumentoituja ja asianmukaisesti toteutettuja</p> <p>Prosessit edellyttävät vähintään kryptografisesti vahvojen avaimien käyttöä, turvallista avaintenjakelua, turvallista avainten säilytystä, säännöllisiä avaintenvaihtoja, vanhojen tai paljastuneiden avainten vaihdon, sekä valtuuttamattomien avaintenvaihtojen estämisen KATAKRI v.2015 (I12)</p> |

|     |      |                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                      |  |
|-----|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|--|
|     |      |                                                                                                                                                             | <p>2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät sähköisen viestinnän kanavat on suojattu salakuuntelulta, manipuloinnilta ja toistolta.<br/>[...]</p> <p>5. Kaikki laitteet ja välineet, jotka sisältävät henkilötietoja, salattuja tietoja tai muita arkaluonteisia tietoja, säilytetään, kuljetetaan ja hävitetään turvallisella ja varmalla tavalla.</p> <p><b>LoA Liite 2.4.6 Tekniset tarkastukset</b><br/>Korotettu: Arkaluonteinen salaustekninen aineisto, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, on suojattu luvattomalta käsittelyltä.</p> <p><b>LoA Liite 2.3.1 Todentamismekanismi</b><br/>Korotettu: 2. Todentamismekanismeissa toteutetaan turvatoimenpiteitä sähköisen tunnistamisen menetelmän varmentamiseksi siten, että on erittäin epätodennäköistä, että viestin arvaaminen, salakuuntelu, toisto tai manipulointi hyökkäyksessä, jonka vakavuusaste on kohtuullinen ("moderate"), voi heikentää todentamismekanismeja.</p> |                                                      |  |
| 31. | H    | <p>Tietoliikenneturvallisuus:</p> <p>Tunnistuspalveluiden ja luottavien osapuolten kryptografisen avainmateriaali tai metadata vaihdetaan turvallisesti</p> | <p>Vrt. yllä sekä <b>LoA Liite 2.3.1 Todentamismekanismi</b><br/>Korkea: Todentamismekanismeissa toteutetaan turvatoimenpiteitä sähköisen tunnistamisen menetelmän varmentamiseksi siten, että on erittäin epätodennäköistä, että viestin arvaaminen, salakuuntelu, toisto tai manipulointi hyökkäyksessä, jonka vakavuusaste on korkea ("high"), voi heikentää todentamismekanismeja.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | A.10.1.2 Salauksenhallinta: salaustavainten hallinta |  |
| 32. | S, H | Tunnistuspalvelun (välityspalvelu tai oman välineen välitys) tarjoajan ja luottavan osapuolen tunnistussanomien on todennettava.                            | <p><b>M72B 9.1.2</b><br/>Tunnistusvälityspalvelun ja luottavan osapuolen välisessä tietoliikenteessä tunnistussanomien on todennettava allekirjoittamalla.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                      |  |

|     |      |                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                              |                                                                                                                                                                                                           |
|-----|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 33. | S, H | Tunnistussanomien eheydestä ja luottamuksellisuudesta huolehditaan.                                                                                                                                                                        | <p><b>M72B 9.1.1</b><br/>Tunnistuspalveluiden välisessä ja tunnistuspalvelun ja luottavan osapuolen välisessä tietoliikenteessä on suojattava henkilötietoja sisältävien tunnistussanomien eheys ja luottamuksellisuus joko:</p> <ul style="list-style-type: none"> <li>a) varmistamalla tietoliikenneyhteyden eheys ja luottamuksellisuus sitomalla osapuolten tietoliikenne 8 kohdan mukaisesti toimitettuihin varmenteisiin tai avaimiin; tai</li> <li>b) salaamalla ja allekirjoittamalla sanomat 8 kohdan mukaisella menettelyllä toimitettulla avaimella.</li> </ul> <p><b>LoA liite 2.4.6 Tekniset tarkastukset</b><br/>1. Käytössä on oikeasuhteiset tekniset tarkastukset palvelujen turvallisuuteen kohdistuvien riskien hallitsemiseksi ja käsiteltävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi.<br/>2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät sähköisen viestinnän kanavat on suojattu salakuuntelulta, manipuloinnilta ja toistolta.</p> |                                                                                              | Kohdassa 8 kuvataan eri menetelmiä, joilla voidaan toteuttaa osapuolten riittävä tietoliikennesuojaus.                                                                                                    |
| 34. | S, H | Tietoliikenneturvallisuus:<br><br>Tunnistusjärjestelmän tietoliikenneyhteyksien <b>suodatusten ja valvontajärjestelmien hallinnosta</b> huolehditaan.                                                                                      | <p><b>M72B 5.2 Tietoliikenneturvallisuus</b><br/>Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:<br/>[...]<br/>d) suodatuksen ja valvontajärjestelmien hallinnointi;<br/>e) turvalliset hallintayhteydet; sekä<br/>[...]</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | A.13.1 viestintäturvallisuus/verkon turvallisuuden hallinta:<br><br>A.13.1.1 verkon hallinta |                                                                                                                                                                                                           |
| 35. | S    | Tietoliikenneturvallisuus/hallinta:<br><br>Tunnistusjärjestelmän etäkäytössä ja hallinnassa on <b>arvioitu ja minimoitu</b> sähköpostin tai web-selailun kautta aiheutuvat tietoturvaohut, sekä hallinnassa käytettävän päätelaitteen mui- | <p><b>M72B 5.2 Tietoliikenneturvallisuus</b><br/>Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:<br/>[...]<br/>d) suodatuksen ja valvontajärjestelmien hallinnointi;<br/>e) turvalliset hallintayhteydet; sekä<br/>[...]</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | A 6.2.2 Etätyö<br><br>A.9.4 Järjestelmien ja sovellusten pääsynhallinta:                     | MPS72: internetiä ja toimistoverkkoa pidetään ei-luotettuna verkkona, ellei toimistoverkko kuulu vaatimustenmukaisuuden arvioinnin piiriin. Tiedonsiirto-kanavan täytyy siis olla etäkäytössä suojattu ja |

|     |   |                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                             |                                                                                                                                                                                           |
|-----|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |   | den kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvaohat.                                                                                                                                                                                                                                                       | <p><b>5.4 Käyttöturvallisuus</b><br/>Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:<br/>[...]<br/>c) etäkäytön ja -hallinnan suojaaminen etäkäyttöympäristön uhkilta;<br/>[...]</p> <p><b>5.5 Tunnistusjärjestelmän tuotantoverkon hallinta- ja etäyhteydet</b><br/>Tuotantoverkko ja sen edellä 5.2.e) ja 5.4.c) alakohtissa tarkoitetut hallintayhteydet ja etäkäyttö ja etähallinta on toteutettava siten, että organisaation muiden palveluiden kuten sähköpostin tai web-selailun kautta aiheutuvat tietoturvaohat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvaohat on:<br/>a) korotetulla varmuustasolla erityisesti arvioitu ja minimoitu ja<br/>[...]</p> | <p>A.9.4.1 Tietoihin pääsyn rajoittaminen</p> <p>A.9.4.4 Ylläpito- ja hallintasoventukset</p> <p>A.13.1.3 verkon turvallisuuden hallinta: Ryhmien eriyttäminen verkossa</p> | toimistoverkon aiheuttamat riskit täytyy huomioida. Korotetun varmuustason vaatimukset ovat tavomaisia ja ne katetaan jo esimerkiksi ISO 27001 -vaatimusten kautta, jos sovelletaan sitä. |
| 36. | H | <p>Tietoliikenneturvallisuus/hallinta:</p> <p>Tunnistusjärjestelmän (tuotantoverkon) etäkäytössä ja etähallinnassa on <b>estetty</b> sähköpostin tai web-selailun kautta aiheutuvat tietoturvaohat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvaohat.</p> | <p><b>M72B 5.2 Tietoliikenneturvallisuus</b><br/>Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:<br/>[...]<br/>d) suodatuksen ja valvontajärjestelmien hallinnointi;<br/>e) turvalliset hallintayhteydet; sekä<br/>[...]</p> <p><b>5.4 Käyttöturvallisuus</b><br/>Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:<br/>[...]<br/>c) etäkäytön ja -hallinnan suojaaminen etäkäyttöympäristön uhkilta;<br/>[...]</p> <p><b>5.5 Tunnistusjärjestelmän tuotantoverkon hallinta- ja etäyhteydet</b></p>                                                                                                                                                                                        | Ks. ed. rivi                                                                                                                                                                |                                                                                                                                                                                           |

|  |  |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |  |  |
|--|--|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
|  |  |  | <p>Tuotantoverkko ja sen edellä 5.2.e) ja 5.4.c) alakohtissa tarkoitetut hallintayhteydet ja etäkäyttö ja etähallinta on toteutettava siten, että organisaation muiden palveluiden kuten sähköpostin tai web-selailun kautta aiheutuvat tietoturvaohat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvaohat on:</p> <p>[...]</p> <p>b) korkealla varmuustasolla kokonaisuutena arvioiden estetty.</p> <p><b>MPS72B soveltamisohje:</b></p> <p>Korkealla varmuustasolla vaatimukset voi toteuttaa ainakin siten, että etäkäytössä olevasta työasemasta estetään pääsy muihin organisaation palveluihin kuten sähköpostiin ja poistetaan työasemasta mahdollisuus käyttää muita kuin hallintaverkon käytön kannalta välttämättömiä toimintoja. Käytännössä tämä tarkoittaa siis erillistä työasemaa hallintakäyttöä varten.</p> <p>Korkealla varmuustasolla edellytetty kokonaisarvio tarkoittaa sitä, että jos käytetään muuta kuin edellä kuvattua kovennettua työasemaa, otetaan toteutuksessa huomioon tuotantojärjestelmän eriyttäminen ja muut järjestelyt, joilla tietoturvaohkat voidaan hallita. Lähtökohtaisesti tällöin edellytetään virtualisoitua terminointia tai kvm-periaatteeseen (etätyöpöytä) perustuvaa ratkaisua. Olennaista on, mitä tehdään sillä päätelaitteella, josta virtualisoitua yhteyttä otetaan ja siten esimerkiksi two-factor VPN-yhteys virtualisoituun työasemaan ei yksin riitä ratkaisuksi. Riittävää ei ole myöskään, että käytetään virustorjuntaa ja web-proxyä.</p> <p>Välttämättömien tiedostojen siirrossa koneelta toiselle on myös huomioitava haittaohjelmien riski mm. pitämällä huolta siitä, että käytetään vain luotettavia lähteitä ja varmistetaan tietoturvasuus (eheys) kaikilla tarpeellisilla menetelmillä.</p> |  |  |
|--|--|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|

## B 3.2 Tietojärjestelmäturvallisuus

| 3.2 Tietojärjestelmäturvallisuus |             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                              |                                                                                                                                              |
|----------------------------------|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| NRO                              | VARMUUSTASO | TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | SÄÄNNÖKSET                                                                                                                                                                                                                                                                                                                                                                                            | STANDARDI-VIITTAUS                                                                                                                                                                           | HUOMIOITA                                                                                                                                    |
| 37.                              | S, H        | <p>Tietojärjestelmäturvallisuus:</p> <p>Tunnistusjärjestelmän <b>tietojärjestelmät ja prosessit</b> (tunnistuspalvelun tuotantoon ml. hallintaan liittyvät tietojärjestelmiä käyttävät prosessit) on <b>tunnistettu, dokumentoitu ja ylläpidetty</b>.</p> <p>Tunnistusjärjestelmän tietojärjestelmät on <b>luokiteltu</b> huomioiden niissä käsiteltävä tieto ja niiden mahdollistamat toiminnot. Järjestelmien luokittelussa tulee huomioida suojattavan tiedon koko elinkaari.</p> <p>Hallintaan käytettävä tietojenkäsittely-ympäristö on erotettu muista ympäristöistä.</p> | <p><b>M72B 5.3 Tietojärjestelmäturvallisuus</b></p> <p>Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:</p> <ul style="list-style-type: none"> <li>a) pääsyoikeuksien hallinta vähimpien oikeuksien periaatteella;</li> <li>b) järjestelmien käyttäjien yksilöity tunnistaminen;</li> </ul> <p>[...]</p>                                         | <p>A.8.1.1 suojattavan omaisuuden hallinta, vastuu suojattavasta omaisuudesta: suojattavan omaisuuden luetteloiminen</p> <p>A.8.2.1 Suojattavan omaisuuden hallinta: tietojen luokittelu</p> | <p>Luokittelu: mm. laitteiden, ohjelmistojen ja muu omaisuuden hyväksytty käyttö tulee olla määriteltynä</p>                                 |
| 38.                              | S, H        | <p>Tietojärjestelmäturvallisuus:</p> <p>Tunnistusjärjestelmän <b>pääsyoikeudet</b> on määriteltä ja dokumentoitu.</p> <p>Pääsyoikeudet <b>perustuvat</b> tietojärjestelmien luokitteluun ja henkilön/käyttäjän tehtäviin.</p>                                                                                                                                                                                                                                                                                                                                                   | <p><b>M72B 5.3 Tietojärjestelmäturvallisuus</b></p> <p>Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:</p> <ul style="list-style-type: none"> <li>a) pääsyoikeuksien hallinta vähimpien oikeuksien periaatteella;</li> <li>b) järjestelmien käyttäjien yksilöity tunnistaminen;</li> <li>c) järjestelmien koventaminen;</li> </ul> <p>[...]</p> | <p>A.9.1.1 pääsynhallinnan liiketoiminnalliset vaatimukset: pääsynhallintapolitiikka</p> <p>A.9.1.2 pääsy verkkoihin ja verkko verkko palveluihin</p>                                        | <p>Pääsyoikeuksien hallinnoinnin avulla rajoitetaan pääsy tietoon ja tiedonkäsitteleympäristöihin suunnitelmallisesti ja dokumentoidusti</p> |

|     |      |                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                    |                                                                                                                                                                                                    |
|-----|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |      | Pääsy tulee myöntää vain tehtävien mukaisesti (vähimpien oikeuksien periaate).                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | A.9.4.1 järjestelmien ja sovellusten pääsynhallinta: tietoihin pääsyn rajoittaminen                                                                                                                                |                                                                                                                                                                                                    |
| 39. | S, H | Tietojärjestelmäturvallisuus:<br><br>Tunnistusjärjestelmän tietojärjestelmien <b>käyttäjät tunnista-</b><br><b>taan</b> tunnetulla ja turvallisena pidetyllä tekniikalla/menetelmällä. | <b>M72B 5.3 Tietojärjestelmäturvallisuus</b><br>Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:<br>a) pääsyoikeuksien hallinta vähimpien oikeuksien periaatteella;<br>b) järjestelmien käyttäjien yksilöity tunnistaminen;<br>c) järjestelmien koventaminen;<br>d) [...]<br>e) turvallisuuteen liittyvien tapahtumien jäljitys-<br>tyskyky ja jäljitysprosessi;<br>f) [...]                                                             | A.9.4.2 järjestelmien ja sovellusten pääsynhallinta: turvallinen kirjautuminen                                                                                                                                     | Esim. varmenteet, 2FA<br><br>pääsääntöisesti muu kuin salasana, mutta jos mukana salasana, kunnolliset salasana-<br>apituudet ja yksilölliset (ei yhteiskäyttöiset) salasanat ja käyttäjätunnukset |
| 40. | S, H | Tietojärjestelmäturvallisuus:<br><br>Pääsyoikeuksia valvotaan ja niiden <b>ajantasaisuudesta</b> huolehditaan.                                                                         | <b>M72B 5.3 Tietojärjestelmäturvallisuus</b><br>Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:<br>a) pääsyoikeuksien hallinta vähimpien oikeuksien periaatteella;<br>b) järjestelmien käyttäjien yksilöity tunnistaminen;<br>c) järjestelmien koventaminen;<br>d) [...]<br>e) turvallisuuteen liittyvien tapahtumien jäljitys-<br>tyskyky ja jäljitysprosessi;<br>f) poikkeamien havainnointikyky ja korjausprosessi; sekä<br>g) [...] | A.9.2 pääsyoikeuksien hallinta<br><br>A.9.2.1 Käyttäjien rekisteröinti ja poistaminen<br><br>A.9.2.3 Ylläpito-oikeuksien hallinta<br><br>A.9.2.5 pääsyoikeuksien uudelleenarviointi<br><br>A.9.2.6 pääsyoikeuksien |                                                                                                                                                                                                    |

|     |      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | poistaminen ja muuttaminen                              |                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 41. | S, H | <p>Tietojärjestelmäturvallisuus:</p> <p>Henkilöstön <b>tehtävät ja toiminnot on määriteltävä</b> siten, ettei yksi henkilö pysty omalla toiminnallaan tahattomasti tai tahallisesti aiheuttamaan vakavaa turvallisuuspoikkeamaa (vaaralliset työyhdistelmät).</p>                                                                                                                                                                                                                                                         | <p><b>M72B 5.3 Tietojärjestelmäturvallisuus</b></p> <p>Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:</p> <ul style="list-style-type: none"> <li>a) pääsyoikeuksien hallinta vähimpien oikeuksien periaatteella;</li> <li>b) järjestelmien käyttäjien yksilöity tunnistaminen;</li> <li>c) järjestelmien koventaminen;</li> <li>d) [...]</li> <li>e) turvallisuuteen liittyvien tapahtumien jäljitys- ja jäljitysprosessi;</li> <li>f) poikkeamien havainnointikyky ja korjausprosessi; sekä</li> <li>g) [...]</li> </ul> | A.6.1.2 Tehtävien eriyttäminen                          | <p>Esimerkiksi vilpillisen tai huolimattoman työntekijän mahdollisuutta myöntää tunnistusmenetelmä vaatimusten vastaisesti voidaan ehkäistä tehtävien määrittelyllä tai muilla kontroleilla, jotka vähentävät erehdyksen ja väärinkäytöksen riskiä.</p> <p>Arvioinnissa on huomiotava tunnistusmenetelmän varmuustason mukaisesti kohtuullinen tai korkea hyökkäyspotentiaali, kuten muissakin kohdissa.</p>                   |
| 42. | S, H | <p>Tietojärjestelmäturvallisuus:</p> <p>Tunnistusjärjestelmän <b>kovennuksista</b> huolehditaan; käytössä on menettelytapa, jolla järjestelmät asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus.</p> <p>Tunnistusjärjestelmässä käytetään <b>vain</b> sen toiminnan kannalta <b>tarvittavia</b> palveluita, toimintoja, prosesseja, laitteita ja komponentteja. Niiden käyttö on määritelty siten, että asennuksesta on poistettu kaikki tarpeettomat oikeudet ja toiminnot/elementit.</p> | <p><b>M72B 5.3 Tietojärjestelmäturvallisuus</b></p> <p>Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:</p> <ul style="list-style-type: none"> <li>[...]</li> <li>c) järjestelmien koventaminen;</li> <li>[...]</li> </ul>                                                                                                                                                                                                                                                                                                  | A.12.5. tuotantokäytössä olevien ohjelmistojen hallinta | <p>Ks. myös tietoliikenne</p> <p>Ohjeessa 211/2016 oli seuraavia kriteereitä, jotka ovat tässä mukana informatiivisina:</p> <p>Kovennettu asennus sisältää vain sellaiset komponentit ja palvelut, sekä käyttäjien ja prosessien oikeudet, jotka ovat välttämättömiä toimintavaatimusten täyttämiseksi ja turvallisuuden varmistamiseksi.</p> <p>Käyttöön on otettu vain käyttövaatimusten ja tietojen käsittelyn kannalta</p> |

|     |      |                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                            |                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |      |                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                            |                                                                                                  | olennaiset toiminnot, laitteet ja palvelut.                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 43. | S, H | Tietojärjestelmäturvallisuus:<br><br>Tunnistusjärjestelmässä huolehditaan <b>haittaohjelmien</b> aiheuttamien haittojen ja uhkien havaitsemisesta, ennaltaehkäisystä, estämisestä ja korjaamisesta. | <b>M72B 5.3 Tietojärjestelmäturvallisuus</b><br>Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:<br>[...]<br>d) haittaohjelasuojaus;<br>e) turvallisuuteen liittyvien tapahtumien jäljitys- ja jäljitysprosessi;<br>f) poikkeamien havainnointikyky ja korjausprosessi; sekä<br>[...] | A.12.2 haittaohjelmilta suojautuminen<br><br>A.12.6. teknisten haavoittuvuuksien hallinta        | Ks. myös poikkeamien havainnointikyky                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 44. | S, H | Tietojärjestelmäturvallisuus:<br><br>Tunnistusjärjestelmässä käytetään kaikilta osin suositeltavia <b>salausratkaisuja</b> .                                                                        | <b>M72B 5.3 Tietojärjestelmäturvallisuus</b><br>Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:<br>[...]<br>g) käytettävä kansainvälisesti tai kansallisesti suositeltuja salausratkaisuja.                                                                                          | A.10.1 salauksen käytön periaatteet<br><br>A.18.1.5 salaustekniikan hallintaa koskevat säädökset | MPS72:ssa mainitaan lähimpinä seuraavia:<br>- SOGIS-MRA<br>- NCSA-FI<br>- NIST<br>- Enisa<br>- SANS<br><br>Ohjeessa 211/2016 oli seuraavia huomioita, jotka ovat tässä mukana informatiivisina:<br><br>Prosessit edellyttävät vähintään kryptografisesti vahvojen avaimien käyttöä, turvallista avaintenjakelua, turvallista avainten säilytystä, säännöllisiä avaintenvaihtoja, vanhojen tai paljastuneiden avainten vaihdon, sekä valtuuttamattomien avaintenvaihtojen estämisen. KATAKRI v.2015 (I12) |
| 45. | S, H | Tietojärjestelmäturvallisuus:                                                                                                                                                                       | <b>LoA Liite 2.4.6 Tekniset tarkastukset</b>                                                                                                                                                                                                                                                                                               | A.8.2.1 tiedon luokittelu                                                                        | Ohjeessa 211/2016 oli seuraavia huomioita, jotka                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

|  |  |                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--|--|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  | <p>Salaustekninen aineisto on suojattu koko elinkaaren ajan</p> | <p>3) Pääsy arkaluonteiseen salaustekniseen aineistoon, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, rajoitetaan tiukasti niihin tehtäviin ja sovelluksiin, jotka edellyttävät tällaista pääsyä. On varmistettava, ettei tällaista aineistoa koskaan tallenneta pysyväisluonteisesti ilmitekstinä.</p> <p>Korotettu: Arkaluonteinen salaustekninen aineisto, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, on suojattu luvattomalta käsittelyltä.</p> <p><b>M72B 5.3 Tietojärjestelmäturvallisuus</b><br/>Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:</p> <ul style="list-style-type: none"> <li>a) pääsyoikeuksien hallinta vähimpien oikeuksien periaatteella;</li> <li>b) järjestelmien käyttäjien yksilöity tunnistaminen;</li> <li>c) järjestelmien koventaminen;<br/>[...]</li> <li>g) käytettävä kansainvälisesti tai kansallisesti suositeltuja salausratkaisuja.</li> </ul> <p><b>M72B 5.4 Käyttöturvallisuus</b><br/>Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:<br/>[...]</p> <ul style="list-style-type: none"> <li>b) tiedon luokitteluun perustuva salassa pidettävän aineiston käsittely-ympäristö ja säilytys;<br/>[...]</li> <li>f) käytettävä kansainvälisesti tai kansallisesti suositeltuja salausratkaisuja.</li> </ul> | <p>A.10.1.1 salauksen käytön periaatteet<br/>A.10.1.2 salausavainten hallinta</p> | <p>ovat tässä mukana informatiivisina:</p> <p>Salaiset avaimet ovat vain valtuutettujen käyttäjien ja prosessien käytössä</p> <p>Salausavaintenhallinnan prosessit ja käytännöt ovat dokumentoituja ja asianmukaisesti toteutettuja.</p> <p>Prosessit edellyttävät vähintään kryptografisesti vahvojen avaimien käyttöä, turvallista avaintenjakelua, turvallista avainten säilytystä, säännöllisiä avaintenvaihtoja, vanhojen tai paljastuneiden avainten vaihdon, sekä valtuuttamattomien avaintenvaihtojen estämisen KATAKRI v.2015 (I12)</p> |
|--|--|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### B 3.3 Käyttöturvallisuus

| 3.3 Käyttöturvallisuus |              |                                                                                                           |                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                     |
|------------------------|--------------|-----------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NRO                    | VARMUUS-TASO | TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ                                                                 | SÄÄNNÖKSET                                                                                                                                                              | STANDARDI-VIITTAUS                                                                                                                                                                                                                                                                                                                                                                          | HUOMIOITA                                                                                                                                                                                                                           |
| 46.                    | S, H         | Käyttöturvallisuus:<br><br>Tunnistusjärjestelmän <b>muutostenhallinta</b> on suunniteltua ja huolellista. | <b>M72B 5.4 Käyttöturvallisuus</b><br>Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:<br>a) muutosten hallinta;<br>[...] | A.12.1.2 käyttöturvallisuus/toiminta-ohjeet ja velvollisuudet: muutoksenhallinta<br>A.14.2.2 järjestelmien hankkiminen, kehittäminen ja ylläpito/kehitys- ja tukiprosessien turvallisuus: järjestelmään tehtävien muutosten hallintamenetelyt<br>A.14.2.3 sovellusten tekeminen katselmointi käyttöalustan muutosten jälkeen<br>A.14.2.4 ohjelmistopakettien muutoksia koskevat rajoitukset | Muutosten hallintaan määriteltynä selkeät prosessit. Uusien ominaisuuksien tai muutosten toteutuksessa testaussuunnitelmassa on myös negatiiviset testitapaukset huomioitu. Testaus ei perustu pelkästään automaattisiin testeihin. |
| 47.                    | S, H         | Käyttöturvallisuus:                                                                                       | <b>M72B 5.4 Käyttöturvallisuus</b><br>Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:                                    | A.12.5.1 käyttöturvallisuus: ohjelmistojen                                                                                                                                                                                                                                                                                                                                                  | Organisaation tulee ylläpitää tietokantaa tai lis-                                                                                                                                                                                  |

|  |  |                                                                                                                                                                                                                                                                                  |                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  | <p>Tunnistusjärjestelmän <b>ohjelmistohaavoittuvuuksien</b> hallinta on suunnitelmallista.</p> <p>Tunnistusjärjestelmässä huolehditaan <b>ohjelmistohaavoittuvuuksien</b> aiheuttamien haittojen ja uhkien havaitsemisesta, ennaltaehkäisystä, estämisestä ja korjaamisesta.</p> | <p>[...]</p> <p>d) ohjelmistokehityksen ja ohjelmistohaavoittuvuuksien hallinta;</p> <p>[...]</p> | <p>asentaminen tuotantokäytössä oleviin järjestelmiin</p> <p>A.12.6.1 käyttöturvallisuus: teknisten haavoittuvuuksien hallinta</p> <p>A.14.2. järjestelmien hankkiminen, kehittäminen ja ylläpito/kehitys- ja tukiprosessien turvallisuus</p> <p>A.14.2.1 turvallisen kehittämisen politiikka</p> <p>A.14.2.2 järjestelmään tehtävien muutosten hallintamenetelyt</p> <p>A.14.2.3 sovellusten tekninen katselmointi käyttöalustan muutosten jälkeen</p> <p>A.14.2.4 ohjelmistopakettien muutoksia koskevat rajoitukset</p> | <p>tausta kaikista tunnustusjärjestelmän eri ohjelmistokomponenteista.</p> <p>Organisaatiolla tulee olla prosessi ohjelmistohaavoittuvuuksien havainnointiin ja seurantaan. Haavoittuneet ohjelmistokomponentit tulee päivittää ajantasaisiin versioihin.</p> <p>Tunnistusjärjestelmässä käytettävien ohjelmistojen tulee noudattaa turvallisen ohjelmoinnin periaatteita.</p> <p>Tunnistusjärjestelmän uudet versiot tulee testata, myös niin että testitapaukset sisältävät negatiivisia testitapauksia.</p> |
|--|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|     |      |                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                     |
|-----|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |      |                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                              | <p>A.14.2.5 turvallisen järjestelmän suunnittelun periaatteet</p> <p>A.14.2.6 turvallinen kehitysympäristö</p> <p>A.14.2.7 ulkoistettu kehittäminen</p> <p>A.14.2.8 järjestelmän turvallisuustestaus</p> <p>A.14.2.9 järjestelmän hyväksymistestaus</p> |                                                                                                                                                                                                                                     |
| 48. | S, H | <p>Käyttöturvallisuus:</p> <p>Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava, ja jatkuvasti ylläpidettävä:</p> <p>Ohjelmistokehityksen hallinta</p>                                               | <p><b>M72B 5.4 Käyttöturvallisuus</b></p> <p>Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:</p> <p>a) muutosten hallinta;<br/>[...];</p> <p>d) ohjelmistokehityksen ja ohjelmistohäviövoittuvuuksien hallinta;<br/>[...]</p> | Kts edellinen                                                                                                                                                                                                                                           | <p>Ohjelmistokehityksen ylläpidossa erityisesti huomioitava toimitusketjun rakenne ja ylläpidettävä tietoa ohjelmiston eri komponenteista ja seurattava niiden päivityksiä.</p> <p>Turvallinen ohjelmistokehitys</p> <p>Testaus</p> |
| 49. | S, H | <p>Käyttöturvallisuus:</p> <p>Tunnistusjärjestelmän <b>varmuuskopioinnista</b> huolehditaan suunnitelmallisesti.</p> <p>Varmuuskopioinnissa huomioidaan tiedon luokittelu (henkilötiedot, salaustekniset tiedot)</p> | <p><b>M72B 5.4 Käyttöturvallisuus</b></p> <p>Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:</p> <p>[...]</p> <p>e) varmuuskopiointi; sekä<br/>[...]</p>                                                                      | A.12.3.1 tietojen varmuuskopiointi                                                                                                                                                                                                                      | <p>Ohjeessa 211/2016 oli seuraavia huomioita, jotka ovat tässä mukana informatiivisina:</p> <p>Varmuuskopioiden fyysinen sijoituspaikka on riittävän eriytetty varsinaisesta järjestelmästä.</p>                                    |

|  |  |                                                                   |  |  |  |
|--|--|-------------------------------------------------------------------|--|--|--|
|  |  | jne.), järjestelmien palautettavuus ja varmuuskopioiden säilytys. |  |  |  |
|--|--|-------------------------------------------------------------------|--|--|--|

## B 4 Poikkeamien havainnointikyky ja hallinta ja häiriöilmoitukset

### KESKEISET SÄÄNNÖKSET

#### M72B 15 Vaatimuksenmukaisuuden arviointikriteerit

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):
- d) teknisiin toimenpiteisiin

#### Yleiset vaatimukset

#### TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset

4) tunnistusjärjestelmä on turvallinen ja luotettava siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdissa...2.4.6 vähintään korotetulle varmuustasolle säädetyt edellytykset täyttyvät ottaen huomioon kulloinkin käytettävissä olevaan tekniikkaan liittyvät tietoturvasuositukset

#### LoA Liite 2.4.6 Tekniset tarkastukset (controls)

1. Käytössä on oikeasuhteiset tekniset tarkastukset palvelujen turvallisuuteen kohdistuvien riskien hallitsemiseksi ja käsiteltävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi.
4. Käytössä on menettelyt, joilla varmistetaan, että turvallisuus säilyy ja että kyetään vastaamaan muutoksiin riskitasoissa, poikkeamiin ja tietoturvaloukkauksiin.

#### TunnL 16 § Tunnistuspalvelun tarjoajan velvollisuus ilmoittaa toimintaan ja tietojen suojaamiseen kohdistuvista uhkista tai häiriöistä

Tunnistuspalvelun tarjoajan on salassapitosäätöjen estämättä ilmoitettava ilman aiheutonta viivästystä tunnistuspalveluunsa luottaville osapuolille, tunnistusvälineiden haltijoille, muille luottamusverkostossa toimiville sopimuspuolilleen sekä Liikenne- ja viestintävirastolle palvelun toimivuuteen, tietoturvaan tai sähköisen henkilöllisyyden käyttöön kohdistuvista merkittävistä uhkista tai häiriöistä. [...]

Edellä 1 momentissa tarkoitettussa ilmoituksessa on kerrottava niistä toimista, joita eri tahoilla on käytettävissään uhkien tai häiriöiden torjumiseksi sekä näistä toimenpiteistä aiheutuvista arvioiduista kustannuksista.  
[...]

Vaatimuksia on tarkennettu määräyksen M72B 5 kohdassa ja 11 kohdassa.

| NRO | VARMUUSTASO | TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ | SÄÄNNÖKSET | STANDARDI-VIITTAUS | HUOMIOITA |
|-----|-------------|-------------------------------------------|------------|--------------------|-----------|
|-----|-------------|-------------------------------------------|------------|--------------------|-----------|

|     |      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                          |
|-----|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| 50. | S, H | <p>Tunnistusjärjestelmän poikkeamien havaitsemiseen on <b>kyvykkyys</b> ja ennalta <b>määritellyt prosessit</b>.</p> <p>Määrittelyissä huomioidaan järjestelmän tietoliikenneyhteyksien ja tietojärjestelmien komponenttien ja prosessien tärkeys/kriittisyys/luokittelu ja se, että turvallisuuteen liittyvät/vaikuttavat tapahtumat kyetään jäljittämään myös jälkikäteen.</p> <p>Tunnistusjärjestelmässä kerätään ja tallennetaan <b>tapahtumalokeja</b> järjestelmän toiminnasta ja tietoturvaan vaikuttavista/liittyvistä tapahtumista ja poikkeamista.</p> | <p><b>M72B 5.2 Tietoliikenneturvallisuus</b><br/>Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:<br/>[...]<br/>d) suodatuksen ja valvontajärjestelmien hallinnointi;<br/>[...]</p> <p><b>M72B 5.3 Tietojärjestelmäturvallisuus</b><br/>Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:<br/>a) pääsyoikeuksien hallinta vähimpien oikeuksien periaatteella;<br/>b) järjestelmien käyttäjien yksilöity tunnistaminen;<br/>[...]<br/>e) turvallisuuteen liittyvien tapahtumien jäljitys- ja jäljitysprosessi;<br/>f) poikkeamien havainnointikyky ja korjausprosessi; sekä<br/>[...]</p> | <p>A.12.4.1 käytöturvallisuus: tapahtumien kirjaaminen<br/>A.12.4.2 käytöturvallisuus: lokitietojen suojaaminen<br/>A.12.4.3 käytöturvallisuus: pääkäyttäjä- ja operaattorilokit<br/>A.16.1 tietoturvahäiriöiden hallinta/tietoturvahäiriöiden ja tietoturvasuuden parannusten hallinta<br/>A. 16.1.1 vastuut ja menettelyt<br/>A.16.1.6 tietoturvahäiriöistä oppiminen</p> | <p>Prosessit sisältävät niin automaattiset kuin manuaalisetkin keinot. Prosessit ovat ylläpidettyjä.</p> |
| 51. | S, H | <p>Tunnistusjärjestelmän <b>hallintalokit</b> on määritelty ja eriytetty muista lokeista. Niiden eheydestä on huolehdittu.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                   | <p><b>M72B 5.2 Tietoliikenneturvallisuus</b><br/>Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:<br/>[...]<br/>d) suodatuksen ja valvontajärjestelmien hallinnointi;<br/>e) turvalliset hallintayhteydet; sekä<br/>[...]</p> <p><b>M72B 5.3 Tietojärjestelmäturvallisuus</b><br/>Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:</p>                                                                                                                                                                                                                                                  | <p>A.12.4.1 käytöturvallisuus: tapahtumien kirjaaminen<br/>A.12.4.2 käytöturvallisuus: lokitietojen suojaaminen<br/>A.12.1.4 kehitys-, testaus-</p>                                                                                                                                                                                                                         | <p>hallintalokeihin tallennetaan tiedot tunnustusjärjestelmässä tehtävistä muutoksista</p>               |

|     |      |                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                              |
|-----|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |      |                                                                                                                                                                                                                                                                                                         | <p>a) pääsyoikeuksien hallinta vähimpien oikeuksien periaatteella;</p> <p>b) järjestelmien käyttäjien yksilöity tunnistaminen;</p> <p>[...]</p> <p>e) turvallisuuteen liittyvien tapahtumien jäljitys- ja jäljitysprosessi;</p> <p>f) poikkeamien havainnointikyky ja korjausprosessi; sekä</p> <p>[...]</p>                                                                                                                                                                                                                                                                            | ja tuotanto-<br>ympäristöjen<br>erottaminen                                                                                                                                                                                                                                           |                                                                                                                                                                                              |
| 52. | S, H | <p>Tunnistusjärjestelmän toimintaa, muutoksia ja tapahtumalokeja <b>monitoroidaan</b> poikkeamien ja tietoturvaloukkausten havaitsemiseksi.</p> <p>Tunnistusjärjestelmän <b>poikkeamat ja häiriöt käsitellään ja analysoidaan</b> ja niiden vaikuttavuus/vakavuus luokitellaan suunnitelmallisesti.</p> | <p><b>M72B 5.2 Tietoliikenneturvallisuus</b><br/>Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:</p> <p>[...]</p> <p>d) suodatuksen ja valvontajärjestelmien hallinnointi;</p> <p>[...]</p> <p><b>M72B 5.3 Tietojärjestelmäturvallisuus</b><br/>Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:</p> <p>[...]</p> <p>e) turvallisuuteen liittyvien tapahtumien jäljitys- ja jäljitysprosessi;</p> <p>f) poikkeamien havainnointikyky ja korjausprosessi; sekä</p> <p>[...]</p> | <p>A.16.1 tietoturvahäiriöiden hallinta/tietoturvahäiriöiden ja parannusten hallinta:</p> <p>A.16.1.2 tietoturvatapahtumien raportointi</p> <p>A.16.1.3 tietoturvaheikkouksien raportointi</p> <p>A.16.1.4 tietoturvatapahtumien arviointi ja niitä koskevien päätösten tekeminen</p> | <p>Kaikki havainnot käsitellään ja niiden vaikuttavuus luokitellaan sovittujen menetelmien mukaan.</p> <p>Lokien analysointiin käytetään automaattisia prosesseja/työkaluja, kuten SIEM.</p> |
| 53. | S, H | <p>Tunnistusjärjestelmän poikkeamien ja häiriöiden edellyttämät <b>korjaavat toimenpiteet</b> ovat suunnitelmallisia ja tehokkaita.</p> <p>Toiminnan jatkuvuussuunnittelu sisältää ennalta ehkäiseviä ja</p>                                                                                            | <p><b>M72B 5.2 Tietoliikenneturvallisuus</b><br/>Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:</p> <p>[...]</p> <p>d) suodatuksen ja valvontajärjestelmien hallinnointi;</p> <p>[...]</p> <p><b>M72B 5.3 Tietojärjestelmäturvallisuus</b></p>                                                                                                                                                                                                                                                                                     | <p>A.16.1. tietoturvahäiriöiden hallinta/tietoturvahäiriöiden ja parannusten hallinta:</p>                                                                                                                                                                                            | <p>Korjaavat toimenpiteet tulee dokumentoida.</p> <p>Saatavuusvaatimukset (SLA) ovat sopimusasia, huomioitava syrjimättömyys</p>                                                             |

|     |      |                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                       |                                                                           |
|-----|------|----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
|     |      | korjaavia toimenpiteitä, joilla minimoidaan merkittävien toimintahäiriöiden tai poikkeuksellisten tapahtumien vaikutukset.       | Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:<br>[...]<br>e) turvallisuuteen liittyvien tapahtumien jäljitys- ja jäljitysprosessi;<br>f) poikkeamien havainnointikyky ja korjausprosessi; sekä<br>[...]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | A.16.1.5 tietoturvahäiriöihin vastaaminen<br><br>7.5 Dokumentoitu tieto<br><br>10.1 Poikkeamat ja korjaavat toimenpiteet                              |                                                                           |
| 54. | S, H | Häiriönhallintaprosesseissa on huomioitu <b>ilmoitusvelvollisuus muille luottamusverkostoon kuuluville tunnistuspalveluille.</b> | <b>TunnL 16 § Tunnistuspalvelun tarjoajan velvollisuus ilmoittaa toimintaan ja tietojen suojaamiseen kohdistuvista uhkista tai häiriöistä</b><br>Tunnistuspalvelun tarjoajan <u>on</u> salassapitosään-<br>nösten estämättä <u>ilmoitettava</u> ilman aiheutonta<br>viivästystä [...] tunnistuspalveluunsa muille luotta-<br>musverkostossa toimiville sopimuspuolilleen [...] palvelun toimivuuteen, tietoturvaan tai sähköisen<br>henkilöllisyyden käyttöön kohdistuvista merkittä-<br>vistä uhkista tai häiriöistä. [...]<br><br>Tunnistuspalvelun tarjoaja <u>voi</u> salassapitosään-<br>nösten estämättä <u>ilmoittaa</u> kaikille luottamusver-<br>koston jäsenille 1 momentissa tarkoitetuista uh-<br>kista ja häiriöistä sekä palvelun tarjoajista, joiden<br>on syytä epäillä tavoittelevan oikeudetonta talou-<br>dellista hyötyä, antavan merkityksellisiä totuuden-<br>vastaisia tai harhaanjohtavia tietoja tai käsittele-<br>vän henkilötietoja lainvastaisesti.<br><br><b>Soveltaminen:</b><br>Luottamusverkoston yhteistoimintaryhmässä on<br>laadittu yhteinen käytäntö keskinäisistä häiriöil-<br>moitustilanteista ja ilmoituskynnyksistä. | A.16.1.2 tietoturvahäiriöiden hal-<br>linta/tietotur-<br>vahäiriöiden ja<br>parannusten<br>hallinta: tieto-<br>turvatapahtu-<br>mien rapor-<br>tointi | Vastuut poikkeamatilantei-<br>siin ja sidosryhmäviestintään on määritelty |
| 55. | S, H | Häiriönhallintaprosesseissa on huomioitu <b>ilmoitusvelvollisuus käyttäjille ja luottaville osapuolille.</b>                     | <b>TunnL 16 § Tunnistuspalvelun tarjoajan velvollisuus ilmoittaa toimintaan ja tietojen suojaamiseen kohdistuvista uhkista tai häiriöistä</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | A.16.1.2 tietoturvahäiriöiden hal-                                                                                                                    | Vastuut poikkeamatilantei-<br>siin ja sidosryhmäviestintään on määritelty |

|     |      |                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                     |                                                                                                                                                                                      |
|-----|------|--------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |      |                                                                                                        | Tunnistuspalvelun tarjoajan on [...] ilmoitettava ilman aiheutonta viivästystä tunnistuspalveluunsa luottaville osapuolille, tunnistusvälineiden haltijoille, [...] palvelun toimivuuteen, tietoturvaan tai sähköisen henkilöllisyyden käyttöön kohdistuvista merkittävistä uhkista tai häiriöistä. Ilmoituksessa on kerrottava niistä toimista, joita eri tahoilla on käytettävissään uhkien tai häiriöiden torjumiseksi sekä näistä toimenpiteistä aiheutuvista arvioituista kustannuksista.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | linta/tietoturvahäiriöiden ja parannusten hallinta: tietoturvatapahtumien raportointi                                                                               | Luottavilla osapuolilla tarkoitetaan asiointipalveluita                                                                                                                              |
| 56. | S, H | Häiriönhallintaprosesseissa on huomioitu <b>ilmoitusvelvollisuus Liikenne- ja viestintävirastolle.</b> | <p><b>TunnL 16 § Tunnistuspalvelun tarjoajan velvollisuus ilmoittaa toimintaan ja tietojen suojaamiseen kohdistuvista uhkista tai häiriöistä</b></p> <p>Tunnistuspalvelun tarjoajan on salassapitosäännösten estämättä ilmoitettava ilman aiheutonta viivästystä [...] Liikenne- ja viestintävirastolle palvelun toimivuuteen, tietoturvaan tai sähköisen henkilöllisyyden käyttöön kohdistuvista merkittävistä uhkista tai häiriöistä. Ilmoituksessa on kerrottava niistä toimista, joita eri tahoilla on käytettävissään uhkien tai häiriöiden torjumiseksi sekä näistä toimenpiteistä aiheutuvista arvioituista kustannuksista.</p> <p><b>M72B 11 Tunnistuspalveluntarjoajan häiriöilmoitukset Liikenne- ja viestintävirastolle</b></p> <p><b>11.1 Merkittävät uhkat tai häiriöt</b></p> <p>Liikenne- ja viestintävirastolle tunnistus- ja luottamuspalvelulain 16 §:n mukaisesti ilmoitettavia merkittäviä tunnistuspalvelun häiriöitä ovat tapahtumat, jotka liittyvät sähköisen henkilöllisyyden virheellisyyteen tai väärinkäyttöön tai tietoturvaan tai -häiriöön, joka vaarantaa tunnistamisen eheyden ja luotettavuuden. Merkittäviä ovat myös ennakoimattomat toimivuushäiriöt, joilla on vähäistä suurempia haittavaikutuksia luottamusverkostoon.</p> <p><b>11.2 Ilmoitettavat tiedot</b></p> | <p>A.6.1.3 Yhteydet viranomaisiin</p> <p>A.16.1.2 tietoturvahäiriöiden hallinta/tietoturvahäiriöiden ja parannusten hallinta: tietoturvatapahtumien raportointi</p> | <p>Noudatetaan luottamusverkoston yhdessä määrittelemää dokumenttia ilmoituskynnyksen ylittymisestä.</p> <p>Vastuut poikkeamatilanteisiin ja sidosryhmäviestintään on määritelty</p> |

|  |  |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |  |  |
|--|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
|  |  |  | <p>Liikenne- ja viestintävirastolle tehtävässä merkittävää uhkaa tai häiriötä koskevassa ilmoituksessa on annettava vähintään seuraavat tiedot:</p> <ol style="list-style-type: none"> <li>1) tunnistusväline tai tunnistusvälityspalvelu, johon häiriö tai uhka vaikuttaa;</li> <li>2) kuvaus häiriöstä tai uhkasta ja sen tiedossa olevista syistä sekä kestosta;</li> <li>3) kuvaus häiriön tai uhkan vaikutuksista, mukaan lukien vaikutus uusien tunnistusvälineiden myöntämiseen, käyttäjiin, luottaviin osapuoliin, muihin luottamusverkoston toimijoihin ja rajat ylittävään käyttöön;</li> <li>4) kuvaus korjaustoimenpiteistä; sekä</li> <li>5) kuvaus häiriöstä tai uhkasta tiedottamisesta luottaville osapuolille, tunnistusvälineiden haltijoille, luottamusverkostolle ja tieto ilmoittamisesta muille viranomaisille.</li> </ol> <p><b>11.3 Ilmoitusmenettely</b><br/>Ilmoitus merkittävästä häiriöstä tai uhkasta on tehtävä sähköisesti Liikenne- ja viestintäviraston verkkolomakkeella, sähköpostilla tai turvasähköpostilla.<br/>Ilmoituksen tietoja voi täydentää myöhemmin, jos kaikki tiedot eivät ole käytettävissä, kun tehdään ensi-ilmoitus tunnistus- ja luottamuspalvelulain 16 §:n mukaisesti ilman aiheetonta viivästystä.</p> <p><b>MPS72B soveltamisohje ilmoituskynnyksestä Liikenne- ja viestintävirastolle</b>, kappale 4.11.1<br/>Säännös 11.1:<br/>Määräyksen säännöksessä 11.1 määritellään yleisellä tasolla niitä tekijöitä, jotka ovat olennaisia häiriön tai uhkan merkittävyyden eli ilmoituskynnyksen kannalta. Tällaisia merkittäviä häiriöitä ovat muun muassa:<br/>- tunnistusvälineen myöntäminen väärälle henkilölle,</p> |  |  |
|--|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|

|  |  |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |  |  |
|--|--|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
|  |  |  | <p>- sellaiset sulkulistojen toimivuuteen liittyvät häiriöt, joissa ajantasaista sulkulistaa ei ole saatavilla,</p> <p>- tunkeutuminen palveluntarjoajan järjestelmiin,</p> <p>- tunnistusvälineen tarjoajan varmenteiden allekirjoitusavaimien paljastuminen,</p> <p>- tunnistusvälineiden vakavat väärinkäytökset kuten tapaukset, jotka liittyvät tunnusten ketjuttamiseen,</p> <p>- vakavat sisäiset väärinkäytökset.</p> <p>Sähköisen henkilöllisyyden virheitä tai väärinkäytöksiä pidetään merkittävänä hyvin matalalla kynnyksellä, samoin esimerkiksi haavoittuvuuksia tai virheitä, jotka vaarantavat tunnistamistiedon oikeellisuuden. Sen sijaan käytettävyyss- tai laatuongelmien ilmoituskynnys on lähtökohtaisesti korkeampi ja niiden merkittävyyttä lisää lähinnä se, että ongelma vaikuttaa muihin luottamusveroston toimijoihin. Tällaisia ongelmia ovat pitkät tunnistusvälineen tai tunnistusvälityspalvelun häiriötilanteet, jotka estävät tunnistuspalveluiden välittämisen asiointipalveluille. Myös ensitunnistamisen ketjuttamisen pitkään estävä häiriö on merkittävä.</p> |  |  |
|--|--|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|

## B 5 Tietojen säilyttäminen ja käsittely

### KESKEISET SÄÄNNÖKSET

#### M72B 15 Vaatimuksenmukaisuuden arviointikriteerit

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):
  - b) tietojen säilyttämiseen ja käsittelyyn
  - d) teknisiin toimenpiteisiin

#### Yleiset vaatimukset

#### TunnL 13 § Tunnistuspalvelun tarjoajan yleiset velvollisuudet

Tunnistuspalvelun tarjoajan tunnistamiseen liittyvien tietojen säilyttämisen, henkilökunnan ja alihankintana käyttämien palvelujen tulee täyttää sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdissa 2.4.4 ja 2.4.5 vähintään korotetulle varmuustasolle säädetyt vaatimukset.

[...]

Tunnistamispalvelun tarjoajan on lisäksi huolehdittava palvelujensa henkilötietolain 32 §:ssä tarkoitetusta tietojen suojaamisesta sekä riittävästä tietoturvasta.

#### LoA Liite 2.4.4 Tietojen säilyttäminen

1. Asiaankuuluvat tiedot kirjataan ja säilytetään käyttämällä tehokasta tiedonhallintajärjestelmää ottaen huomioon sovellettava lainsäädäntö ja tietosuojan ja tietojen säilyttämiseen liittyvät hyvät käytännöt.
2. Järjestelmään kirjatut tiedot säilytetään siltä osin kuin tämä on kansallisen lainsäädännön tai muun kansallisen hallinnollisen järjestelyn mukaan sallittua ja suojataan niin kauan kuin niitä tarvitaan tarkastuksia ja tietoturvaloukkausten tutkimista varten ja säilytetään siihen asti, kun tiedot hävitetään turvallisesti.

#### TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset

4) tunnustusjärjestelmä on turvallinen ja luotettava siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdissa [...] 2.4.6 vähintään korotetulle varmuustasolle säädetyt edellytykset täyttyvät ottaen huomioon kulloinkin käytettävissä olevaan tekniikkaan liittyvät tietoturvallisuusuhat

#### LoA Liite 2.4.6 Tekniset tarkastukset (controls)

1. Käytössä on oikeasuhteiset tekniset tarkastukset palvelujen turvallisuuteen kohdistuvien riskien hallitsemiseksi ja käsiteltävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi.

Korotettu: Arkaluonteinen salaustekninen aineisto, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, on suojattu luvattomalta käsittelyltä.

| NRO | VARMUUSTASO | TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ                                                                                                      | SÄÄNNÖKSET                                                                                                                                                                                                                                                                                                                                                                                                                                                     | STANDARDI-VIITTAUS                                                                                                                                                                 | HUOMIOITA                                                                                                                                                                       |
|-----|-------------|------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 57. | S, H        | Tunnistusjärjestelmään ja tunnistamiseen liittyvien <b>tietojen hallinta on suunnitelmallista</b> ja perustuu <b>tietojen luokitte- luun</b> . | <p><b>LoA Liite 2.4.4 Tietojen säilyttäminen</b></p> <p>1. Asiaankuuluvat tiedot kirjataan ja säilytetään käyttämällä tehokasta <u>tiedonhallintajärjestelmää</u> ottaen huomioon sovellettava lainsäädäntö ja tietosuojan ja tietojen säilyttämiseen liittyvät hyvät käytännöt.</p> <p><b>LoA Liite 2.4.6 Tekniset tarkastukset (controls)</b></p> <p>1. Käytössä on oikeasuhteiset tekniset tarkastukset palvelujen turvallisuuteen kohdistuvien riskien</p> | <p>A.8.2.1 suo- jattavan omai- suuden hal- linta/tietojen luokittelu: tie- don luokittelu</p> <p>A.18.1.4 vaa- timustenmu- kaisuus/lain- säädäntöön ja sopimuksiin sisältyvien</p> | Luokittelussa huomioidaan esim. salaustekniset tie- dot, tunnistustapahtuma- tiedot, henkilötiedot, liike- salaisuudet ja järjestel- mien turvallisuuteen vai- kuttavat tiedot. |

|     |      |                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----|------|--------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |      |                                                                                                                                      | <p>hallitsemiseksi ja <u>käsiteltävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi</u>.</p> <p>Korotettu: Arkaluonteinen <u>salaustekninen aineisto</u>, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, on suojattu luvattomalta käsittelyltä.</p> <p><b>M72B 5.4 Käyttöturvallisuus</b><br/>Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:<br/>[...]<br/>2. tiedon luokitteluun perustuva salassa pidettävän aineiston käsittely-ympäristö ja säilytys;<br/>[...]</p>                                                                                           | <p>vaatimusten noudattaminen: tietosuoja ja henkilötietojen suojaaminen</p>                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 58. | S, H | <p>Tiedonhallinnan suunnittelussa on huomioitu tiedon koko <b>elin-kaari</b>.</p> <p>Tietojen <b>säilytysajat</b> on määriteltä.</p> | <p><b>LoA Liite 2.4.4 Tietojen säilyttäminen</b><br/>2. Järjestelmään kirjatut tiedot <u>säilytetään</u> siltä osin kuin tämä on kansallisen lainsäädännön tai muun kansallisen hallinnollisen järjestelyn mukaan sallittua ja <u>suojetaan</u> niin kauan kuin niitä tarvitaan tarkastuksia ja tietoturvaloukkausten tutkimista varten ja säilytetään siihen asti, kun tiedot hävitetään turvallisesti.</p> <p><b>M72B 5.4 Käyttöturvallisuus</b><br/>Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:<br/>[...]<br/>b) tiedon luokitteluun perustuva salassa pidettävän aineiston käsittely-ympäristö ja säilytys;<br/>[...]</p> | <p>A.8.1.1 Suojattavan omaisuuden luettelointi</p> <p>A.18.1.4 vaatimustenmukaisuus/lainsäädäntöön ja sopimuksiin sisältyvien vaatimusten noudattaminen: tietosuoja ja henkilötietojen suojaaminen</p> | <p>Huomioon on otettava mm. turvallisuuteen liittyvien tapahtumien jäljitettävyyden ja tunnistuslain 24 §:ää <i>vastaavien</i> käsittelyperusteiden aiheuttamat tarpeet.</p> <p>Yksityiskohtana ftn_chain_level -attribuutin käyttäminen ensitunnistuksen yhteydessä.</p> <p>Ohjeessa 211/2016 oli seuraavia huomioita, jotka ovat tässä mukana informatiivisina:<br/>Lokeille pitää määritellä säilöntään riittävän pitkä aika jälkikäteen tapahtuvaa selvitystä varten.</p> |

|     |      |                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                     |                                                                                                                                                                                                                  |
|-----|------|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 59. | S, H | Tunnistustalain 24 §:ssä säädettyistä erityisistä tallennusvelvollisuuksista on huolehdittu. | <p><b>TunnL 24 § Tunnistustapahtumaa ja tunnistusvälinettä koskevien tietojen tallentaminen ja käyttö</b></p> <p>Tunnistuspäalvelun tarjoajan on tallennettava:</p> <ol style="list-style-type: none"> <li>1) yksittäisen tunnistustapahtuman ja sähköisen allekirjoittamisen tapahtuman todentamiseksi tarvittavat tiedot;</li> <li>2) tiedot 18 §:ssä tarkoitetuista tunnistusvälineen käyttöön liittyvistä estoista ja käyttörajoituksista;</li> <li>3) varmenteen osalta 19 §:ssä tarkoitettun varmenteen tietosisältö.</li> </ol> <p>Tunnistusvälineen tarjoajan on tallennettava tarvittavat tiedot 17 ja 17 a §:ssä tarkoitettusta hakijan ensitunnistamisesta ja siinä käytetystä asiakirjasta tai sähköisestä tunnistamisesta.</p> <p>Edellä 1 momentin 1 kohdassa tarkoitettut tiedot on säilytettävä viiden vuoden ajan tunnistustapahtumasta. Muut 1 ja 2 momentissa tarkoitettut tiedot on säilytettävä viiden vuoden ajan vakituisen asiakassuhteen päättymisestä.</p> <p>Tunnistustapahtuman yhteydessä syntyneet henkilötiedot on hävitettävä tunnistustapahtuman jälkeen, jollei tallentaminen ole välttämätöntä yksittäisen tunnistustapahtuman todentamiseksi.</p> <p>Tunnistuspäalvelun tarjoaja saa käsitellä tallennettuja tietoja ainoastaan palvelun toteuttamiseksi ja ylläpitämiseksi, laskutusta varten, omien oikeuksien turvaamista varten riitatilanteissa, väärinkäytöstilanteiden selvittämisessä sekä tunnistuspalvelua käyttävän palveluntarjoajan tai tunnistusvälineen haltijan pyynnöstä. Tunnistuspäalvelun tarjoajan on tallennettava tieto käsittelyn ajankohdasta, syystä ja käsittelijästä.</p> | A.12.4.1 käytöturvallisuus: tapahtumien kirjaaminen | "...ainoastaan laskee liikkeelle tunnistusvälineitä" tarkoittaa säännöksessä dvv:n varmenteen kaltaista tunnistuspäalvelua, jossa tunnistusvälineen myöntäjä ei välitä tunnistustussanomia tunnistustapahtumassa |
|-----|------|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|     |      |                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                         |
|-----|------|------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |      |                                                                                                                                                | Jos palveluntarjoaja ainoastaan laskee liikkeelle tunnistusvälineitä:<br>1) 1 momentin 1 kohtaa ja 4 momenttia ei sovelleta siihen;<br>2) 3 momentissa tarkoitettu viiden vuoden tallennusaika lasketaan tunnistusvälineen voimassaolon päättymisestä.                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                         |
| 60. | S, H | Tunnistustalain 24 §:n erityisvaatimus tallennettavaksi säädetyjen tietojen käsittelyyn liittyvien tietojen tallentamisesta.                   | <b>TunnL 24 § Tunnistustapahtumaa ja tunnistusvälinettä koskevien tietojen tallentaminen ja käyttö</b><br>[...]<br>Tunnistuspalvelun tarjoaja saa käsitellä tallennettuja tietoja ainoastaan palvelun toteuttamiseksi ja ylläpitämiseksi, laskutusta varten, omien oikeuksien turvaamista varten riitatilanteissa, väärinkäytöstilanteiden selvittämisessä sekä tunnistuspalvelua käyttävän palveluntarjoajan tai tunnistusvälineen haltijan pyynnöstä. <u>Tunnistuspalvelun tarjoajan on tallennettava tieto käsittelyn ajankohdasta, syystä ja käsitteijästä.</u><br>[...]                                                                                                    | A.12.4.1 käytöturvallisuus: tapahtumien kirjaaminen<br><br>A.12.4.3 Pääkäyttäjä- ja operaattorilokit                                                                                           | Huomioitava käsittelytietojen jäljitettävyyden ja lokien eheyden turvaaminen                                                                                                                                                                                                                                                            |
| 61. | S, H | Tunnistusjärjestelmässä käsiteltävien ja säilytettävien tietojen eheydestä ja luottamuksellisuudesta on huolehdittu teknisillä toimenpiteillä. | <b>TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset</b><br>[...]<br>4) tunnistusjärjestelmä on turvallinen ja luotettava siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdissa...2.4.6 vähintään korotetulle varmuustasolle säädetyt edellytykset täyttyvät ottaen huomioon kulloinkin käytävissä olevaan tekniikkaan liittyvät tietoturvalisuushat<br><br><b>LoA Liite 2.4.6 Tekniset tarkastukset</b> (controls)<br>1. Käytössä on oikeasuhteiset tekniset tarkastukset palvelujen turvallisuuteen kohdistuvien riskien hallitsemiseksi ja käsiteltävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi. | A.9.1.1 pääsynhallintapolitiikka<br><br>A.9.1.2 pääsy verkkoihin ja verkkopalveluihin<br><br>A.10.1.1 salauksen käytön periaatteet<br><br>A.12.4.2 käytöturvallisuus: lokitietojen suojaaminen | Tiedon salaus ja/tai pääsynhallinta<br><br>Eriyttäminen tarvittaessa (vrt. erityisesti salaustekninen aineisto)<br><br>Varmuuskopiointi/palautettavuus<br><br>Suosituksessa salausvaatimuksille määritelty avainenvaihto voi olla relevantti tunnistuspalvelun ja sen alihankkijan välillä, vaikka se ei ole relevantti levysalauksessa |

|  |  |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                         |
|--|--|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  |  | <p>Korotettu: Arkaluonteinen salaustekninen aineisto, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, on suojattu luvattomalta käsittelyltä.</p> <p><b>M72B 5.4 Käyttöturvallisuus</b><br/>Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:<br/>[...]<br/>b) tiedon luokitteluun perustuva salassa pidettävän aineiston käsittely-ympäristö ja säilytys;<br/>[...]<br/>e) varmuuskopiointi; sekä<br/>f) käytettävä kansainvälisesti tai kansallisesti suositeltuja salausratkaisuja.</p> <p><b>M72B 7 Tunnistusjärjestelmän rajapintojen salausvaatimukset</b><br/><b>7.1 Tietoliikenteen salausmenetelmät</b><br/>7.1.1<br/>Tunnistuspalvelun tarjoajien välisten ja tunnistuspalvelun tarjoajan ja luottavan osapuolen välisten rajapintojen liikenne on salattava. Salauksessa, avaintenvaihdossa, varmenteissa sekä salaukseen liittyvässä allekirjoituksessa on noudatettava seuraavia menetelmiä:<br/>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.<br/>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</p> | <p>Luottosuhteen perustana olevien salaisuuksien hallinta ja turvaaminen</p> <p>Säilyttämisessä täytyy huomioida fyysisen sijoi-<br/>tuspaikan eriyttäminen<br/>varsinaisesta järjestel-<br/>mästä.</p> |
|--|--|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|  |  |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |  |  |
|--|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
|  |  |  | <p>EdDSA:ta äärellisen kunnan koon tulee olla vähintään 224 bittiä.</p> <p>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.</p> <p>4) Tiivistefunktiot: Tiivistefunktion tai autentikaatiokoodin on oltava SHA-2, SHA-3, Whirlpool tai Poly1305.</p> <p>7.1.2<br/>Kohdassa 7.1.1 mainittujen lisäksi voidaan noudattaa menetelmiä ja arvoja, jotka on arvioitu turvallisiksi 1-4 alakohdissa tarkoitettuun käyttöön seuraavien asiakirjojen ajantasaisissa versioissa:</p> <p>a) Liikenne- ja viestintävirastossa toimivan salaustuotteiden hyväksyntäviranomaisen (Crypto Approval Authority) ohje Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset turvallisuusluokat (Dnro 190/651/2015); tai</p> <p>b) eräiden Euroopan unionin tai ETA-alueen jäsenvaltioissa toimivien sertifiointielinten välisen SOGIS-MRA (Senior Officers Group for Information Systems, Mutual Recognition Agreement) asiakirja SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms.</p> <p>7.1.3<br/>Salausasetukset tulee teknisesti pakottaa edellä lueteltuihin vähimmäistasoihin, jotta yhteyskätteilyissä ei päädyttäisi vähimmäistasoja heikompiin asetuksiin.</p> <p><b>7.2 Tietoliikenteen salausprotokolla</b><br/>Mikäli yhteyskäytännössä käytetään TLS-protokollaa, tulee käyttää vähintään TLS versiota 1.2.</p> |  |  |
|--|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|

|     |   |                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |          |                                                                                  |
|-----|---|---------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|----------------------------------------------------------------------------------|
| 62. | H | Tietojen käsittelyssä ja säilyttämisessä noudatetaan <b>suositusten</b> mukaisia tiukennettuja/korkean tason salausvaatimuksia. | <p><b>MPS M72B kohta 4.7.1.3 (20.5.2022) suositus</b></p> <p>Korkealla varmuustasolla tunnistusjärjestelmässä suositellaan sovellettavaksi määräyksessä säännöksessä 7.1 edellytettyjen korotetun varmuustason vaatimusten sijaan seuraavassa esitettyjä su-<br/>luissa olevia arvoja, <b>joilla saavutetaan vähintään 128 bitin vahvuustaso</b>:</p> <ol style="list-style-type: none"> <li>1) <b>Avaintenvaihto</b>: Avaintenvaihdossa on käytettävä DHE-menetelmiä tai elliptisiä käyriä käyttäviä ECDHE-menetelmiä. Laskutoimituksissa käytetyn äärellisen kunnan (finite field) koon tulee olla DHE-menetelmässä vähintään 2048 (<b>korkealla varmuustasolla 4096</b>) bittia ja ECDHE-menetelmässä vähintään 224 (<b>korkealla varmuustasolla 256</b>) bittia.</li> <li>IANA:n IKEv2-määrittysten mukaiset DH-ryhmät 14 - 21, 23, 24 ja 26 (<b>korkealla varmuustasolla 16 - 21</b>) toteuttavat edellä mainitut edellytykset.</li> <li>2) Allekirjoitus tai epäsymmetrinen salaus: Käytettäessä RSA:ta sähköiseen allekirjoitukseen tai salaukseen, avaimen pituuden tulee olla vähintään 2048 (<b>korkealla varmuustasolla 3072</b>) bittia. Käytettäessä elliptisen käyrän menetelmää ECDSA:ta tai EdDSA:ta, alla olevan kunnan koon tulee olla vähintään 224 (<b>korkealla varmuustasolla 256</b>) bittia.</li> <li>3) Symmetrinen salaus: Salausalgoritmin on oltava AES, Serpent tai ChaCha20 (<b>korkealla varmuustasolla AES tai Serpent</b>). Avaimen pituuden tulee olla vähintään 128 (<b>korkealla varmuustasolla 128</b>) bittia. Salausmoodin on oltava CBC, CCM, GCM tai CTR.</li> </ol> | ks. yllä | Avaintenvaihto voi olla relevantti tunnistuspalvelun ja sen alihankkijan välillä |
|-----|---|---------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|----------------------------------------------------------------------------------|

|     |      |                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                               |                                     |
|-----|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|
|     |      |                                                                                                                                                                                                     | 4) Tiivistefunktiot: Tiivistefunktion tai autentikaatiokoodin on oltava SHA-2, SHA-3, Whirlpool tai Poly1305. SHA-2:lla tarkoitetaan funktioita SHA224, SHA256, SHA384 ja SHA512 ( <b>korkealla varmuustasolla SHA-3-256, SHA-3-384, SHA-3-512</b> )                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                               |                                     |
| 63. | S, H | Kaikki <b>laitteet ja välineet</b> , jotka sisältävät henkilötietoja, salattuja tietoja tai muita arkaluonteisia tietoja, säilytetään, kuljetetaan ja hävitetään turvallisella ja varmalla tavalla. | <p><b>LoA Liite 2.4.6 Tekniset tarkastukset</b> (controls)</p> <p>5) Kaikki <u>laitteet ja välineet</u>, jotka sisältävät henkilötietoja, salattuja tietoja tai muita arkaluonteisia tietoja, säilytetään, kuljetetaan ja hävitetään turvallisella ja varmalla tavalla.</p> <p><b>M72B 5.4 Käyttöturvallisuus</b></p> <p>Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:</p> <p>[...]</p> <p>b) tiedon luokitteluun perustuva salassa pidettävän aineiston käsittely-ympäristö ja säilytys;</p> <p>[...]</p> | <p>A.8.3 Suojattava omaisuus/tietovälineiden käsittely</p> <p>A.11.2.6 toimitilojen ulkopuolelle vietyjen laitteiden ja suojattavan omaisuuden turvallisuus</p> <p>A.11.2.7 laitteiden turvallinen käytöstä poistaminen ja kierrättäminen</p> | hallinta, hävittäminen, siirtäminen |

## B 6 Tilaturvallisuus

### KESKEISET SÄÄNNÖKSET

#### M72B 15 Vaatimuksenmukaisuuden arviointikriteerit

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):
- c) tiloihin ja [...]

#### TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset

- 4) tunnistusjärjestelmä on turvallinen ja luotettava siten, että [...] tunnistuspalvelun tarjoamiseen käytettävät tilat ovat turvallisia sähköisen tunnistamisen varmuus-tasoasetuksen liitteen kohdassa 2.4.5 säädetyllä tavalla;

| NRO | VARMUUS-TASO | TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | SÄÄNNÖKSET                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | STANDARDI-VIITTAUS                                                                                                                                                                                                                                             | HUOMIOITA                                                                                                                                                                                                                                                           |
|-----|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 64. | S, H         | <p><b>Tilaturvallisuus</b></p> <p>Tunnistusjärjestelmän tilat on jaettu turvavyöhykkeisiin käsiteltävän tiedon luottamuksellisuus ja kriittisyys huomioiden.</p>                                                                                                                                                                                                                                                                                                                                                                                                                    | <p><b>LoA Liite 2.4.5 Tilat ja henkilökunta</b></p> <p>3. Palvelun tarjoamiseen käytetyt tilat ovat jatkuvasti seurattuja ja suojattuja ympäristötapahtumien aiheuttamilta vahingoilta, luvattomalta käytöltä ja muilta tekijöiltä, jotka voivat vaikuttaa palvelun turvallisuuteen.</p> <p>4. Palvelun tarjoamiseen käytetyissä tiloissa varmistetaan, että <u>pääsy alueille</u>, joilla säilytetään tai käsitellään henkilötietoja, salattuja tietoja tai muita arkaluonteisia tietoja, rajoitetaan koskemaan valtuutettuja henkilöstön jäseniä tai alihankkijoita.</p>        | <p>A.11.1 fyysinen turvallisuus ja ympäristön turvallisuus/turva-alueet:</p> <p>A.11.1.1 fyysinen turva-alue</p>                                                                                                                                               | <p>Kaikki tunnistuspalvelun tuotantoon liittyvät/vaikuttavat tilat, myös alihankkijat</p> <p>Mahdollinen Katakriin täyttäminen oletusarvoisesti riittävä, jos tunnistusjärjestelmän tuottaminen ko. tiloissa. Muiden standardien kattavuutta ei ole selvitetty.</p> |
| 65. | S, H         | <p>Tunnistuspalvelun tuotannossa käytettävät laitteistot <b>on suojattu</b> murtoa, ilkeävaltaa, paloa, lämpöä, kaasuja, pölyä, ääntä, vettä ja sähkökäytön katkoksia vastaan. Suojauksen vahvuudessa on huomioitu turvavyöhykkeet.</p> <p>Tiloissa on toteutettu tarkoituksenmukainen <b>kulunvalvonta</b>/pääsynvalvonta jolla varmistetaan siitä, että vain asianomaisilla henkilöillä on pääsy.</p> <p>Tietojen fyysiseen suojaamiseen tarkoitetut turvallisuusjärjestelmät ja laitteet ovat yleisesti käytettyjen teknisten standardien tai vähimmäisvaatimusten mukaisia.</p> | <p><b>LoA Liite 2.4.5 Tilat ja henkilökunta</b></p> <p>3. Palvelun tarjoamiseen käytetyt tilat ovat <u>jatkuvasti seurattuja ja suojattuja</u> ympäristötapahtumien aiheuttamilta vahingoilta, luvattomalta käytöltä ja muilta tekijöiltä, jotka voivat vaikuttaa palvelun turvallisuuteen.</p> <p>4. Palvelun tarjoamiseen käytetyissä tiloissa varmistetaan, että <u>pääsy alueille</u>, joilla säilytetään tai käsitellään henkilötietoja, salattuja tietoja tai muita arkaluonteisia tietoja, rajoitetaan koskemaan valtuutettuja henkilöstön jäseniä tai alihankkijoita.</p> | <p>A.11.1.2 kulunvalvonta</p> <p>A.11.1.3 toimistojen, tilojen ja laitteistojen suojaus,</p> <p>A.11.1.4 suojaus ulkoisia ja ympäristön aiheuttamia uhkia vastaan</p> <p>A.11.2.1 laitteiden sijoitus ja suojaus</p> <p>A.11.2.3 kaapeloinnin turvallisuus</p> |                                                                                                                                                                                                                                                                     |

|     |      |                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                        |  |
|-----|------|-----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|--|
| 66. | S, H | Turvavyöhykkeillä huolehditaan siitä, ettei niillä ole <b>asiaankulumattomia</b> laitteita tai yhteyksiä. | <b>LoA Liite 2.4.5 Tilat ja henkilökunta</b><br>3. Palvelun tarjoamiseen käytetyt tilat ovat jatkuvasti seurattuja ja suojattuja ympäristötapahtumien aiheuttamilta vahingoilta, luvattomalta käytöltä ja muilta tekijöiltä, jotka voivat vaikuttaa palvelun turvallisuuteen.<br>4. Palvelun tarjoamiseen käytetyissä tiloissa varmistetaan, että pääsy alueille, joilla säilytetään tai käsitellään henkilötietoja, salattuja tietoja tai muita arkaluonteisia tietoja, rajoitetaan koskemaan valtuutettuja henkilöstön jäseniä tai alihankkijoita. | A.11. fyysinen turvallisuus ja ympäristön turvallisuus |  |
|-----|------|-----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|--|

## B 7 Riittävät ja pätevät henkilöresurssit

| KESKEISET SÄÄNNÖKSET                                                                                                                                                                                                                                                                                                                                                                                      |             |                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                               |                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>M72B 15.1 Tunnistusjärjestelmän ja tunnistusmenetelmän arvioitavat toiminnot</b></p> <p>Tunnistuspalvelun tunnistus- ja luottamuspalvelulain 29 §:n mukaisen arvioinnin täytyy kattaa kaikki laissa ja tässä määräyksessä asetetut vaatimukset, jotka kohdistuvat:</p> <p>1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän):</p> <p>c) [...] ja henkilökuntaan</p> |             |                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                               |                                                                                                                                                                                                                                                                           |
| NRO                                                                                                                                                                                                                                                                                                                                                                                                       | VARMUUSTASO | TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ                                                                                                                                                                      | SÄÄNNÖKSET                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | STANDARDI-VIITTAUS                                                                            | HUOMIOITA                                                                                                                                                                                                                                                                 |
| 67.                                                                                                                                                                                                                                                                                                                                                                                                       | S, H        | <b>Henkilökunnan riittävyys ja pätevyys</b><br><br>Tunnistuspalvelun tuotanto-organisaatiolla on käytössään riittävä asiantuntemus ja henkilöstöresurssit tietoturvallisuuden ja tietosuojaan varmistamiseksi. | <b>TunnL 13 § Tunnistuspalvelun tarjoajan yleiset velvollisuudet</b><br>Tunnistuspalvelun tarjoajan tunnistamiseen liittyvien [...] henkilökunnan ja alihankintana käyttämien palvelujen tulee täyttää sähköisen tunnistamisen varmuustasoa-asetuksen liitteen kohdissa [...] ja 2.4.5 vähintään korotetulle varmuustasolle säädetyt vaatimukset.<br><br><b>LoA Liite 2.4.5 Tilat ja henkilökunta</b><br>Vaatimukset, jotka koskevat tiloja ja henkilöstöä sekä tarvittaessa alihankkijoita, jotka suorittavat | A.7.2.2 Henkilöstöturvallisuus/työsuhteen aikana: Tietoturvatietoisuus, -opastus ja -koulutus | Arviointi<br>- henkilöresurssien riittävyys toiminnan luonteen nähtäessä (24/7/365)<br>- tekniset valvontajärjestelyt huomioidaan, ei tarkkoja vaatimuksia henkilöstömäärälle tai pätevyykselle<br>- tarpeellisten osa-alueiden osaamisesta (tekniikka, oikeudellinen mm. |

|     |      |                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                   |                                                                                                                                                                             |
|-----|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |      |                                                                                                                                                                             | tämän asetuksen soveltamisalaan kuuluvia tehtäviä. Kunkin vaatimuksen noudattaminen on suhteutettava siihen, minkä tasoinen riski tarjottavaan varmuustasoon liittyy.<br>1. Käytössä on menettelyt, joilla varmistetaan, että henkilöstöllä ja alihankkijoilla on riittävä koulutus, pätevyys ja kokemus taidoissa, joita he tarvitsevat suorittaakseen tehtävänsä.<br>2. Käytössä on riittävästi henkilöstöä ja alihankkijoita, jotta palvelua voidaan toteuttaa ja resursoida asianmukaisesti sen toimintaperiaatteiden ja menettelyjen mukaisesti. |                                                                                                                                   | henkilötietojen käsittelyn takia)                                                                                                                                           |
| 68. | S, H | Tunnistusjärjestelmään alihankitut palvelut ja toiminnot on tunnistettu ja dokumentoitu.<br><br>Alihankkijoiden henkilöstöresurssien pätevyys ja riittävyys on varmistettu. | <b>Ks. ed. rivi</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Ks. ed. rivi<br><br>A.15.1.1 Toimittajasuhteen tietoturvapoliittikka<br>A.15.2.1 toimittajien palvelujen seuranta ja katselmointi | Tiedot tunnustusjärjestelmän alihankkijoista (toimistojärjestelmät, käyttöpalvelut, ohjelmistot, infra...) ja vähintään yleisellä tasolla arvio näiden henkilöresursseista. |

## B 8 Tietoturvallisuuden hallinta

### KESKEISET SÄÄNNÖKSET

#### M72B 15.1 Tunnistusjärjestelmän ja tunnistusmenetelmän arvioitavat toiminnot

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

- 1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän):
  - a) tietoturvallisuuden hallintaan

#### M72B 4 Tunnistuspalvelun tarjoajan tietoturvallisuuden hallintajärjestelmä

##### 4.1 Tietoturvallisuuden hallinnan standardi

Tunnistuspalveluntarjoajan on noudatettava tunnustusjärjestelmän 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.

#### TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset

Sähköisen tunnistamisen järjestelmän on täytettävä seuraavat vaatimukset:

- 5) tietoturvallisuuden hallinnasta on huolehdittu siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdan 2.4 johdanto-osassa ja kohdissa 2.4.3 ja 2.4.7 vähintään korotetulle varmuustasolle säädetyt edellytykset täyttyvät.

#### LoA Liite 2.4 Hallinto ja organisointi

Kaikilla osallistujilla, jotka tarjoavat sähköiseen tunnistamiseen liittyvää rajat ylittävää palvelua (jäljempänä tässä liitteessä "palveluntarjoajat"), on oltava käytössä dokumentoidut tietoturvallisuuden hallintakäytännöt, toimintaperiaatteet, lähestymistavat riskien hallintaan ja muut hyväksytyt turva-toimenpiteet siten, että asiaankuuluvilla sähköisen tunnistamisen järjestelmien hallintoelimillä on kyseeseen tulevissa jäsenvaltioissa varmuus siitä, että tehokkaat menettelyt ovat käytössä. Kaikki 2.4 jakson vaatimukset/osatekijät on ymmärrettävä suhteutettuina riskeihin kulloisellakin tasolla.

#### LoA Liite 1. Sovellettavat määritelmät

- 4) 'tietoturvallisuuden hallintajärjestelmällä' tarkoitetaan prosesseja ja menettelyjä, joiden tarkoituksena on pitää tietoturvallisuuteen liittyvät riskit hyväksyttävällä tasolla.

#### LoA Liite 2.4.7 Noudattaminen ja tarkastus

Korotettu: Määräajoin tehdään riippumattomia sisäisiä tai ulkoisia tarkastuksia, jotka kattavat kaikki palvelujen tarjonnan kannalta merkitykselliset toimintalohkot, jotta voidaan varmistaa sovellettavien toimintaperiaatteiden noudattaminen.

| NRO | VARMUUSTASO | TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ                                                                                                                                                                                                                  | SÄÄNNÖKSET                                                                                                                                                                                                                                                                                                                                    | STANDARDI-VIITTAUS                           | HUOMIOITA                                                                                                            |
|-----|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| 69. | S, H        | Tunnistuspalvelun tarjoajalla on käytössä tehokas <b>tietoturvallisuuden hallintajärjestelmä</b> tunnistusjärjestelmän (ml. organisatoriset ja tekniset toimet) tunnistuspalvelun toiminnan tietoturvaan liittyvien riskien hallintaa ja valvontaa varten. | <b>LoA Liite 2.4.3 Tietoturvallisuuden hallinta</b><br>Käytössä on tehokas tietoturvallisuuden hallintajärjestelmä tietoturvaan liittyviä riskien hallintaa ja valvontaa varten.<br>Korotettu: Tietoturvallisuuden hallintajärjestelmässä noudatetaan vakiintuneita standardeja tietoturvaan liittyviä riskien hallintaa ja valvontaa varten. | 5 Johtajuus<br><br>A.5 tietoturva-politiikat | ISO 27001 noudattaminen ilman merkittäviä poikkeamia osoittaa tietoturvallisuuden hallinnan vaatimuksen täyttämisen. |

|     |      |                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                 |                                                                                                                                                                             |
|-----|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 70. | S, H | Tietoturvallisuuden hallintajärjestelmä perustuu yleisesti tunnettuun standardiin tai standardeihin.                                                                                                                                                                                                                    | <p><b>M72B 4 Tunnistuspalvelun tarjoajan tietoturvallisuuden hallintajärjestelmä</b></p> <p><b>4.1 Tietoturvallisuuden hallinnan standardi</b></p> <p>Tunnistuspalveluntarjoajan on noudatettava tunnustusjärjestelmän tietoturvallisuuden hallinnassa ISO/IEC 27001 -standardia tai muuta yleisesti tunnettua vastaavaa tietoturvallisuuden hallinnan standardia. Tietoturvallisuuden hallinta voi perustua myös useamman standardin yhdistelmään.</p> <p><b>LoA Liite 2.4.3 Tietoturvallisuuden hallinta</b></p> <p>Korotettu: Tietoturvallisuuden hallintajärjestelmässä noudatetaan vakiintuneita standardeja tietoturvaan liittyviä riskien hallintaa ja valvontaa varten.</p> |                                                                                                                                                                                 |                                                                                                                                                                             |
| 71. | S, H | Tietoturvallisuuden hallintajärjestelmä kattaa tunnustusjärjestelmään vaikuttavat olennaiset sisäiset ja ulkoiset tekniset, oikeudelliset ja hallinnolliset vaatimukset ja tarpeet.                                                                                                                                     | <p><b>M72B 4.2 Tietoturvallisuuden hallinnan kattavuus</b></p> <p>Tietoturvallisuuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osa-alueet:</p> <ol style="list-style-type: none"> <li>1) tunnistuspalveluntarjoajan toimintaympäristö kokonaisuutena;</li> <li>2) tietoturvallisuuden hallinnan johtaminen, organisointi ja ylläpito;</li> </ol> <p>[...]</p>                                                                                                                                                                                                                                                                                      | 4 organisaation toimintaympäristö                                                                                                                                               | Tunnistuspalvelussa tulee mm. noudattaa ajantasaisia lainsäädäntöjä ja määräyksiä, kuten tunnustus- ja luottamuspalvelulakia, määräystä M72 ja yleistä tietosuoja-asetusta. |
| 72. | S, H | <p>Tietoturvallisuuden hallintajärjestelmä kattaa hallinnan johtamisen, organisoinnin ja ylläpidon.</p> <p>Käytössä on ajantasainen ja johdon hyväksymä <b>tietoturvapoliittikka</b>. Turvallisuusperiaatteet ja politiikat ovat organisaation ja suojattavien kohteiden kannalta kattavat ja tarkoituksenmukaiset.</p> | <p><b>M72B 4.2 Tietoturvallisuuden hallinnan kattavuus</b></p> <p>Tietoturvallisuuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osa-alueet:</p> <ol style="list-style-type: none"> <li>1) [...]</li> <li>2) tietoturvallisuuden hallinnan johtaminen, organisointi ja ylläpito;</li> <li>3) [...]</li> <li>4) tietoturvallisuuden resursointi, pätevyys, henkilöstön tietoisuus tietoturvalisuu-desta, viestintä ja dokumentointi sekä dokumentoidun tiedon hallinta;</li> </ol> <p>[...]</p>                                                                                                                                                       | 5 johtajuus<br>9.2 sisäinen auditointi<br>9.3 johdon katselmus<br>10 hallintajärjestelmän parantaminen<br>A.5.1.1 Tietoturvapoliittikat<br>A.6.1.1 Tietoturvaroolit ja -vastuut |                                                                                                                                                                             |

|     |      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                           |                                                   |  |
|-----|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|--|
|     |      | Henkilökunnan ja alihankkijoiden tietoturvaluuteen liittyvät vastuut on kuvattu.                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                           | A.15.1.1 toimittajasuhteiden tietoturvapolitiikka |  |
| 73. | S, H | <p>Tietoturvaluuden hallintajärjestelmä kattaa tunnistuspalvelun tarjontaan liittyvien tietoturvallisuusriskien hallinnan.</p> <p>Riskienhallinta on säännöllinen ja jatkuva, dokumentoitu prosessi.</p> <p>Tunnistetut riskit luokitellaan ja priorisoidaan.</p> <p>Riskienhallintaprosessi tunnistaa tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen kohdistuvat riskit.</p> <p>Riskienhallintaprosessia ja sen tuloksia hyödynnetään tunnistuspalvelun/tunnistusjärjestelmän turvatoimien suunnittelussa.</p> | <p><b>M72B 4.2 Tietoturvaluuden hallinnan kattavuus</b></p> <p>Tietoturvaluuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osat:</p> <p>[...]</p> <p>3) tunnistuspalvelun tarjontaan liittyvien tietoturvallisuusriskien hallinta;</p> <p>[...]</p>                                                                        | 6 Suunnittelu<br>8 Toiminta                       |  |
| 74. | S, H | <p>Tietoturvaluuden hallintajärjestelmä kattaa tietoturvaluuden resursoinnin, pätevyysvaatimukset, henkilöstön tietoisuuden tietoturvaluudesta, viestinnän ja dokumentoinnin sekä dokumentoidun tiedon hallinnan.</p> <p>Ajantasaiset tietoturvaohjeet ja käytännöt ovat kaikkien sähköisen tunnistamisen tehtäviin osallistuvien saatavilla ja tiedossa.</p>                                                                                                                                                           | <p><b>M72B 4.2 Tietoturvaluuden hallinnan kattavuus</b></p> <p>Tietoturvaluuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osat:</p> <p>[...]</p> <p>4) tietoturvaluuden resursointi, pätevyys, henkilöstön tietoisuus tietoturvaluudesta, viestintä ja dokumentointi sekä dokumentoidun tiedon hallinta;</p> <p>[...]</p> | 7 Tukitoiminnot                                   |  |

|     |      |                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                 |                                                                                                                                                                     |
|-----|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |      | Henkilöstön turvallisuuskoulutus on säännöllistä ja dokumentoitua. Koulutuksen tehokkuutta seurataan.                                                                                        |                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                 |                                                                                                                                                                     |
| 75. | S, H | Tietoturvallisuuden hallintajärjestelmässä huolehditaan tunnistuspalvelun tarjonnan suunnittelusta ja ohjauksesta siten, että tunnistuspalvelulle säädetyt tietoturva-vaatimukset täyttyvät. | <b>M72B 4.2 Tietoturvallisuuden hallinnan kattavuus</b><br>Tietoturvallisuuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osa-alueet:<br>[...]<br>5) tunnistuspalvelun tarjonnan suunnittelu ja ohjaus tietoturva-vaatimusten täyttämiseksi; ja<br>[...] | 8 Toiminta<br><br>A.18.1.1 vaatimustenmukaisuus/lainsäädäntöön ja sopimukseen sisältyvien vaatimusten noudattaminen: sovellettavien lakisääteisten ja sopimuksellisten vaatimusten yksilöiminen | Tunnistuspalvelulle säädetyt vaatimukset<br><br>Soveltuvien osien tietosuojasääntely<br><br>Soveltuvien osien luottamusverkoston sopimussääntely                    |
| 76. | S, H | Tietoturvallisuuden hallintajärjestelmä kattaa tietoturvallisuuden hallinnan tehokkuuden ja toimivuuden säännöllisen arvioinnin.                                                             | <b>M72B 4.2 Tietoturvallisuuden hallinnan kattavuus</b><br>Tietoturvallisuuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osa-alueet:<br>[...]<br>6) tietoturvallisuuden hallinnan tehokkuuden ja toimivuuden arviointi.                                 | 9.1 seuranta, mittaaminen, analysointi, arviointi                                                                                                                                               | Miten hyvin tietoturvallisuuden hallinta tehoa/vaikuttaa niihin tekijöihin, prosesseihin ja ongelmiin, jotka vaikuttavat tunnistusjärjestelmän tietoturvallisuuteen |

## B 9 Tunnistusvälineen hakijan henkilöllisyyden todistaminen ja varmentaminen (ensitunnistaminen)

### KESKEISET SÄÄNNÖKSET

#### M72B 15.1 Tunnistusjärjestelmän ja tunnistusmenetelmän arvioitavat toiminnot

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

- 2) tunnistusmenetelmään eli tunnistusvälineen
- b) hakijan henkilöllisyyden todistamiseen ja varmentamiseen

### **TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset**

Sähköisen tunnistamisen järjestelmän on täytettävä seuraavat vaatimukset:

- 1) tunnistusmenetelmän perustana on 17 ja 17 a §:n mukainen tunnistaminen, jota koskevat tiedot ovat jälkikäteen 24 §:n mukaisesti tarkastettavissa;
- 2) tunnistusmenetelmällä voidaan yksiselitteisesti tunnistaa tunnistusvälineen haltija siten, että teknisten vähimmäiseritelmien ja -menettelyjen vahvistamisesta sähköisen tunnistamisen menetelmien varmuustasoa varten sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 8 artiklan 3 kohdan mukaisesti annetussa komission täytäntöönpanoasetuksen (EU) 2015/1502, jäljempänä sähköisen tunnistamisen varmuustasoasetus, liitteen kohdissa 2.1.2, 2.1.3 ja 2.1.4 vähintään korotetulle varmuustasolle säädetyt edellytykset täyttyvät;

[...]

### **TunnL 17 § Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen**

Ensimmäisessä luonnollisen henkilön tunnistaminen tulee tehdä henkilökohtaisesti tai sähköisesti siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.1.2 korotetulle tai korkealle varmuustasolle säädetyt vaatimukset täyttyvät. Henkilön henkilöllisyyden varmentaminen voi perustua viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan tai tässä laissa tarkoitettuun vahvaan sähköiseen tunnistusvälineeseen. Lisäksi henkilöllisyyden varmentaminen voi perustua julkisen tai yksityisen tahon aiemmin muuhun tarkoitukseen kuin vahvan sähköisen tunnistusvälineen myöntämiseen käyttämään menettelyyn, jonka Liikenne- ja viestintävirasto hyväksyy menettelyä koskevien säännösten ja viranomaisvalvonnan perusteella tai 28 §:n 1 kohdassa tarkoitettua vaatimustenmukaisuuden arviointilaitoksen vahvistuksen perusteella.

Ensimmäisessä, joka perustuu yksinomaan viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan, hyväksyttäviä asiakirjoja ovat voimassa oleva Euroopan talousalueen jäsenvaltion, Sveitsin tai San Marinon viranomaisen myöntämä passi tai henkilökortti. Halutessaan tunnistusvälineen tarjoaja voi käyttää henkilöllisyyden varmentamisessa myös muun valtion viranomaisen myöntämää voimassa olevaa passia.

Jos tunnistusvälineen hakijan henkilöllisyyttä ei voida luotettavasti todentaa, hakemukseen liittyvän ensimmäisen tunnistamisen tekee poliisi. [...]

#### **LoA Liite 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)**

#### **LoA Liite 2.1.3 Henkilöllisyyden todistaminen ja varmentaminen (oikeushenkilö)**

#### **LoA Liite 2.1.4 Luonnollisten ja oikeushenkilöiden sähköisen tunnistamisen menetelmien välinen kytkös**

### **OIKEUSHENKILÖ**

*Oikeushenkilön tunnistusvälineen myöntämistä koskevia vaatimuksia ei käsitellä tarkemmin tässä kriteeristössä. Jos tunnistuspalvelun tarjoaja ryhtyy tarjoamaan vahvoja tunnistusvälineitä oikeushenkilöille, arvioinnissa on huomioitava tätä koskevat säännökset.*

### **TunnL 17 a § Tunnistusvälineen hakijana olevan oikeushenkilön tunnistaminen**

Oikeushenkilön ilmoitettu henkilöllisyys tulee varmentaa yritys- ja yhteisörekistereistä tai siten, että vähintään oikeushenkilön henkilöllisyyden todistamista ja varmentamista koskevat sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.1.3 korotetulle varmuustasolle säädetyt vaatimukset täyttyvät.

### **TunnL 7 a § yritys- ja yhteisörekisterien tietojen käyttäminen**

Tunnistusvälineen tarjoajan ja luottamuspalvelua tarjoavan varmentajan on hankittava ja päivitettävä oikeushenkilön tunnistuspalvelun tarjoamiseksi tarvitsemansa tiedot yritys- ja yhteisörekistereistä. Tämän lisäksi tunnistuspalvelun tarjoajan on varmistettava, että sen tunnistuspalvelun tarjoamiseksi tarvitsemat tiedot ovat ajan tasalla yritys- ja yhteisörekisterien tietojen kanssa.

## MÄÄRITELMÄT

### TunnL 2 § Määritelmät

7) ensitunnistamisella tunnistusvälineen hakijan henkilöllisyyden todentamista välineen hankkimisen yhteydessä;

### LoA Liite 1. Sovellettavat määritelmät

1) 'luotettavalla lähteellä' tarkoitetaan mitä tahansa sellaista lähdetä muodosta riippumatta, josta voidaan luotettavasti saada paikkansapitäviä tietoja ja/tai todisteita, joita voidaan käyttää henkilöllisyyden todistamiseen;

**Standardi: ETSI TS 119 461**

| NRO                                                                                                | VARMUUSTASO | TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ                                                                                                                                                                                         | SÄÄNNÖKSET                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | STANDARDI-VIITTAUS | HUOMIOITA                                                                |
|----------------------------------------------------------------------------------------------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|--------------------------------------------------------------------------|
| <b>Tapa 1: Ensitunnistus perustuu Suomessa hyväksytyn henkilöllisyydestodistuksen esittämiseen</b> |             |                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                    |                                                                          |
| 77.                                                                                                | S, H        | Henkilöllisyyden todistaminen perustuu tunnustuslaissa hyväksyttyihin henkilöllisyydestodistuksiin.<br><br>Muiden kuin laissa lueteltujen valtioiden myöntämien henkilöllisyydestodistuksen hyväksyminen on selkeästi määritelty. | <b>TunnL 17 § Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen</b><br>[...]<br>Ensitunnistamisessa, joka perustuu yksinomaan viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan, hyväksyttäviä asiakirjoja ovat voimassa oleva Euroopan talousalueen jäsenvaltion, Sveitsin tai San Marinon viranomaisen myöntämä passi tai henkilökortti. Halutessaan tunnistusvälineen tarjoaja voi käyttää henkilöllisyyden varmentamisessa myös muun valtion viranomaisen myöntämää voimassa olevaa passia.<br>[...] |                    | Jos käytössä on henkilöllisyydestodistuksiin perustuva ensitunnistaminen |
| 78.                                                                                                | S, H        | Henkilöllisyydestodistus esitetään ja sen aitous tarkistetaan <b>paikan päällä</b> .<br><br>Henkilöstö tuntee henkilöllisyydestodistusten aitoustehtävät ja pystyy tarkistamaan ne.                                               | <b>TunnL 17 § Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen</b><br>Ensitunnistamisessa luonnollisen henkilön tunnistaminen tulee tehdä <u>henkilökohtaisesti tai sähköisesti</u> siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.1.2 korotetulle tai korkealle varmuustasolle säädetyt vaatimukset                                                                                                                                                                                     |                    | Jos käytössä on etätunnistusratkaisu, kts. Kriteerit kohdassa "Tapa 5".  |

|     |   |                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |  |                            |
|-----|---|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|----------------------------|
|     |   | Varmistetaan, että henkilöllisyystodistus on sen esittävän henkilön oma.           | <p>täyttyvät. Henkilön henkilöllisyyden varmentaminen voi perustua <u>viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan</u> tai tässä laissa tarkoitettuun vahvaan sähköiseen tunnistusvälineeseen. [...]</p> <p><b>LoA Liite 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)</b><br/>Korotettu:<br/>1. Henkilöllä on <u>varmennettu olevan hallussaan sen jäsenvaltion hyväksymä todiste ilmoitetusta henkilöllisyydestä</u>, jossa sähköisen tunnistamisen menetelmää haetaan<br/>ja<br/><u>todiste on tarkastettu sen varmistamiseksi, että se on aito</u>; tai luotettavasta lähteestä tiedetään sen olevan olemassa ja liittyvän todelliseen henkilöön<br/>ja<br/>on ryhdytty toimiin sen riskin minimoimiseksi, että henkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, että todiste on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt;</p> <p>tai</p> <p>2. <u>henkilöllisyystodistus esitetään rekisteröintiprosessin aikana</u> siinä jäsenvaltiossa, jossa todistus on myönnetty, ja todistus näyttää liittyvän sen esittäneeseen henkilöön<br/>ja<br/>on ryhdytty toimiin sen riskin minimoimiseksi, että henkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, että todistus on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt;</p> |  |                            |
| 79. | S | Henkilöllisyystodistus esitetään ja sen aitous tarkistetaan <b>etäyhteydellä</b> . | <b>TunnL 17 § Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |  | Ks. tämän ohjeen kohta 3.9 |

|  |                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |  |  |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
|  | <p>Henkilöstö tuntee henkilöllisyystodistusten aitoustekijät ja pystyy tarkistamaan ne.</p> <p>Varmistetaan, että henkilöllisyystodistus on sen esittävän henkilön oma.</p> <p>Etäyhteyden luotettavuusvaatimuksissa huomioidaan korotetun tason hyökkäyspotentiaali.</p> | <p>Ensitunnistamisessa luonnollisen henkilön tunnistaminen tulee tehdä henkilökohtaisesti tai <u>sähköisesti</u> siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.1.2 korotetulle tai korkealle varmuustasolle säädetyt vaatimukset täyttyvät. Henkilön henkilöllisyyden varmentaminen voi perustua <u>viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan</u> tai tässä laissa tarkoitettuun vahvaan sähköiseen tunnistusvälineeseen. [...]</p> <p><b>LoA Liite 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)</b><br/>Korotettu:</p> <p>1. Henkilöllä on <u>varmennettu olevan hallussaan sen jäsenvaltion hyväksymä todiste ilmoitetusta henkilöllisyydestä</u>, jossa sähköisen tunnistamisen menetelmää haetaan<br/>ja<br/><u>todiste on tarkastettu sen varmistamiseksi, että se on aito</u>; tai luotettavasta lähteestä tiedetään sen olevan olemassa ja liittyvän todelliseen henkilöön<br/>ja<br/>on ryhdytty toimiin sen riskin minimoimiseksi, että henkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, että todiste on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt;</p> <p>tai</p> <p>2. <u>henkilöllisyystodistus esitetään rekisteröintiprosessin aikana</u> siinä jäsenvaltiossa, jossa todistus on myönnetty, ja todistus näyttää liittyvän sen esittäneeseen henkilöön<br/>ja<br/>on ryhdytty toimiin sen riskin minimoimiseksi, että henkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, että todistus on kadonnut tai</p> |  |  |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|

|     |      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |  |                                                                                                                                                             |
|-----|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |  |                                                                                                                                                             |
| 80. | H    | <p>Henkilöllisyystodistus esitetään ja sen aitous tarkistetaan etäyhteydellä.</p> <p>Henkilöllisyystodistuksen aitous tarkistetaan sen myöntäjän sähköisen allekirjoituksen perusteella henkilöllisyystodistuksen sirulta.</p> <p>Varmistetaan, että henkilöllisyystodistus on sen esittävän henkilön oma vertaamalla esittäneen henkilön ominaisuuksia henkilöllisyystodistuksesta saatuun sähköisesti allekirjoitettuun vertailutietoon.</p> <p>Etäyhteyden luotettavuusvaatimuksissa huomioidaan korkean tason hyökkäyspotentiaali.</p> | <p><b>LoA Liite 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)</b></p> <p>Korkea:</p> <p>1.a) Jos henkilöllä on varmennettu olevan hallussaan <u>sen jäsenvaltion hyväksymä valokuva tai biometrinen tunniste, jossa sähköisen tunnistamisen menetelmää haetaan</u>, ja kyseinen todiste edustaa ilmoitettua henkilöllisyyttä, todiste tarkistetaan sen määrittämiseksi, onko se luotettavan lähteen mukaan voimassa;</p> <p>ja</p> <p>hakijalla todetaan olevan ilmoitettu henkilöllisyys vertaamalla yhtä tai useampaa henkilön fyysistä ominaisuutta luotettavaan lähteeseen;</p>                                                                                                             |  | Ks. tämän ohjeen kohta 3.9                                                                                                                                  |
| 81. | S, H | Tieto passin tai henkilökortin voimassaolosta tarkistetaan käytävissä olevista poliisin tietojärjestelmästä tai kansainvälisistä luotettavista lähteistä.                                                                                                                                                                                                                                                                                                                                                                                  | <p><b>LoA Liite 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)</b></p> <p><i>Menettelyt 1 ja 2, osavaatimus:</i></p> <p>on ryhdytty toimiin sen riskin minimoimiseksi, että henkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, <u>että todiste on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt;</u></p> <p><b>TunnL 7 b § Tieto passin tai henkilökortin voimassaolosta</b></p> <p>Tunnistuspalvelun tarjoajalla on oikeus saada salassapitosäännösten estämättä rajapinnan kautta tai muutoin sähköisesti poliisin tietojärjestelmässä oleva tieto ensitunnistamisessa käytettävän passin tai henkilökortin voimassaolosta.</p> |  | <p>Ei pakolliseksi säädetty vaatimus, mutta vaikuttaa riskiarviointiin ja voi vaikuttaa korvausvastuuseen.</p> <p>Korkealla varmuustasolla välttämätön.</p> |

|                                                              |      |                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |  |                                                                                                                                                                                                                            |
|--------------------------------------------------------------|------|------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 82.                                                          | S, H | Henkilön olemassaolo tarkistetaan väestötietojärjestelmästä                                                      | <p><b>TunnL 7 § Väestötietojärjestelmän tietojen käyttäminen</b></p> <p>Tunnistusvälineen tarjoajan ja luottamuspalvelua tarjoavan varmentajan on hankittava ja päivitettävä luonnollisen henkilön tunnistuspalvelun tarjoamiseksi tarvitsemansa tiedot väestötietojärjestelmästä. Tämän lisäksi tunnistuspalvelun tarjoajan on varmistettava, että sen tunnistuspalvelun tarjoamiseksi tarvitsemat tiedot ovat ajan tasalla väestötietojärjestelmän tietojen kanssa. [...]</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |  | Koskee kaikkia ensitunnistusmenettelyjä.                                                                                                                                                                                   |
| <b>Tapa 2: Ensitunnistus sähköisellä tunnistusvälineellä</b> |      |                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |  |                                                                                                                                                                                                                            |
| 83.                                                          | S    | Henkilöllisyyden todistaminen perustuu tunnistuslaissa hyväksyttyihin vahvoihin sähköisiin tunnistusvälineisiin. | <p><b>TunnL 17 § Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen</b></p> <p>Ensitunnistamisessa luonnollisen henkilön tunnistaminen tulee tehdä henkilökohtaisesti <u>tai sähköisesti</u> siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.1.2 korotetulle tai korkealle varmuustasolle säädetyt vaatimukset täyttyvät. Henkilön henkilöllisyyden varmentaminen voi perustua viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan <u>tai tässä laissa tarkoitettuun vahvaan sähköiseen tunnistusvälineeseen</u>. [...]</p> <p><b>LoA Liite 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)</b></p> <p>Korotettu:</p> <p>4. Jos sähköisen tunnistamisen menetelmiä myönnetään sellaisen <u>voimassa olevan ilmoitetun sähköisen tunnistamisen menetelmän perusteella</u>, jonka varmuustaso on ”korotettu” tai ”korkea”, ja ottaen huomioon riskit henkilön tunnistetiedoissa tapahtuvista muutoksista, henkilöllisyyden todistamis- ja varmentamismenettelyjä ei tarvitse toistaa. Jos perustana olevaa sähköisen tunnistamisen menetelmää ei ole ilmoitettu, varmuustason ”korotettu” tai ”korkea” on oltava asetuksen (EY) N:o 765/2008 2 artiklan 13 kohdassa tarkoitettun</p> |  | <p>Jos käytössä on vahvaan sähköiseen tunnistamiseen perustuva ensitunnistaminen.</p> <p>Tunnistuslain mukaisesti hyväksytyt korotetun varmuustason tunnistusvälineet ovat Liikenne- ja viestintäviraston rekistressä.</p> |

|                                                                                                             |      |                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                             |      |                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <u>vaatimustenmukaisuuden arviointilaitoksen</u> tai vastaavan elimen vahvistama.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |  |                                                                                                                                                                                                                                                                                                                                                                                   |
| 84.                                                                                                         | H    | <p>Henkilöllisyyden todistaminen perustuu tunnustuslaissa hyväksyttyihin vahvoihin sähköisiin tunnustusvälineisiin.</p> <p>Korkean varmuustason tunnustusvälineen myöntäminen sähköisen tunnituksen perusteella on mahdollista vain korkean varmuustason välineellä.</p>                                                                                                                                                                                    | <p><b>LoA Liite 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)</b></p> <p>Korkea:</p> <p>3. Jos sähköisen tunnistamisen menetelmiä myönnetään sellaisen voimassa olevan ilmoitetun sähköisen tunnistamisen menetelmän perusteella, jonka varmuustaso on "korkea", henkilöllisyyden todistamis- ja varmentamismenettelyjä ei tarvitse toistaa. Jos perustana olevaa sähköisen tunnistamisen menetelmää ei ole ilmoitettu, varmuustason "korkea" on oltava asetuksen (EY) N:o 765/2008 2 artiklan 13 kohdassa tarkoitetun vaatimustenmukaisuuden arviointilaitoksen tai vastaavan elimen vahvistama</p> <p>ja</p> <p>on ryhdytty toimiin sen osoittamiseksi, että sen menettelyn tulokset, jossa ilmoitettu sähköisen tunnistamisen menetelmä aiemmin myönnettiin, ovat edelleen voimassa.</p> |  | <p>Jos käytössä on vahvaan sähköiseen tunnistamiseen perustuva ensitunnistaminen.</p> <p>Tunnustuslain mukaisesti hyväksytyt korkean varmuustason tunnustusvälineet ovat Liikenne- ja viestintäviraston rekistressä.</p>                                                                                                                                                          |
| <b>Tapa 3: Ensitunnistus muuhun tarkoitukseen tehdyn tunnistamisen perusteella ("aikaisempi asiakkuus")</b> |      |                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |                                                                                                                                                                                                                                                                                                                                                                                   |
| 85.                                                                                                         | S, H | <p>Henkilöllisyyden varmentamisessa luotetaan menettelyyn, jolla henkilöllisyys on todistettu ja varmennettu aikaisemmin muuta kuin vahvan sähköisen tunnustusvälineen myöntämistä varten.</p> <p>Menettely voi perustua muuhunkin sääntelyyn kuin tunnustuslakiin tai eIDAS-asetukseen ja sitä valvoo viranomainen.</p> <p>Menettely tarjoaa vastaavan varmuuden kuin tunnustussääntelyn mukainen henkilöllisyystodistuksen esittämiseen perustuva tai</p> | <p><b>TunnL 17 § Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen</b></p> <p>Ensitunnistamisessa luonnollisen henkilön tunnistaminen tulee tehdä henkilökohtaisesti tai sähköisesti siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.1.2 korotetulle tai korkealle varmuustasolle säädetyt vaatimukset täyttyvät. Henkilön henkilöllisyyden varmentaminen voi perustua viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan tai tässä laissa tarkoitettuun vahvaan sähköiseen tunnustusvälineeseen. <u>Lisäksi henkilöllisyyden varmentaminen voi perustua julkisen tai yksityisen tahon aiemmin muuhun tarkoitukseen kuin vahvan sähköisen tunnustusvälineen myöntämiseen käyttämään menettelyyn, jonka Liikenne- ja viestintävirasto hyväksyy</u></p>      |  | <p>Tämän kohdan mukaisen ensitunnistusmenettelyn käyttö edellyttää Liikenne- ja viestintäviraston nimenomaista vahvistusta. Menettelyä koskevaan ilmoitukseen täytyy liittää arviointi vaatimustenmukaisuudesta.</p> <p>Kyseeseen voi tulla esimerkiksi hyväksytyyn sähköisen allekirjoituksen tai kehittyneen sähköisen allekirjoituksen, johon liittyy hyväksytty varmenne,</p> |

|                                              |      |                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |  |                                                                                                                                                                                                                                   |
|----------------------------------------------|------|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                              |      | sähköisellä tunnistusmenetelmällä tunnistamiseen perustuva menettely. | <p><u>menettelyä koskevien säännösten ja viranomaisvalvonnan perusteella tai 28 §:n 1 kohdassa tarkoitetun vaatimustenmukaisuuden arviointilaitoksen vahvistuksen perusteella.</u></p> <p>[...]</p> <p><b>LoA Liite 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)</b></p> <p>Korotettu:</p> <p>3. Jos julkisen tai yksityisen tahon samassa jäsenvaltiossa aiemmin <u>muuhun tarkoitukseen</u> kuin sähköisen tunnistamisen menetelmien myöntämiseen käyttämät <u>menettelyt</u> tarjoavat vastaavan varmuuden kuin 2.1.2. kohdassa esitetty menettelyt varmuustasolla ”korotettu”, rekisteröinnistä vastaavan tahon ei tarvitse toistaa kyseisiä aiempia menettelyjä edellyttäen, että tällaisen vastaavan tasoisen varmuuden on vahvistanut Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 765/2008 (1) 2 artiklan 13 kohdassa tarkoitettu vaatimustenmukaisuuden arviointilaitos tai vastaava elin;</p> |  | joka on myönnetty sähköistä allekirjoitusta varten, käyttö osana ensitunnistusprosessia. Uutta tunnistusvälinettä luovutuksessa on tällöin varmistettava muin keinoin, että uusi tunnistusväline luovutetaan oikealle henkilölle. |
| <b>Tapa 4: Poliisin tekemä ensitunnistus</b> |      |                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |  |                                                                                                                                                                                                                                   |
| 86.                                          | S, H | Ensitunnistamisen tekee tarvittaessa poliisi.                         | <p><b>TunnL 17 § Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen</b></p> <p>[...]</p> <p>Jos tunnistusvälineen hakijan henkilöllisyyttä ei voida luotettavasti todentaa, hakemukseen liittyvän ensitunnistamisen tekee poliisi.</p> <p>[...]</p> <p><b>LoA Liite 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)</b></p> <p>Korkea</p> <p>2. Jos hakija ei esitä valokuvaa tai biometristä tunnistetta, sovelletaan samoja menettelyjä, joita tällaisen hyväksytyn valokuvan tai biometrisen todisteen saamiseksi käytetään kansallisella tasolla rekisteröinnistä vastaavan tahon jäsenvaltiossa.</p>                                                                                                                                                                                                                                                                                       |  |                                                                                                                                                                                                                                   |

**Tapa 5: Etäensitunnistus**

|     |   |                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                          |                                                                                                                                                                                                                                                                                                                                                                                  |
|-----|---|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 87. | S | Etäensitunnistuksen ratkaisu tulee perustua riskiarvioon (Level of Identity Proofing, LoIP) | <p><b>TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset</b><br/>[...]</p> <p>4) tunnistusjärjestelmä on turvallinen ja luotettava siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdissa 2.2.1, 2.3.1 ja 2.4.6 vähintään korotetulle varmuustasolle säädetty edellytykset täyttyvät ottaen huomioon kulloinkin käytettävissä olevaan tekniikkaan liittyvät tietoturvallisuusuhat sekä tunnistuspalvelun tarjoamiseen käytettävät tilat ovat turvallisia sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.4.5 säädetyllä tavalla;</p> <p>5) tietoturvallisuuden hallinnasta on huolehdittu siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdan 2.4 johdanto-osassa ja kohdissa 2.4.3 ja 2.4.7 vähintään korotetulle varmuustasolle säädetty edellytykset täyttyvät.<br/>[...]</p> <p><b>M72B 6.1 Tunnistusmenetelmän ominaispiirteet ja suojautumiskyky</b><br/>6.1.1<br/>Tunnistusmenetelmän todentamistekijät, todentamismekanismi ja turvatoimenpiteet on suunniteltava, toteutettava ja ylläpidettävä siten, että ne suojaavat tunnustusmenetelmän eheyden ja luottamuksellisuuden. Tunnistusmenetelmällä on oltava suojautumiskyky vähintään tunnistuspalvelun varmuustason mukaista <i>sähköisen tunnistamisen varmuustasoasetuksen</i> liitteen kohdassa 2.3 tarkoitettua kohtuullisen tai korkean vakavuustason uhkaa ja hyökkäyspotentiaalia vastaan.<br/>Suojautumiskyvyn on perustuttava <u>riskiarvioon</u>, jossa arvioidaan erikseen hallussapitoon, tietoon ja ominaisuuteen perustuviin todentamistekijöihin ja todentamismekanismiin kohdistuvat uhkat sekä uhkilta suojaavat turvatoimenpiteet.</p> | ETSI TS 119 461<br>ISO/IEC TS 29003:2018 | Hyökkäyspotentiaali (korotettu/korkea) ja sen selvittäminen, määritellyt kriteerit mitkä tulee täyttyä, jotta myöntöprosessi voidaan viedä loppuun, toimitusketjun turvallisuus, jos käytetään palveluntarjoajaa, perustuuko kuvalliseen (selfie) vai videomateriaalin tarkasteluun, kriteerit, joiden täytyessä siirrytään automaattisesta prosessista manuaaliseen prosessiin. |
|-----|---|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|     |   |                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |  |  |
|-----|---|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
|     |   |                                                    | <p><b>LoA liite 2.4.3 Tietoturvallisuuden hallinta</b><br/>Matala:<br/>Käytössä on tehokas tietoturvallisuuden hallintajärjestelmä tietoturvaan liittyviä riskien hallintaa ja valvontaa varten.<br/>Korotettu:<br/>Tietoturvallisuuden hallintajärjestelmässä noudatetaan vakiintuneita standardeja tietoturvaan liittyviä riskien hallintaa ja valvontaa varten.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |  |  |
| 88. | S | Asiakkaan tiedottaminen ehdoista ja edellytyksistä | <p><b>TunnL 20 § Tunnistusvälineen myöntäminen</b><br/>Tunnistusvälineen liikkeelle laskeminen perustuu tunnistusvälineen hakijan ja tunnistuspalvelun tarjoajan väliseen sopimukseen. Sopimus on tehtävä kirjallisesti. Sopimus voidaan tehdä myös sähköisesti, jos sen sisältöä ei voida yksipuolisesti muuttaa ja se säilyy osapuolten saatavilla. Tunnistuspalvelun tarjoajan tulee kohdella asiakkaitaan syrjimättä ja tunnistusvälineiden hakijoita tasapuolisesti sopimuksen tekemisen yhteydessä.<br/>[...]</p> <p><b>TunnL 23 § Tunnistusvälineen haltijan velvollisuudet</b><br/>Tunnistusvälineen haltijan on käytettävä tunnistusvälinettä sopimuksen ehtojen mukaisesti. Haltijan on säilytettävä tunnistusvälinettä huolellisesti. Haltijan velvollisuus huolehtia tunnistusvälineestä alkaa, kun hän on vastaanottanut sen. Tunnistusvälineen haltija ei saa luovuttaa välinettä toisen käyttöön.</p> <p><b>LoA 2.1.1. Hakemus ja rekisteröinti</b><br/>1.Varmistetaan, että hakija on tietoinen sähköisen tunnistamisen menetelmien käyttöön liittyvistä ehdoista ja edellytyksistä.<br/>2.Varmistetaan, että hakija on tietoinen sähköisen tunnistamisen menetelmiin liittyvistä suositelluista varotoimista.<br/>[...]</p> |  |  |

|     |   |                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                 |
|-----|---|----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 89. | S | Hyväksytyt ensitunnistusasiakirjat ja niiden voimassaolon tarkistus. | <p><b>TunnL 17 § Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen</b><br/>[...]<br/>Ensitunnistamisessa, joka perustuu yksinomaan viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan, hyväksyttäviä asiakirjoja ovat voimassa oleva Euroopan talousalueen jäsenvaltion, Sveitsin tai San Marinon viranomaisen myöntämä passi tai henkilökortti. Halutessaan tunnistusvälineen tarjoaja voi käyttää henkilöllisyyden varmentamisessa myös muun valtion viranomaisen myöntämää voimassa olevaa passia.<br/>[...]</p> <p><b>TunnL 7 b § Tieto passin tai henkilökortin voimassaolosta</b><br/>Tunnistuspalvelun tarjoajalla on oikeus saada sassaapitosäännösten estämättä rajapinnan kautta tai muutoin sähköisesti poliisin tietojärjestelmässä oleva tieto ensitunnistamisessa käytettävän passin tai henkilökortin voimassaolosta.</p> <p><b>LoA 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)</b><br/>Matala:<br/>1. Henkilöllä voidaan olettaa olevan hallussaan sen jäsenvaltion hyväksymä todiste ilmoitetusta henkilöllisyydestä, jossa sähköisen tunnistamisen menettelmää haetaan.<br/>2. Todisteen voidaan olettaa olevan aito tai luotettavan lähteen mukaan olemassa oleva, ja se näyttää olevan voimassa.<br/>3. Luotettavan lähteen tiedossa on, että ilmoitettu henkilöllisyys on olemassa, ja voidaan olettaa, että henkilöllisyyden ilmoittaneella henkilöllä on tämä sama henkilöllisyys.</p> <p>Korotettu:<br/>Lisäksi vähintään 1 kpl kohdasta korotettu, esim.</p> | Tällä hetkellä käytännössä passi, mahdollisesti myös henkilökortti. Ensitunnistusasiakirjan voimassaolo on tarkistettava poliisin rajapintaa tai muuta kansainvälisesti luotettua rajapintaa vasten (Interpol). |
|-----|---|----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|     |   |                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                     |                                                                                                                                                         |
|-----|---|------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |   |                                                                                                                              | <p>1. Henkilöllä on varmennettu olevan hallussaan sen jäsenvaltion hyväksymä todiste ilmoitetusta henkilöllisyydestä, jossa sähköisen tunnistamisen menettelmää haetaan</p> <p>ja</p> <p>todiste on tarkastettu sen varmistamiseksi, että se on aito; tai luotettavasta lähteestä tiedetään sen olevan olemassa ja liittyvän todelliseen henkilöön</p> <p>ja</p> <p>on ryhdytty toimiin sen riskin minimoimiseksi, että henkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, että todiste on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt;</p>                                                                                                                                                                                |                                                     |                                                                                                                                                         |
| 90. | S | Henkilön olemassaolo tarkistetaan väestötietojärjestelmästä.                                                                 | <p><b>TunnL 7 § Väestötietojärjestelmän tietojen käyttäminen</b></p> <p>Tunnistusvälineen tarjoajan ja luottamuspalvelua tarjoavan varmentajan on hankittava ja päivitettävä luonnollisen henkilön tunnistuspalvelun tarjoamiseksi tarvitsemansa tiedot väestötietojärjestelmästä. Tämän lisäksi tunnistuspalvelun tarjoajan on varmistettava, että sen tunnistuspalvelun tarjoamiseksi tarvitsemat tiedot ovat ajan tasalla väestötietojärjestelmän tietojen kanssa.</p> <p>[...]</p> <p><b>LoA 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)</b></p> <p>Matala:</p> <p>3. Luotettavan lähteen tiedossa on, että ilmoitettu henkilöllisyys on olemassa, ja voidaan olettaa, että henkilöllisyyden ilmoittaneella henkilöllä on tämä sama henkilöllisyys.</p> |                                                     | Koskee kaikkia ensitunnistusmenettelyjä.                                                                                                                |
| 91. | S | Etäensitunnistusta tekevä sovelus ja ulkopuoliset ratkaisut tai komponentit tulee arvioida tai niiden pitää olla arvioituja. | <p><b>TunnL 29 § Sähköisen tunnistuspalvelun vaatimustenmukaisuuden arviointi</b></p> <p>Tunnistuspalvelun tarjoajan on määräajoin teetettävä palvelulle 28 §:ssä mainitun arviointielimen arviointi siitä, täyttääkö tunnistuspalvelu tässä</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <p>ETSI TS 119 461</p> <p>ISO/IEC TS 29003:2018</p> | Arviointilaitoksen tekemä arviointi, FAR-arvo, mihin testidataan FAR perustuu, vastaavuus hyökkäyspotentiaaliin (korotettu/korkea). PAD-kyvykkyys (Pre- |

|  |  |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                      |                                                                                                                                                                               |
|--|--|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  |  | <p>laissa säädetyt yhteentoimivuutta, tietoturvaa, tietosuojaa ja muuta luotettavuutta koskevat vaatimukset.<br/>[...]</p> <p><b>M72B 4.2 Tietoturvallisuuden hallinnan kattavuus</b><br/>Tietoturvallisuuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osat alueet:</p> <ol style="list-style-type: none"> <li>1) tunnistuspalveluntarjoajan toimintaympäristö kokonaisuutena;</li> <li>2) tietoturvallisuuden hallinnan johtaminen, organisointi ja ylläpito;</li> <li>3) tunnistuspalvelun tarjontaan liittyvien tietoturvallisuusriskien hallinta;</li> <li>4) tietoturvallisuuden resursointi, pätevyys, henkilöstön tietoisuus tietoturvallisuudesta, viestintä ja dokumentointi sekä dokumentoidun tiedon hallinta;</li> <li>5) tunnistuspalvelun tarjonnan suunnittelu ja ohjaus tietoturvavaatimusten täyttämiseksi; ja</li> <li>6) tietoturvallisuuden hallinnan tehokkuuden ja toimivuuden arviointi.</li> </ol> <p><b>M72B 15 Vaatimuksenmukaisuuden arviointikriteerit</b><br/><b>15.1 Tunnistusjärjestelmän ja tunnistusmenetelmän arvioitavat toiminnot</b><br/>Tunnistuspalvelun tunnistus- ja luottamuspalvelulain 29 §:n mukaisen arvioinnin täytyy kattaa kaikki laissa ja tässä määräyksessä asetetut vaatimukset, jotka kohdistuvat:</p> <ol style="list-style-type: none"> <li>1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän): <ol style="list-style-type: none"> <li>a) tietoturvallisuuden hallintaan;</li> <li>b) tietojen säilyttämiseen ja käsittelyyn;</li> <li>c) tiloihin ja henkilökuntaan;</li> <li>d) teknisiin toimenpiteisiin; ja</li> </ol> </li> </ol> | <p>ISO/IEC 30107</p> | <p>sensation Attack Detection). FRR ei oleellinen. Sovellus tulee myös arvioida tai muuten todentaa turvallisuus Liite C:n mukaisella tai muulla vastaavalla menettelyllä</p> |
|--|--|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|     |   |                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |  |                                                                                                                             |
|-----|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|-----------------------------------------------------------------------------------------------------------------------------|
|     |   |                                                                                                                                                                                                                                                            | <p>[...]</p> <p>2) tunnistusmenetelmään eli tunnistusväli-<br/>neen:</p> <ul style="list-style-type: none"> <li>a) hakemiseen ja rekisteröintiin;</li> <li>b) hakijan henkilöllisyyden todistamiseen<br/>ja varmentamiseen;</li> <li>[...]</li> <li>d) myöntämiseen, toimittamiseen ja akti-<br/>vointiin;</li> <li>e) voimassaolon keskeyttämiseen, peruut-<br/>tamiseen ja uudelleen aktivointiin;</li> <li>f) uusimiseen ja korvaamiseen; ja</li> <li>g) todentamismekanismeihin.</li> </ul> <p><b>LoA 2.1.2 Henkilöllisyyden todistaminen ja<br/>varmentaminen (luonnollinen henkilö)</b><br/>Korotettu:<br/>1. Henkilöllä on varmennettu olevan hallussaan sen<br/>jäsenvaltion hyväksymä todiste ilmoitetusta henki-<br/>löllisyydestä, jossa sähköisen tunnistamisen mene-<br/>telmää haetaan<br/>ja<br/>todiste on tarkastettu sen varmistamiseksi, että se<br/>on aito; tai luotettavasta lähteestä tiedetään sen<br/>olevan olemassa ja liittyvän todelliseen henkilöön<br/>ja<br/>on ryhdytty toimiin sen riskin minimoimiseksi,<br/>että henkilön henkilöllisyys ei ole ilmoitettu henki-<br/>löllisyys, ml. riski siitä, että todiste on kadonnut<br/>tai varastettu tai sen voimassaolo on keskeytetty,<br/>peruutettu tai päättynyt;</p> |  |                                                                                                                             |
| 92. | S | Varmistetaan esitetyn dokumen-<br>tin aitous ja tietojen muuttumat-<br>tomuus. Ensitunnistuksessa käy-<br>tettävän dokumentin aktiivinen<br>ja passiivinen todennus, doku-<br>mentin tarkastelu videoyhteyden<br>yli (MRZ, visuaaliset turvateki-<br>jät). | <p><b>LoA liite 2.1.2 Henkilöllisyyden todistaminen<br/>ja varmentaminen (luonnollinen henkilö)</b><br/>Matala:<br/>2. Todisteen voidaan olettaa olevan aito tai luotet-<br/>tavan lähteen mukaan olemassa oleva, ja se näyt-<br/>tää olevan voimassa.</p> <p>Korotettu:<br/>1.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |  | Ensitunnistusdokumentin<br>(passi, henkilökortti) ai-<br>tous ja sirulle tallennettu<br>tiedon aitous on tarkistet-<br>tava |

|     |   |                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |  |                                                                                                                                                                                                                              |
|-----|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |   |                                                                                                                                                                                                                      | [...]<br>todiste on tarkastettu sen varmistamiseksi, että se on aito; tai luotettavasta lähteestä tiedetään sen olevan olemassa ja liittyvän todelliseen henkilöön<br>[...]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |  |                                                                                                                                                                                                                              |
| 93. | S | Etätunnistustapahtuma ja henkilön todennus videoyhteyden yli suoritetaan olosuhteissa, joiden vähimmäisvaatimukset on määritetty.                                                                                    | <b>LoA liite 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)</b><br>Korotettu:<br>1. Henkilöllä on varmennettu olevan hallussaan sen jäsenvaltion hyväksymä todiste ilmoitetusta henkilöllisyydestä, jossa sähköisen tunnistamisen menetelmää haetaan<br>ja<br>todiste on tarkastettu sen varmistamiseksi, että se on aito; tai luotettavasta lähteestä tiedetään sen olevan olemassa ja liittyvän todelliseen henkilöön<br>ja<br>on ryhdytty toimiin sen riskin minimoimiseksi, että henkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, että todiste on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päätynyt; |  | Etäensitunnistustapahtuma suoritetaan sellaisessa tilanteessa tai olosuhteissa, joissa pystytään maksimoimaan automaattisten turvakontrollien toteutuminen.                                                                  |
| 94. | S | Etäensitunnistuksen biometriikkaa analysoivat automaattiset turvakontrollit. Turvakontrollit ovat sattumanvaraisia tai perustuvat menetelmiin, joilla voidaan osoittaa varmuustasoasetuksen vaatimusten täyttyminen. | <b>LoA liite 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)</b><br>Matala:<br>3. Luotettavan lähteen tiedossa on, että ilmoitettu henkilöllisyys on olemassa, ja voidaan olettaa, että henkilöllisyyden ilmoittaneella henkilöllä on tämä sama henkilöllisyys.<br><br>Korotettu:<br>1. Henkilöllä on varmennettu olevan hallussaan sen jäsenvaltion hyväksymä todiste ilmoitetusta henkilöllisyydestä, jossa sähköisen tunnistamisen menetelmää haetaan<br>ja<br>todiste on tarkastettu sen varmistamiseksi, että se on aito; tai luotettavasta lähteestä tiedetään sen olevan olemassa ja liittyvän todelliseen henkilöön<br>ja                                     |  | Toiminnalla pyritään estämään esim. ennalta valmistettujen videosyötteiden luominen. Elävyyden havainnointi eri keinoin automatisoidusti esimerkiksi joko videomateriaalista tai biosignaalien havainnoinnista kasvokuvasta. |

|     |   |                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |  |                                                                                                                                                                                    |
|-----|---|------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |   |                                                                                                                                    | on ryhdytty toimiin sen riskin minimoimiseksi, että henkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, että todiste on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |  |                                                                                                                                                                                    |
| 95. | S | Etäensitunnistustapahtumalle on määritelty tekniset vähimmäisvaatimukset, joiden alittuessa etäensitunnistusta ei voida suorittaa. | <p><b>LoA liite 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)</b></p> <p>Matala:</p> <p>3. Luotettavan lähteen tiedossa on, että ilmoitettu henkilöllisyys on olemassa, ja voidaan olettaa, että henkilöllisyyden ilmoittaneella henkilöllä on tämä sama henkilöllisyys.</p> <p>Korotettu:</p> <p>[...]</p> <p>ja</p> <p>todiste on tarkastettu sen varmistamiseksi, että se on aito; tai luotettavasta lähteestä tiedetään sen olevan olemassa ja liittyvän todelliseen henkilöön</p> <p>ja</p> <p>on ryhdytty toimiin sen riskin minimoimiseksi, että henkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, että todiste on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt;</p> |  | Esim. laitteistotason vähimmäisvaatimukset, tietoliikenneyhteyden katkotomuus ja nopeus, resoluutio, kameran kyvykkyydet, artefaktien esiintyminen, Liite C:n resilienssikriteerit |
| 96. | S | Tietojen siirtäminen, tallennus                                                                                                    | <p><b>LoA liite 2.4.4 Tietojen säilyttäminen</b></p> <p>1. Asiaankuuluvat tiedot kirjataan ja säilytetään käyttämällä tehokasta tiedonhallintajärjestelmää ottaen huomioon sovellettava lainsäädäntö ja tietosuojan ja tietojen säilyttämiseen liittyvät hyvät käytännöt.</p> <p>2. Järjestelmään kirjatut tiedot säilytetään siltä osin kuin tämä on kansallisen lainsäädännön tai muun kansallisen hallinnollisen järjestelyn mukaan sallittua ja suojataan niin kauan kuin niitä tarvitaan tarkastuksia ja tietoturvaloukkausten tutkimista varten ja säilytetään siihen asti, kun tiedot hävitetään turvallisesti.</p>                                                                                                                                                 |  | Tietosuojaa, varsinkin jos tietoa siirtyy EU-alueen ulkopuolelle. Tallennus myös häisempää tarkastelua varten jos esim. havaitaan väärinkäytös.                                    |

|     |   |                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |  |                                                                                                                                                                                         |
|-----|---|----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |   |                                                                                  | <b>myös M72B 7 Tunnistusjärjestelmän rajapintojen salausvaatimukset</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |  |                                                                                                                                                                                         |
| 97. | S | Etäensitunnistuksen suorittava ohjelmistokomponentti tulee olla todennettu.      | <p><b>TunnL 13 § Tunnistuspalvelun tarjoajan yleiset velvollisuudet</b></p> <p>[...]</p> <p>Tunnistuspalvelun tarjoaja vastaa apunaan käyttämiensä henkilöiden tuottamien palveluiden ja tuotteiden luotettavuudesta ja toimivuudesta.</p> <p><b>LoA liite 2.4.6 Tekniset tarkastukset</b></p> <p>1. Käytössä on oikeasuhteiset tekniset tarkastukset palvelujen turvallisuuteen kohdistuvien riskien hallitsemiseksi ja käsiteltävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi.</p> <p>2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät sähköisen viestinnän kanavat on suojattu salakuuntelulta, manipuloinnilta ja toistolta.</p> <p>[...]</p> <p><b>M72B Vaatimuksenmukaisuuden arviointikriteerit</b></p> <p><b>15.1 Tunnistusjärjestelmän ja tunnistusmenetelmän arvioitavat toiminnot</b></p> <p>Tunnistuspalvelun tunnistus- ja luottamuspalvelulain 29 §:n mukaisen arvioinnin täytyy kattaa kaikki laissa ja tässä määräyksessä asetetut vaatimukset, jotka kohdistuvat:</p> <p>1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän):</p> <p>a) tietoturvallisuuden hallintaan;</p> |  | Käytännössä mobiilisovellus ja sovelluksen attestaatio taustajärjestelmälle                                                                                                             |
| 98. | S | Etätunnistuksen on perustuttava ainakin osittain automatisoituihin prosesseihin. | <p><b>LoA liite 2.4.6 Tekniset tarkastukset</b></p> <p>4. Käytössä on menettelyt, joilla varmistetaan, että turvallisuus säilyy ja että kyetään vastaamaan muutoksiin riskitasoissa, poikkeamiin ja tietoturvaloukkauksiin.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |  | Pelkän virkailijan käyttö etäensitunnistamisessa ei ole riittävää, vaan prosessin on perustuttava ainakin osittain tietokoneella tehtyyn vertailuun edellä olevien kriteerien kohdalla. |

|     |   |                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                              |  |                                                                                                                                                                                                                 |
|-----|---|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 99. | S | Etätunnistusprosessiin osallistuvien työntekijöiden tulee olla koulutettuja. | <b>LoA liite 2.4.5 Tilat ja henkilökunta</b><br>1. Käytössä on menettelyt, joilla varmistetaan, että henkilöstöllä ja alihankkijoilla on riittävä koulutus, pätevyys ja kokemus taidoissa, joita he tarvitsevat suorittaakseen tehtävänsä.<br>2. Käytössä on riittävästi henkilöstöä ja alihankkijoita, jotta palvelua voidaan toteuttaa ja resursoida asianmukaisesti sen toimintaperiaatteiden ja menettelyjen mukaisesti. |  | Jos etäensitunnistusprosessissa päätöksentekoon osallistuu myös työntekijä, tulee hänet kouluttaa riittävällä tasolla arvioimaan mahdollisen videomateriaalin aitoutta, ensitunnistuskokemuksen aitoustehtäviä. |
|-----|---|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## B 10 Tunnistusvälineen eli tunnistusmenetelmän elinkaari

### KESKEISET SÄÄNNÖKSET

#### M72B 15.1 Tunnistusjärjestelmän ja tunnistusmenetelmän arvioitavat toiminnot

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

- 2) tunnistusmenetelmään eli tunnistusvälineen
  - a) hakemiseen ja rekisteröintiin
  - b) [...]
  - c) [...]
  - d) myöntämiseen, toimittamiseen ja aktivointiin
  - e) voimassaolon keskeyttämiseen, peruuttamiseen ja uudelleen aktivointiin
  - f) uusimiseen ja korvaamiseen
  - g) [...]

| NRO  | VARMUUSTASO | TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ                                                                                                     | SÄÄNNÖKSET                                                                                                                                                                                                                                                                                    | STANDARDI-VIITTAUS | HUOMIOITA |
|------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-----------|
| 100. | S, H        | Tunnistusvälinettä ei liitetä henkilöön eli personoida ennen ensitunnistamista. Tunnistuksen tekijät kytketään tunnistusmenetelmän haltijaan. | <b>M72B 6.3 Tunnistusvälineen kytkeminen henkilöön</b><br>6.3.1<br>Tunnistusmenetelmän todentamistekijät on kytkettävä tunnistusjärjestelmässä tunnistusvälineen haltijaan.<br><br>6.3.2<br>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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |  |                                                                                                                                                                                                                                                                                                                                                                                                     |
| 101. | S, H | Luonnollisen henkilön henkilötiedot tarkistetaan väestötietojärjestelmästä tunnistusvälinettä myönnettäessä ja säännöllisesti tunnistusvälineen voimassaolon aikana. | <p><b>TunnL 7 § Väestötietojärjestelmän tietojen käyttäminen</b></p> <p>Tunnistusvälineen tarjoajan ja luottamuspalvelua tarjoavan varmentajan on hankittava ja päivitettävä luonnollisen henkilön tunnistuspalvelun tarjoamiseksi tarvitsemansa tiedot väestötietojärjestelmästä. Tämän lisäksi tunnistuspalvelun tarjoajan on varmistettava, että sen tunnistuspalvelun tarjoamiseksi tarvitsemat tiedot ovat ajan tasalla väestötietojärjestelmän tietojen kanssa.<br/>[...]</p> <p><b>Ks. M72B 12 Luottamusverkostossa välitettävät vähimmäistiedot</b></p> <p><b>LoA liite 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)</b></p> <p>Korotettu:</p> <p>1. Henkilöllä on varmennettu olevan hallussaan sen jäsenvaltion hyväksymä todiste ilmoitetusta henkilöllisyydestä, jossa sähköisen tunnistamisen menetelmää haetaan<br/>ja<br/>todiste on tarkastettu sen varmistamiseksi, että se on aito; tai luotettavasta lähteestä tiedetään sen olevan olemassa ja liittyvän todelliseen henkilöön<br/>ja<br/>on ryhdytty toimiin sen riskin minimoimiseksi, että henkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, että todiste on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt;</p> |  | <p>Säännöllisen tarkistamisen tiheyttä ei ole säädetty. Hyvä vakiintunut käytäntö on tarkistus viikoittain.</p> <p>Vrt. (ei viittausta tunnistuslaissa eli muodollisesti sovelletaan vain, jos menetelmä notifioidaan)</p> <p><b>LoA 2.1.1 Hakemus ja rekisteröinti</b></p> <p>3. Kerätään asiaankuuluvat tunnistetiedot, jotka tarvitaan henkilöllisyyden todistamista ja varmentamista varten</p> |
| 102. | S, H | <b>Tunnistusvälineen myöntäminen, toimittaminen, aktivointi</b>                                                                                                      | <b>TunnL 20 § Tunnistusvälineen myöntäminen</b><br>Tunnistusvälineen liikkeelle laskeminen perustuu tunnistusvälineen hakijan ja tunnistuspalvelun tarjoajan väliseen sopimukseen. Sopimus on tehtävä                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |  | Sopimusehdot (mm. TunnL 15 §) kuuluvat toimijan itse selvitettäviin asioihin,                                                                                                                                                                                                                                                                                                                       |

|  |  |                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--|--|---------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  | <p>Tunnistusvälineen luovutus- tai toimitusmenettelyssä varmistetaan, ettei tunnistusväline joudu oikeudettomasti toisen haltuun.</p> | <p>kirjallisesti. Sopimus voidaan tehdä myös sähköisesti, jos sen sisältöä ei voida yksipuolisesti muuttaa ja se säilyy osapuolten saatavilla. [...]</p> <p>Vrt. (Kohtaan LoA 2.1.1 ei ole viittausta tunnistuslaissa eli muodollisesti sitä sovelletaan vain, jos menetelmä notifioidaan)</p> <p><b>LoA 2.1.1 Hakemus ja rekisteröinti</b></p> <p>1. Varmistetaan, että hakija on tietoinen sähköisen tunnistamisen menetelmien käyttöön liittyvistä ehdoista ja edellytyksistä.</p> <p>2. Varmistetaan, että hakija on tietoinen sähköisen tunnistamisen menetelmiin liittyvistä suositelluista varotoimista.</p> <p><b>TunnL 21 § Tunnistusvälineen luovuttaminen hakijalle</b></p> <p>Tunnistusvälineen tarjoajan on luovutettava tunnistusväline sen hakijalle siten kuin sopimuksessa on sovittu. <u>Tunnistuspalvelun tarjoajan on varmistettava, ettei tunnistusväline joudu oikeudettomasti toisen haltuun välinettä luovutettaessa siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.2.2 vähintään korotetulle varmuustasolle säädetty vaatimukset täyttyvät.</u></p> <p><b>LoA Liite 2.2.2 Myöntäminen, toimittaminen ja aktivointi</b></p> <p>Korotettu:</p> <p>Sähköisen tunnistamisen menetelmän myöntämisen jälkeen se toimitetaan käyttäen mekanismia, jonka kautta se voidaan olettaa toimitettavan vain sen henkilön haltuun, jolle se kuuluu.</p> | <p>eivät kuulu auditoinnin piiriin.</p> <p>TunnL 8 §:n ja LoA 2.2.1 mukainen vaatimus varmistaa, että ainoastaan tunnistusvälineen haltija voi käyttää välinettä, liittyy myös luovuttamisen osalta 21 §:ssä erikseen säädettyyn vaatimukseen, jonka mukaan tunnistuspalvelun tarjoajan on varmistettava, ettei tunnistusväline joudu oikeudettomasti toisen haltuun välinettä luovutettaessa.</p> <p>Ks. LoA guidance:</p> <p>Mahdollisia mekanismeja ovat esimerkiksi seuraavat:</p> <ul style="list-style-type: none"> <li>- henkilökohtainen toimitus</li> <li>- toimitus kirjattuna kirjeenä</li> <li>- sellaisen aktivointimenettelyn käyttö, josta voidaan kohtuudella olettaa, että vain henkilöllä on menetelmän aktivointiin tarvittavat tiedot (esimerkiksi oletus-PIN-koodi, joka toimitetaan erillään tunnistamismenetelmästä).</li> </ul> <p>Tasolla "korotettu" on käytettävä useita todentamistekijöitä. Aktivointikoodeja</p> |
|--|--|---------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|      |   |                                                                                                                                                                                                              |                                                                                                                                                                                                                                    |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |   |                                                                                                                                                                                                              |                                                                                                                                                                                                                                    |  | <p>ei välttämättä tarvita. Tason "korotettu" vaatimukset voidaan täyttää monenlaisilla myöntämis-, toimitus- ja aktivointitapojen yhdistelmillä:</p> <ul style="list-style-type: none"> <li>- Sähköisen tunnistamisen menetelmä voidaan toimittaa postitse ja aktivointi tehdä lähettämällä koodi henkilön pankkitilille. Hakija antaa koodin, jolla sähköisen tunnistamisen menetelmä aktivoidaan. Oletuksena on, että pankin todentaminen on vähintään tasolla "korotettu".</li> <li>- Sähköisen tunnistamisen menetelmä ja aktivointikoodi toimitetaan erikseen postitse henkilön varmennettuun osoitteeseen.</li> <li>- Sähköisen tunnistamisen menetelmä toimitetaan postitse hakijan osoitteeseen.</li> <li>- Sähköisen tunnistamisen menetelmä annetaan käyttöön, kun hakijan henkilöllisyys on varmennettu.</li> </ul> |
| 103. | H | <p><b>Tunnistusvälineen myöntäminen, toimittaminen, aktivointi</b></p> <p>Tunnistusvälineen luovutus- tai toimitusmenettelyssä varmistetaan, ettei tunnistusväline joudu oikeudettomasti toisen haltuun.</p> | <p><b>LoA Liite 2.2.2 Myöntäminen, toimittaminen ja aktivointi</b></p> <p><u>Korkea:</u></p> <p>Aktivointiprosessi varmistaa, että sähköisen tunnistamisen menetelmä on toimitettu vain sen henkilön haltuun, jolle se kuuluu.</p> |  | <p>Aktivointiprosessi lähtökohtaisesti edellyttää aktivointikoodin käyttöä. Eriyisesti tulee huolehtia, että aktivointikoodi ei voi päätyä muiden haltuun</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

|      |      |                                                                                                                                                                           |                                                                                                                                                                                                                                                    |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |      |                                                                                                                                                                           |                                                                                                                                                                                                                                                    |  | <p>toimittamisprosessissa, ja että aktivointikoodi on kertakäyttöinen, eikä sitä voi käyttää esimerkiksi uudelleenaktivointiin tai uuden pin-koodin luomiseen. Jos aktivointia ei suoriteta tietyn ajan kuluessa, aktivointikoodi vanhenee.</p> <p>Tarkoituksena on varmistaa, ettei käyttämättä jääneellä tai uudelleen käytettävällä aktivointikoodilla voida mitätöidä eli ylikirjoittaa vain käyttäjän tiedossa oleva todentamiskijä (PIN) tai aktivoida tunnistusmenetelmää tämän tietämättä. Tunnistustuloksissa ei ole viittausta LoA kohtaan 2.2.3 "Käytössä ovat toimenpiteet, joilla estetään voimassaolon luvaton keskeyttäminen, peruuttaminen ja/tai uudelleenaktivointi." Koodin kertakäyttöisyys on kuitenkin hyvä käytäntö, jollei muin tavoin voida suojata tunnistusvälineen luvaton uudelleenaktivointi.</p> |
| 104. | S, H | <p><b>Tunnistusvälineen voimassaolon keskeyttäminen, peruuttaminen ja uudelleen aktivointi</b></p> <p>Tunnistusvälineen tarjoajalla on 24/7 -sulkupalvelu käyttäjille</p> | <p><b>TunnL 25 § Tunnistusvälineen peruuttamista tai käytön estämistä koskeva ilmoitus</b></p> <p>Tunnistusvälineen haltijan on ilmoitettava tunnistusvälineen tarjoajalle tai tämän nimeämälle muulle taholle tunnistusvälineen katoamisesta,</p> |  | <p>Vrt. (kohtaan LoA 2.2.3 ei ole viittausta tunnistustuloksissa eli sitä sovelletaan vain, jos menetelmä notifioidaan)</p> <p><b>LoA Liite 2.2.3 Voimassaolon keskeyttäminen,</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

|  |  |                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  | <p>sekä sulkulista luottaville osapuolille tai mahdollisuus teknisesti estää käyttäjän kadonneeksi tai varastetuksi ilmoittaman tunnistusvälineen käyttö.</p> | <p>joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä ilman aiheetonta viivytystä havaittuaan asian.</p> <p><u>Tunnistusvälineen tarjoajan on tarjottava mahdollisuus tehdä 1 momentissa tarkoitettu ilmoitus milloin tahansa. Tunnistusvälineen tarjoajan on viipymättä peruutettava tunnistusväline tai estettävä sen käyttö saatuaan asiaa koskevan ilmoituksen.</u></p> <p>Tunnistusvälineen tarjoajan on asianmukaisesti ja viipymättä merkittävä järjestelmään tieto peruuttamisen tai käytön estämisen ajankohdasta. Tunnistusvälineen haltijalla on oikeus saada pyynnöstä todistus siitä, että hän on tehnyt 1 momentissa tarkoitettun ilmoituksen. Todistusta on pyydetävä 18 kuukauden kuluessa ilmoituksesta.</p> <p><u>Järjestelmän on oltava sellainen, että tunnistuspalvelua käyttävä palveluntarjoaja voi helposti tarkastaa siihen merkityt tiedot ympäri vuorokauden. Velvollisuutta järjestää tarkastusmahdollisuutta ei kuitenkaan ole, jos tunnistusvälineen käyttö voidaan teknisesti estää tai se voidaan sulkea.</u><br/>[...]</p> <p><b>26 § Tunnistusvälineen tarjoajan oikeus peruuttaa tai estää tunnistusvälineen käyttö</b><br/>Sen lisäksi, mitä 25 §:ssä säädetään, tunnistusvälineen tarjoaja voi peruuttaa tunnistusvälineen tai estää sen käytön, jos:</p> <ol style="list-style-type: none"> <li>1) tunnistusvälineen tarjoajalla on syytä epäillä, että joku muu kuin se, jolle tunnistusväline on myönnetty, käyttää sitä;</li> <li>2) tunnistusväline sisältää ilmeisen virheellisyiden;</li> <li>3) tunnistusvälineen tarjoajalla on syytä epäillä, että tunnistusvälineen käytön turvallisuus on vaarantunut;</li> </ol> | <p><b>peruuttaminen ja uudelleenaktivointi</b></p> <ol style="list-style-type: none"> <li>1. Sähköisen tunnistamisen menetelmän voimassaolo on mahdollista keskeyttää ja/tai peruuttaa viivyttelemättä ja tehokkaasti.</li> <li>2. Käytössä ovat toimenpiteet, joilla estetään voimassaolon luvaton keskeyttäminen, peruuttaminen ja/tai uudelleenaktivointi.</li> <li>3. Uudelleenaktivoinnin ehtona on, että ennen voimassaolon keskeyttämistä tai peruuttamista asetetut varmuusvaatimukset täyttyvät edelleen.</li> </ol> |
|--|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|      |      |                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |  |                                                                                                                                                                                                                                                                                                                            |
|------|------|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |      |                                                   | <p>4) tunnistusvälineen haltija käyttää tunnistusvälinettä olennaisesti sopimusehtojen vastaisella tavalla;</p> <p>5) tunnistusvälineen haltija on kuollut.</p> <p>Tunnistusvälineen tarjoajan tulee ilmoittaa haltijalle niin pian kuin mahdollista tunnistusvälineen peruuttamisesta tai käytön estämisestä ja sen ajankohdasta sekä siihen johtaneista syistä.</p> <p>Tunnistusvälineen tarjoajan on palautettava mahdollisuus käyttää tunnistusvälinettä tai annettava haltijalle uusi väline välittömästi 1 momentin 2 ja 3 kohdassa tarkoitetun syyn poistuttua.</p> <p><b>LoA liite 2.2.3 Voimassaolon keskeyttäminen, peruuttaminen ja uudelleenaktivointi</b></p> <p>1. Sähköisen tunnistamisen menetelmän voimassaolo on mahdollista keskeyttää ja/tai peruuttaa viivyttämättä ja tehokkaasti.</p> <p>2. Käytössä ovat toimenpiteet, joilla estetään voimassaolon luvaton keskeyttäminen, peruuttaminen ja/tai uudelleenaktivointi.</p> <p>3. Uudelleenaktivoinnin ehtona on, että ennen voimassaolon keskeyttämistä tai peruuttamista asetetut varmuusvaatimukset täyttyvät edelleen.</p> |  |                                                                                                                                                                                                                                                                                                                            |
| 105. | S, H | <b>Tunnistusvälineen uusiminen ja korvaaminen</b> | <p><b>TunnL 22 § Tunnistusvälineen uusiminen</b></p> <p>Tunnistusvälineen tarjoaja saa toimittaa tunnistusvälineen haltijalle uuden välineen ilman nimenomaista pyyntöä vain, jos aikaisemmin annettu tunnistusväline on korvattava uudella. Tunnistusvälineen uusimisessa tulee noudattaa sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.2.4 vähintään korotetulle varmuustasolle säädettyjä vaatimuksia.</p> <p><b>LoA Liite 2.2.4 Uusiminen ja korvaaminen</b></p> <p>Ottaen huomioon riskit henkilön tunnistetiedoissa tapahtuvista muutoksista uusimisen tai korvaamisen on täytettävä samat varmuusvaatimukset kuin</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                      |  | <p>TunnL 8 §:n ja LoA 2.2.1 ja 2.2.2 mukaisen varmistusvaatimuksen, että ainoastaan tunnistusvälineen haltija voi käyttää välinettä, täytyy toteutua myös kaikissa tilanteissa, joissa osa tai kaikki todenmistekijät tai uusi aktiivointikoodi luovutetaan uusimisen/korvaamisen tai uudelleenaktivoinnin yhteydessä.</p> |

|      |   |                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------|---|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |   |                                                   | <p>henkilöllisyyden alkuperäisen todistamisen ja varmentamisen yhteydessä tai sen on perustuttava saman tai korkeamman varmuustason voimassa olevaan sähköisen tunnistamisen menetelmään.</p> <p><b>LoA liite 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu</b><br/>Korotettu:<br/>2. Sähköisen tunnistamisen menetelmä on suunniteltu siten, että sitä voidaan olettaa käytettävän vain, jos se on sen henkilön hallinnassa tai hallussa, jolle se kuuluu.</p> <p><b>LoA Liite 2.2.2 Myöntäminen, toimittaminen ja aktivointi</b><br/>Korotettu:<br/>Sähköisen tunnistamisen menetelmän myöntämisen jälkeen se toimitetaan käyttäen mekanismia, jonka kautta se voidaan olettaa toimitettavan vain sen henkilön haltuun, jolle se kuuluu.</p> |  | <p>Ks. Tulkintakannanotto<br/>Dnro: Traficom/106/09.02.00/2019 (25.3.2019) Liikenne- ja viestintäviraston tulkintamuistio ajokortin käyttämisestä henkilöllisyyden todentamisessa tunnistusvälineen lukkiutuessa tai uusittaessa tunnistusväline tai todentamistekijä. Kannanotto löytyy viraston verkkosivuilta<br/><a href="https://www.kyberturvallisuuskeskus.fi/fi/sahkoi-nen-tunnistaminen">https://www.kyberturvallisuuskeskus.fi/fi/sahkoi-nen-tunnistaminen</a></p> |
| 106. | H | <b>Tunnistusvälineen uusiminen ja korvaaminen</b> | <p><b>LoA Liite 2.2.4 Uusiminen ja korvaaminen</b><br/>Matala/korotettu:<br/>Ottaen huomioon riskit henkilön tunnistetiedoissa tapahtuvista muutoksista uusimisen tai korvaamisen on täytettävä samat varmuusvaatimukset kuin henkilöllisyyden alkuperäisen todistamisen ja varmentamisen yhteydessä tai sen on perustuttava saman tai korkeamman varmuustason voimassa olevaan sähköisen tunnistamisen menetelmään.<br/>Korkea:<br/>Jos uusiminen tai korvaaminen perustuu voimassa olevaan sähköisen tunnistamisen menetelmään, tunnistetiedot varmennetaan luotettavasta lähteestä.</p> <p><b>LoA liite 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu</b><br/>Korkea:</p>                                                                   |  | <p>TunnL 8 §:n ja LoA 2.2.1 ja 2.2.2 mukaisen varmistusvaatimuksen, että ainoastaan tunnistusvälineen haltija voi käyttää välinettä, täytyy toteutua myös kaikissa tilanteissa, joissa osa tai kaikki todentamistekijät tai uusi aktivointikoodi luovutetaan uusimisen/korvaamisen tai uudelleenaktivoinnin yhteydessä.</p>                                                                                                                                                  |

|  |  |  |                                                                                                                                                                                                                                                                                                                                                                      |  |  |
|--|--|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
|  |  |  | <p>2. Sähköisen tunnistamisen menetelmä on suunniteltu niin, että henkilö, jolle se kuuluu, voi suojata sen luotettavasti muiden käytöltä.</p> <p><b>LoA Liite 2.2.2 Myöntäminen, toimittaminen ja aktivointi</b><br/>Korkea:<br/>Aktivointiprosessi varmistaa, että sähköisen tunnistamisen menetelmä on toimitettu vain sen henkilön haltuun, jolle se kuuluu.</p> |  |  |
|--|--|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|

## **Sähköisen tunnistuspalvelun arviointiohje**

Liikenne- ja viestintäviraston ohje

211/2023 O Liite C Mobiilikriteeristö

## LIITE C Mobiilitunnistusratkaisun erityiskriteeristö

### Yleistä

Mobiilisovelluskriteeristö **täydentää yleistä kriteeristöä**, jos tunnistusmenetelmässä tai -järjestelmässä on yhtenä osana mobiilisovellus.

Kriteeristö on laadittu **pääsääntöisesti varmuustasolle korotettu**. Viittaukset varmuustasoasetukseen (EU) 2015/1502 (LoA) ovat varmuustasolle korotettu, ellei toisin mainita. Kriteeristöä voidaan tulevaisuudessa päivittää ja huomioida myös korkea varmuustaso, kun soveltamisesta saadaan kokemusta Suomessa ja kun eIDAS-sääntelyn vaatimusten tulkinnasta syntyy yhtenäisiä käytäntöjä Euroopassa.

Tämä asiakirja on luonteeltaan ohje. Arvioijan tehtävänä on punnita kuinka hyvin sovellus vastaa ohjeen kriteereitä. Poikkeamien aiheuttama riski arvioidaan kokonaisuutena. Käyttöjärjestelmän ja tunnistussovelluksen versiointia on seurattava ja arvioitava muutosten kokonaisvaikutusta vaatimustenmukaisuuden toteutumiseen. Tunnistuspalvelun tarjoajan on varmistuttava siitä, että se saa riittävästi ajantasaista tietoa sovelluksen toimittajalta laitteisto- ja ohjelmistotason muutoksista.

Arkaluonteinen tieto (OWASP:n kriteeristössä "sensitive") tarkoittaa tässä yhteydessä esimerkiksi henkilötietoja, salausteknistä aineistoa tai tunnistus- tai rekisteröintitapahtumaan liittyviä luottamuksellisia/salassa pidettäviä tietoja.

Ohje on tarkoitettu mobiilitunnistussovellusten tietoturvallisuuden arviointiin. Tällaisilla sovelluksilla on tyypillisesti vahva yhteys myöntäjän taustajärjestelmään. Tämän ohjeen avulla voidaan myös arvioida lompakotyyppisiä sovelluksia, joiden yhteys taustajärjestelmään on minimoitu.

App/Wallet -merkinnällä tarkoitetaan tunnistusmenetelmää, eli päätelaitteessa ajettavaa sovellusta tai sovelluksen osaa, joka tekee vahvaa sähköistä tunnistusta.

Kriteeristö pohjautuu OWASP:n englanninkieliseen Mobile AppSec Verification -dokumenttiin (OWASP Mobile Application Security Verification Standard, MASVS version 1.4.2), jota on laajennettu ja muokattu vastaamaan tunnistuksen käyttötapauksia.

OWASP:n alkuperäistä kriteeristöä vastaava testausohje löytyy OWASP:n verkkosivuilta. Tästä julkaisusta löytyvät yksityiskohtaiset ja kattavat ohjeet alkuperäisten OWASP kriteerien testaukseen.

Vaihtoehtoiset kriteerit:

- FIDO 3 & 3+ (<https://fidoalliance.org/certification/authenticator-certification-levels/>)

## C 1 Arkkitehtuuri, suunnittelu ja uhkakuvien mallintaminen

| NRO  | VAR-<br>MUUS-<br>TASO | KRITEERI                                                                                                                                                                              | PERUSTE                                                           | Lisätieto / kommentti                                                                                                    |
|------|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| 400. |                       | Kaikki sovelluksen/lompakon komponentit on tunnistettu, luokiteltu ja ne ovat tarpeellisia.                                                                                           | LoA 2.4.6, kohta 1<br>TunnL 8.1 § 4 kohta                         |                                                                                                                          |
| 401. |                       | Turvakontrolleja ei toteuteta vain asiakkaan puolella, vaan aina molemmissa etäpäätepisteissä.                                                                                        | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.3.c                        |                                                                                                                          |
| 402. |                       | Korkean tason arkkitehtuuri on määritelty itse sovellukselle/lompakolle ja siihen liittyville ulkoisille palveluille, ja tietoturva on arkkitehtuurissa huomioitu.                    | LoA 2.4.6, kohta 1<br>TunnL 8.1 § 4 kohta                         |                                                                                                                          |
| 403. |                       | Sovelluksessa/lompakossa käsiteltävät arkaluonteiset tiedot on selvästi tunnistettu ja luokiteltu, ja niiden suojaustoimenpiteet on dokumentoitu.                                     | LoA 2.4.4, kohta 1<br>LoA 2.4.6, kohta 1 ja 3                     |                                                                                                                          |
| 404. |                       | Kaikki sovelluksen/lompakon komponentit on määritelty niiden tarjoamien liiketoiminta- ja/tai turvallisuuksien pohjalta.                                                              | LoA 2.4.6, kohta 1<br>TunnL 8.1 § 4 kohta                         |                                                                                                                          |
| 405. |                       | Sovellukseen/lompakkoon ja sen käyttämiin ulkoisiin palveluihin liittyvät uhkakuvat ja mahdolliset vastatoimet on tunnistettu.                                                        | LoA 2.3.1, korotettu, kohta 2<br>LoA 2.3.1, korkea                | Arvioidaan hyökkäyspotentiaalia koh-<br>tuullinen (korotettu) tai korkea (korkea)                                        |
| 406. |                       | Kaikilla turvakontrolleilla on keskitetty toteutus                                                                                                                                    | LoA 2.4.6, kohta 1                                                |                                                                                                                          |
| 407. |                       | Paikalliset turvakontrollit on toteutettu alan parhaiden käytäntöjen mukaisesti ja validoitu näillä kriteereillä.                                                                     | LoA 2.4.6, kohta 1<br>M72B, alakohta 6.1.1                        |                                                                                                                          |
| 408. |                       | Salausavainten hallintaan on tarkkaan määritelty menetelmätapa, joka pohjautuu kansainvälisesti hyväksyttyyn ajantasaiseen standardiin.                                               | LoA 2.4.6, kohta 3<br>LoA 2.4.6, korotettu                        |                                                                                                                          |
| 409. |                       | Sovellus/lompakko ilmoittaa (sovelluksen/lompakon myöntäjän) palvelimelle käytössä olevan käyttöjärjestelmän, laitteiston ominaisuudet ja sovellusversion numeron.                    | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.3.c                        |                                                                                                                          |
| 410. |                       | Ratkaisuun sisältyy mekanismi, jolla varmistetaan, että sovellus on aito eikä sitä ole käsitelty asiattomasti, kun se esittää todentamis-/attribuuttitietoja luottavalle osapuolelle. | LoA 2.3.1, korotettu                                              |                                                                                                                          |
| 411. |                       | Sovellus/lompakko ei tue mobiilikäyttöjärjestelmien versioita, joiden tuki/turvallisuuspäivitykset käyttöjärjestelmien tarjoajilta ovat päättyneet, eikä toimi niillä.                | TunnL 8.1 § 4 kohta<br>M72B, alakohta 5.4.d<br>LoA 2.4.6, kohta 4 | Sovelluksen/lompakon on läpäistävä riskiarviointiprosessi. Jos riskiarvioinnissa päädytään siihen tulokseen, että vanhat |

|      |  |                                                                                                                                                                                     |                                                |                                                                                                                                                                                          |
|------|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |  |                                                                                                                                                                                     |                                                | käyttöjärjestelmät, jotka eivät enää vastaanota tietoturvapäivityksiä, ovat sopivia, voidaan käyttää myös tuettomia käyttöjärjestelmiä. Tämä selvitys on liitettävä tarkastusraporttiin. |
| 412. |  | Olemassa on mekanismi sovelluksen/lompakon päivityksen pakottamiseen.                                                                                                               | ITSA section 8.1.4 M72B, subsection 5.4. d     |                                                                                                                                                                                          |
| 413. |  | Vanhentunut sovellus/lompakko kehottaa käyttäjää päivittämään käyttöjärjestelmän ja/tai sovelluksen/lompakon, jotta transaktio voidaan suorittaa tai kun sovellus/lompakko avataan. | (LoA 2.1.1, kohta 2)                           | Suositeltava käytäntö / Best practise (BP). LoA 2.1.1 ei sisälly tunnustuslakiin.                                                                                                        |
| 414. |  | Tietoturvallisia käytäntöjä noudatetaan koko ohjelmistokehityksen elinkaaren ajan                                                                                                   | LoA 2.4.6, kohta 1 ja 4<br>TunnL 8.1 § 4 kohta |                                                                                                                                                                                          |

## C 2 Tietojen tallennus ja tietosuoja

Arkaluonteinen tieto (OWASP:n kriteeristössä "sensitive") tarkoittaa tässä yhteydessä esimerkiksi henkilötietoja, salausteknistä aineistoa tai tunnistus- tai rekisteröintitapahtumaan liittyviä luottamuksellisia/salassa pidettäviä tietoja.

| NRO  | VAR-<br>MUUS-<br>TASO | KRITEERI                                                                                                                                                                         | PERUSTE                                    | Lisätieto / kommentti |
|------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|-----------------------|
| 415. |                       | Alustan tarjoamia turvapalveluita ja -ominaisuuksia hyödynnetään täysimittaisesti sovelluksen tallentaessa arkaluonteista tietoa.                                                | LoA 2.4.6, kohta 1, kohta 3                |                       |
| 416. |                       | Käyttäjää informoidaan selkeästi siitä, minkä tasoista tunnistusta ollaan tekemässä.                                                                                             | LoA 2.1.1, kohta 2                         | Suositeltava käytäntö |
| 417. |                       | Mitään arkaluonteista tietoa ei tallenneta sovellus-/lompakkoympäristön tai alustan tarjoaman salaisuuk-<br>sien tallennusta varten tarkoitettun ominaisuuden ulko-<br>puolelle. | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.4.b |                       |
| 418. |                       | Mitään arkaluonteista tietoa ei kirjoiteta sovelluksen lokeihin.                                                                                                                 | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.4.b |                       |
| 419. |                       | Mitään arkaluonteista tietoa ei jaeta ulkoisten tahojen kanssa, ellei se ole ennalta määritelty arkkitehtuurissa.                                                                | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.4.b |                       |
| 420. |                       | Välimuistia ei käytetä tekstinsyöttökentissä, jotka saattavat sisältää arkaluonteista tietoa.                                                                                    | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.4.b |                       |

|      |  |                                                                                                                                                                                                       |                                                                            |                                                                                                                                                                                               |
|------|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 421. |  | Arkaluontaista tietoa tai salaisuuksia (salasana, PIN-koodi) ei missään vaiheessa paljasteta käyttöliittymän kautta.                                                                                  | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.4.b                                 |                                                                                                                                                                                               |
| 422. |  | Leikepöytää ei käytetä tietoelementtien kohdalla, jotka saattavat sisältää arkaluonteista tietoa.                                                                                                     | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.4.b                                 |                                                                                                                                                                                               |
| 423. |  | Arkaluonteista tietoa ei jaeta käytettäessä IPC-mekanismia                                                                                                                                            | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.4.                                  |                                                                                                                                                                                               |
| 424. |  | Tunnistukseen käytettyjä salaisuuksia ei tallenneta tai siirretä sovelluksessa käytetyn tietovaraston ulkopuolelle.                                                                                   | LoA 2.4.6, matala, kohta 3<br>LoA 2.4.6, korotettu<br>M72B, alakohta 5.4.b |                                                                                                                                                                                               |
| 425. |  | Sovelluksen/lompakon siirtyessä taustalle arkaluonteinen tieto poistetaan käyttöliittymäkomponenteista.                                                                                               | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.4.b                                 |                                                                                                                                                                                               |
| 426. |  | Sovellus/lompakko ei pidä arkaluonteista tietoa muistissa tarpeettoman pitkään, ja kun tietoa ei enää tarvita, se poistetaan muistista.                                                               | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.4.b                                 |                                                                                                                                                                                               |
| 427. |  | Sovellus/lompakko suosittelee loppukäyttäjälle minimitalon laiteturvallisuuden käyttöönottoa (puhelimien PIN-koodisuojaus tai biometrinen avausmekanismi tai vastaavat).                              | LoA 2.1.1, kohta 2                                                         | Suositeltava käytäntö                                                                                                                                                                         |
| 428. |  | Käyttäjälle kerrotaan parhaista käytännöistä, joita hänen tulisi noudattaa henkilöllisyyden määrittämistä koskevien tietojen käsittelyssä                                                             | LoA 2.1.1, kohta 2                                                         | Suositeltava käytäntö                                                                                                                                                                         |
| 429. |  | Mitään arkaluonteista tietoa ei tulisi tallentaa paikallisesti mobiililaitteelle. Tiedot tulee sen sijaan hakea etäpäätepuolelta tarvittaessa ja säilyttää vain muistissa.                            | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.4.b                                 |                                                                                                                                                                                               |
| 430. |  | Jos arkaluonteista tietoa on tästä huolimatta tallennettava paikallisesti, se on salattava laitteistoon perustuvan tietovaraston avaimella, joka edellyttää todentamiskäytön tai -tekijöiden käyttöä. | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.4.b                                 | Periaatteena on arkaluonteisen tiedon tallentamisen minimointi. Lompakko-tyyppinen sovellus tallentaa arkaluonteista tietoa, joten tätä kriteeriä tulee soveltaa lompakotyyliin sovelluksiin. |
| 431. |  | Sovellus/lompakko on poistettava käytöstä (todentamiskäytön) viiden epäonnistuneen todennusyrityksen jälkeen.                                                                                         | M72B, alakohta 6.1.2                                                       | Sovelluksen käytön jatkaminen edellyttää normaalin myöntämis-/aktivointiprosessin noudattamista.                                                                                              |
| 432. |  | Jos uudelleenyritysten määrää ei voida kommunikoida palvelimelle, sovelluksen/lompakon paikallisen uudelleenyrityslaskurin on oltava asianmukaisesti suojattu.                                        | LoA 2.3.1, korotettu, kohta 2<br>M72B, alakohta 5.3.e-f                    |                                                                                                                                                                                               |

### C 3 Salausvaatimukset

| NRO  | VAR-<br>MUUS-<br>TASO | KRITEERI                                                                                                                                 | PERUSTE                                                                               | Lisätieto / kommentti                                                                                                                                                                                                                                                                                          |
|------|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 433. |                       | Sovellus/lompakko ei luota symmetrisiin salausmenetelmiin ja kovakoodattuihin avaimiin ainoana salauskeinona.                            | M72B, alakohta 5.3.g,<br>M72B, kohta 7                                                |                                                                                                                                                                                                                                                                                                                |
| 434. |                       | Sovellus/lompakko käyttää hyväksi havaittuja salausprimitiivejä, jotka soveltuvat käyttötapauksiin ja noudattavat säädöksiä.             | M72B, alakohta 5.3.g                                                                  |                                                                                                                                                                                                                                                                                                                |
| 435. |                       | Sovellus/lompakko ei käytä vanhentuneita tai huonoiksi todettuja salauskäytäntöjä tai -algoritmeja                                       | M72B, alakohta 5.3.g<br>M72B, kohta 7                                                 |                                                                                                                                                                                                                                                                                                                |
| 436. |                       | Salausprimitiivit on konfiguroitu parhaiden käytäntöjen ja säädösten vaatimusten mukaisesti (jos olemassa).                              | LoA 2.4.6, kohta 2<br>M72B, alakohta 7.1                                              |                                                                                                                                                                                                                                                                                                                |
| 437. |                       | Sovellus/lompakko ei käytä samoja salausavaimia uudelleen eri tarkoituksiin.                                                             | LoA 2.4.6, kohta 1<br>TunnL 8.1 § 4 kohta                                             |                                                                                                                                                                                                                                                                                                                |
| 438. |                       | Käytetty satunnaislukugeneraattori on tarpeeksi turvallinen ja laadukas.                                                                 | LoA 2.4.6, kohta 1<br>TunnL 8.1 § 4 kohta                                             |                                                                                                                                                                                                                                                                                                                |
| 439. |                       | Sovelluksen/lompakon käytössä on allekirjoituslaskuri, eli palvelin pystyy mahdollisesti huomaamaan sovelluksen kloonausyrityksen        | LoA 2.3.1, korotettu, kohta 2<br>LoA 2.3.1, korkea                                    |                                                                                                                                                                                                                                                                                                                |
| 440. |                       | Sovellus/lompakko ei sisällä eikä käytössä ole mitään kovakoodattuja käyttäjätunnuksia tai salasanoja.                                   | LoA 2.4.6, kohta 1<br>LoA 2.3.1, kohta 2<br>M72B, kohta 6                             | Kehitysaikaiset käyttäjätunnukset (jos olemassa) on puhdistettava tuotantoon menevästä versiosta. Ei kovakoodattuja käyttäjätunnuksia/salaisuuksia, jotka antavat palveluntarjoajalle pääsyn sovellukseen.<br>Mahdolliset aktivointi- ja PUK-koodit ovat kertakäyttöisiä ja voimassa ennalta määritellyn ajan. |
| 441. |                       | Sovelluksen mahdolliset heikommat kehitysaikaiset salauskäytännöt, tunnisteet ja varmenteet on poistettu tuotantoon menevästä versiosta. | LoA 2.4.6, kohta 1 ja 3<br>LoA 2.4.6, korkea<br>M72B, alakohta 5.3.g<br>M72B, kohta 7 |                                                                                                                                                                                                                                                                                                                |

## C 4 Tunnistaminen, tunnistusmenetelmän ominaispiirteet ja istunnonhallinta

Tässä kappaleessa käytetään soveltuvin osin OWASP:n standardia ja kappaletta 4. Lisäksi kriteerejä on listattu nimenomaan tunnistusmenetelmän ominaispiirteisiin liittyen.

| NRO  | VAR-MUUS-TASO | KRITEERI                                                                                                                                                                                                                                   | PERUSTE                                                                   | Lisätieto / kommentti                                                                                                                                                                        |
|------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 442. |               | Sovelluksen/lompakon yksilöinnissä rekisteröintivaiheen aikana varmistetaan siitä, että sovellus kytketään tunnistusvälineen haltijaan.                                                                                                    | LoA 1 (määritelmät), kohta 2<br>LoA 2.2.1, korotettu, kohta 2             |                                                                                                                                                                                              |
| 443. |               | Tunnistuksen toteuttava salaisuus on suojattu väärinkäyttöä vastaan, ja salaisuuteen pääsee käsiksi vain ennalta määritellyllä, turvallisella tavalla.                                                                                     | LoA 2.4.6, kohta 3<br>LoA 2.4.6, korotettu<br>M72B, alakohta 6.4.2        | Esim. yksityinen avain.                                                                                                                                                                      |
| 444. |               | Salaisuudet / tunnistusavaimet ovat yksilöllisiä                                                                                                                                                                                           | M72B, alakohta 5.3.g                                                      |                                                                                                                                                                                              |
| 445. |               | Tunnistuksen toteuttavat asymmetriset salaisuudet luodaan päätelaitteessa (avainpari, muu salainen avain / salaisuus)                                                                                                                      | M72B, alakohta 5.3.g<br>M72B, alakohta 5.4.b                              | vrt RTS                                                                                                                                                                                      |
| 446. |               | Jos tunnistuksen toteuttavat salaisuudet luodaan laitteen ulkopuolella, ne provisioidaan turvallisesti käytettävään laitteeseen.                                                                                                           | LoA 2.4.6, kohta 2<br>LoA 2.4.6, korotettu<br>M72B, alakohta 5.4.b        | vrt. RTS                                                                                                                                                                                     |
| 447. |               | Jos tunnistuksen toteuttavat salaisuudet luodaan laitteen ulkopuolella ja provisioidaan turvallisesti käytettävään laitteeseen, yhteys salaisuuden ja PID:n (henkilön/haltijan) välille luodaan laitteella ja vain rekisteröintivaiheessa. | LoA 2.3.1, kohta 2<br>LoA 2.2.1, korotettu, kohta 2<br>M72B, alakohta 6.3 |                                                                                                                                                                                              |
| 448. |               | Tunnistus ei saa pohjautua pelkästään jaettuun salaisuuteen.                                                                                                                                                                               | LoA 2.2.1, korotettu, kohta 2                                             |                                                                                                                                                                                              |
| 449. |               | Sovelluksen alustuksessa salaisuudet sidotaan päätelaitteeseen niin, että salaisuuksia ei voi kopioimalla käyttää toisessa laitteessa tai siirtää toiseen laitteeseen niin, että salaisuuksia pystyttäisiin siinä käyttämään.              | LoA 2.2.1, korotettu, kohta 2<br>M72B, alakohta 6.4.2                     |                                                                                                                                                                                              |
| 450. |               | Sovellus/lompakko toteuttaa laitesidonnan usean laitteelle uniikin ominaisuuden pohjalta luodun laitteen sormenjäljen avulla.                                                                                                              | LoA 2.3.1, matala, kohta 3, korotettu, kohta 2<br>M72B, alakohta 6.1      | Sovelluksen/lompakon tulee ottaa käyttöön menetelmiä/mekanismeja laitteen sitomiseen tai laitesidontaa vastaava mekanismi. Tämä saattaa kuitenkin olla ongelmallista sekä iOS- että Android- |

|      |  |                                                                                                                                                                                                                                                                        |                                                                                                                                                  |                                                                                |
|------|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
|      |  |                                                                                                                                                                                                                                                                        |                                                                                                                                                  | alustoille käytettäessä laitteen sormen-jälkiominaisuuksia.                    |
| 451. |  | Sovellus/lompakko ei missään vaiheessa tallenna pysyvästi tunnistetietoja/käyttäjätunnuksia (salasanat, PIN-koodit, käyttäjätunnukset jne.).                                                                                                                           | LoA 2.2.1, korotettu, kohta 2<br>LoA 2.2.1, korkea, kohta 2<br>LoA 2.3.1, korotettu, kohta 2<br>LoA 2.3.1, korkea, kohta 2<br>LoA 2.4.6, kohta 3 |                                                                                |
| 452. |  | Sovellus/lompakko mahdollistaa pseudonymisoidun tunnistautumisen.                                                                                                                                                                                                      | M72B, alakohta 12.3 (GDPR 32 artikla)                                                                                                            | Koskee lompakkotyyppisiä sovelluksia tai yksityisyyden suojaamista.            |
| 453. |  | Jos sovellus/lompakko voi tallentaa kolmannelta osapuolelta provisioituja tai käyttäjän luomia attribuutteja, sovellus/lompakko tallentaa ne turvallisesti.                                                                                                            | LoA 2.4.6, kohta 1–2<br>M72B, alakohta 6.1 ja 9.1.1                                                                                              | Koskee lompakkotyyppisiä sovelluksia.                                          |
| 454. |  | Jos sovellus/lompakko mahdollistaa kolmannen osapuolen attribuuttien lisäämisen, ne provisioidaan turvallisella käytännöllä ja esityksellä.                                                                                                                            | LoA 2.4.6, kohta 1–2<br>M72B, alakohta 6.1 ja 9.1.1                                                                                              | Koskee lompakkotyyppisiä sovelluksia.                                          |
| 455. |  | Attribuutteja paikallisesti tallentava sovellus/lompakko varmistaa attribuuttien salassapidon ja eheyden turvaelementin avulla.                                                                                                                                        | LoA 2.4.6, kohta 1–2                                                                                                                             | Joko itse turvaelementissä tai käyttämällä avainta, jota turvaelementti suoja. |
| 456. |  | Jos sovelluksen/lompakon avulla esitetään attribuutteja suoraan luottavalle osapuolelle, sovellus/lompakko toteuttaa sekä siirron että esityksen turvallisella käytännöllä, yksityisyyden suojaavalla esitystavalla ja turvallisella formaatilla.                      | LoA 2.4.6, kohta 1–2<br>M72B, alakohta 6.1 ja 9.1.1                                                                                              | Koskee lompakkotyyppisiä sovelluksia.                                          |
| 457. |  | Jos sovellus/lompakko sallii käyttäjän esittää attribuutteja suoraan luottavalle osapuolelle, sovelluksen/lompakon on todennettava luotettavasta lähteestä, että luottavalla osapuolella on oikeus vastaanottaa näitä attribuutteja.                                   | [eIDAS2]<br>LoA 2.4.6, matala kohta 3                                                                                                            | Koskee lompakkotyyppisiä sovelluksia.                                          |
| 458. |  | Jos sovellus/lompakko havaitsee, että luottava osapuoli pyytää tietoa, johon sillä ei ole oikeutta, sovellus varoittaa selkeästi loppukäyttäjää luottavan osapuolen oikeuksien ulkopuolisten attribuuttien jakamisesta.                                                | [eIDAS2]<br>LoA 2.4.6, matala kohta 3                                                                                                            | Koskee lompakkotyyppisiä sovelluksia.                                          |
| 459. |  | Jos sovellus/lompakko lähettää palvelimelle viestejä, joiden palvelinpäässä tapahtuva validointi johtaa tunnistukseen, tulee kyseiset viestit lähettää turvallisesti käyttäen ajantasaisia ja hyväksytyjä salauskäytäntöjä (esim. Mutual / 2-way TLS 1.2 tai uudempi). | LoA 2.4.6, kohta 2<br>M72B, alakohta 5.3.g<br>M72B, alakohta 7.1.1, alakohtat 1–4                                                                |                                                                                |

|      |  |                                                                                                                                                                                                                                                                                                                                                                             |                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 460. |  | Jos sovelluksen/lompakon ja palvelimen välillä vaihdetaan henkilötietoa, suojataan nämä tiedot myös sanomatason salauksella.                                                                                                                                                                                                                                                | LoA 2.4.6, kohta 2<br>LoA 2.4.6, korotettu<br>M72B, alakohta 5.3.g |                                                                                                                                                                                                                                                                                                                                                                                                           |
| 461. |  | Jos sovellus/lompakko perustuu kertakäyttösalasanoihin perustuvalla menetelmällä tai sisältää sellaisen, tulee kertakäyttösalasanana (OTP) luonnissa käyttää hyväksi havaittuja ja standardeihin perustuvia ratkaisuja.                                                                                                                                                     | M72B, alakohta 5.3.g                                               |                                                                                                                                                                                                                                                                                                                                                                                                           |
| 462. |  | Tunnistukseen käytetyn salaisuuden tallennukseen käytetään mahdollisuuksien mukaan alustan tarjoamia palveluita laitteistopohjaisessa turvallisessa ympäristössä.                                                                                                                                                                                                           | M72B, alakohta 5.3.c<br>M72B, alakohta 5.4.b                       | Turvaelementti (SE, secure element), luotettu ajoympäristö (TEE, trusted execution environment) jne.<br><br>Sovelluksen/lompakon tulee perustua riskiarvioon. Jos riskiarvio osoittaa, että turvaelementtiä ei tarvitse käyttää, voidaan salaisuuden/salaisuuksien tallentamiseen käyttää myös muita ratkaisuja. Poikkeaman perusteet on toimitettava arviointiraportin yhteydessä (osana riskiarvioita). |
| 463. |  | Tieto virheellisestä syötteestä lähetetään jokaisen keran jälkeen palvelimelle. Palvelin seuraa virheellisten syötteiden määrää ja sovellus lukittuu automaattisesti X virheellisen syötteen jälkeen. Jos verkkoyhteyttä ei ole, eikä viestejä saada lähetettyä palvelimelle turvallisesti, sovellus/lompakko itse noudattaa samaa logiikkaa (PSD2, viiden virheen sääntö). | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.3.f                         | vrt. RTS ja SCA                                                                                                                                                                                                                                                                                                                                                                                           |
| 464. |  | Sovelluksen/lompakon ja palvelimen välillä käytetään tekniikoita, joilla pystytään estämään replay-hyökkäykset ja nonce:n tapauksessa: Bounded Probability of a Birthday Collision.                                                                                                                                                                                         | LoA 2.3.1, korotettu, kohta 2<br>LoA 2.3.1, korkea                 |                                                                                                                                                                                                                                                                                                                                                                                                           |
| 465. |  | Jos käytössä on istuntotunnisteet, käytetään satunnaisia istuntotunnisteita.                                                                                                                                                                                                                                                                                                | LoA 2.3.1, korotettu, kohta 2<br>LoA 2.3.1, korkea                 |                                                                                                                                                                                                                                                                                                                                                                                                           |
| 466. |  | (Ohjelmisto/OAuth) Token-pohjaisen teknologian ratkaisussa varmistetaan, että token on allekirjoitettu hyväksyttävällä ja turvallisella algoritmilla.                                                                                                                                                                                                                       | LoA 2.4.6, kohta 2<br>M72B, alakohta 7.1.1, alakohta 2             |                                                                                                                                                                                                                                                                                                                                                                                                           |
| 467. |  | Istunnon tai tokenin voimassaoloaika määritellään palvelinpäässä.                                                                                                                                                                                                                                                                                                           | LoA 2.4.6, kohta 1 ja 4                                            |                                                                                                                                                                                                                                                                                                                                                                                                           |
| 468. |  | Valtuutuspolitiikat, joiden perusteella myönnetään pääsy kohdesovellukseen/palveluun, määritellään (tunnistus)palvelinpäässä.                                                                                                                                                                                                                                               | LoA 2.4.6, kohta 1 ja 4                                            |                                                                                                                                                                                                                                                                                                                                                                                                           |

|      |  |                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                          |
|------|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 469. |  | Jos alustan ominaisuuksien takia todentamistekijän toteutuksessa ei pystytä erottelemaan päätelaitteeseen rekisteröityneitä henkilöitä, on käytettävä yhdistelmää, jotta käyttäjä pystytään yksilöimään luotettavasti (Esim. päätelaite = hallinta, salaisuuteen liittyvä PIN-koodi = tieto ja sormenjälki = ominaisuus).                                       | LoA 2.2.1, korotettu, kohta 1                                                                  | Esim. Apple iOS, biometria<br>Vahvaan tunnistusmenetelmään ei tarvita kaikkia kolmea tekijää, vaan kaksi riittää, jos pystytään todentamaan, että tekijät ovat toisistaan riippumattomia ja ne on kytketty tunnistusvälineen haltijaan.                                                                                                                                                  |
| 470. |  | Jos biometrasta todentamistekijää käytetään ja alustan ominaisuuksien takia rekisteröityneitä henkilöitä ei pystytä erottelemaan, on käyttäjää selkeästi ohjeistettava poistamaan muiden henkilöiden biometriset tunnisteet/salaisuudet, jotka kuuluvat muille laitteen käyttäjille                                                                             | LoA 2.2.1, korotettu, kohta 1<br>LoA 2.1.1, kohta 2<br>LoA 1 (määritelmät), kohta 2            | LoA 2.1.1. Ei kuulu tunnistuslain piiriin, hyväksi havaittu käytäntö                                                                                                                                                                                                                                                                                                                     |
| 471. |  | Jos sovelluksessa/lompakossa sallitaan uusien, täydentävien todentamistekijöiden määrittäminen tai todentamistekijän vaihtaminen, kommunikoidaan tämä tieto myös palvelinpäähän. Vaihtaminen ja lisääminen vaativat aina tunnistuksen vähintään samalla tasolla kuin uusi yhdistelmä mahdollistaisi. Yhdistelmät tulee dokumentoida ja arvioida ominaisuuksina. | LoA 1 (määritelmät), kohta 2<br>LoA 2.2.1, korotettu, kohta 2<br>LoA 2.2.4, korotettu          | Todentamistekijöiden riippumattomuus on varmistettava. Tarkoittaa esim. yhden todentamistekijän kategorian vaihtoa, tai uuden lisäämistä, jolloin käytössä olisi todentamistekijöitä kolmesta kategoriasta.<br>Tarkoitus on tarjota käyttäjälle mahdollisuus valita todentamistekijöitä, mutta varmistaa samalla, että tunnistuspalvelu voi koko ajan huolehtia niiden turvallisuudesta. |
| 472. |  | Useamman tekijän tunnistuksessa (multi-factor, strong authentication) käytetään käyttäjän tietoon (salasana, PIN-koodi) tai ominaisuuteen (sormenjälki, kasvot, iiris) perustuvaa tekijää avaamaan salaisuus, jolla itse tunnistuspyyntöön vastataan.                                                                                                           | LoA 1 (määritelmät), kohta 3<br>LoA 2.2.1, korotettu, kohta 2<br>LoA 2.3.1, korotettu, kohta 2 |                                                                                                                                                                                                                                                                                                                                                                                          |
| 473. |  | Biometrisen todentamistekijän toteutuksessa käytetään ainoastaan alustan tarjoamia rajapintoja.                                                                                                                                                                                                                                                                 | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.3.c                                                     | Eryityskäyttötapaus: Passin/henkilökortin sirun lukeminen NFC:n yli. Tässäkin tapauksessa tulee käyttää alustan tarjoamia rajapintoja.                                                                                                                                                                                                                                                   |
| 474. |  | Biometrasta tekijää hyödynnettäessä itse biometrasta tallennetta (sormenjälki, kasvokuva, iirisskannaus jne.) ei siirretä tunnistustapahtumassa sovelluksen/lompakon ulkopuolelle.                                                                                                                                                                              | LoA 2.2.1, korotettu, kohta 2<br>LoA 2.3.1, korotettu, kohta 2                                 |                                                                                                                                                                                                                                                                                                                                                                                          |
| 475. |  | Rekisteröintivaiheessa käytettävää arkaluonteista tai henkilöllisyyden määrittämistä koskevaa tietoa voidaan                                                                                                                                                                                                                                                    | LoA 2.4.6, kohta 2                                                                             |                                                                                                                                                                                                                                                                                                                                                                                          |

|      |  |                                                                                                                                                                                                                    |                                                     |                                                                                                                                                                                                                                                                                                                                                   |
|------|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |  | siirtää palvelinpäähän arvioitavaksi ainoastaan käyttäen turvallisia keinoja.                                                                                                                                      |                                                     |                                                                                                                                                                                                                                                                                                                                                   |
| 476. |  | Käyttäjällä tulee olla mahdollisuus väliaikaisesti sulkea salaisuus a) yhdestä laitteesta b) useammasta laitteesta c) kaikista laitteista kerralla.                                                                | LoA 2.2.3, korotettu, kohta 1                       |                                                                                                                                                                                                                                                                                                                                                   |
| 477. |  | Väliaikaisesti suljetun salaisuuden avaamiseksi vaaditaan aina tunnistus vähintään samalla tasolla kuin sovelluksen/lompakon käyttöönotossa.                                                                       | LoA 2.2.3, korotettu, kohta 3                       |                                                                                                                                                                                                                                                                                                                                                   |
| 478. |  | Käyttäjällä tulee olla mahdollisuus turvallisesti poistaa käytöstä tunnistussovellus ja salaisuus a) yhdestä laitteesta b) useammasta laitteesta c) kaikista laitteista.                                           | LoA 2.2.3, korotettu, kohta 1 ja 2                  |                                                                                                                                                                                                                                                                                                                                                   |
| 479. |  | Laitekohtainen salaisuuden väliaikainen sulkeminen ja salaisuuden poistaminen tulee olla myös mahdollista palvelinpäässä.                                                                                          | LoA 2.2.3, korotettu, kohta 1 ja 2                  |                                                                                                                                                                                                                                                                                                                                                   |
| 480. |  | Tunnistus sidotaan haluttuun tapahtumaan tai selainistuntoon, eli tunnistussovelluksessa näytetään selkeästi tieto, mitä ollaan tekemässä.                                                                         | LoA 2.3.1, korotettu, kohta 2                       | Esim. RTS, dynaaminen yhdistäminen. EU 2018/389.<br><br>PSD2-sääntelyssä asetetaan yksityiskoh-<br>taisempia vaatimuksia dynaamiselle yh-<br>distämiselle. Niitä vaatimuksia on nou-<br>datettava, kun tunnistussovellusta halu-<br>taan käyttää sekä yleiskäyttöiseen tun-<br>nistautumiseen että maksamiseen liitty-<br>vään tunnistautumiseen. |
| 481. |  | Tunnistussovellus/lompakko toteuttaa myös ns. binding messagen, jossa käyttäjälle muodostuu mahdolli-<br>suus ymmärrettävästi yhdistää mobiililaitteessa tapah-<br>tuva tunnistus esim. selainistuntoon.           | LoA 2.3.1, korotettu, kohta 2, M72B, alakohta 6.2.1 | Käytetään kieltä, joka auttaa käyttäjää ymmärtämään, mikä istuntoa koskeva viesti on.                                                                                                                                                                                                                                                             |
| 482. |  | Tunnistussovellus/lompakko näyttää aina sen palve-<br>lun/sovelluksen nimen, johon käyttäjä tunnistautuu attribuutilla sp_name. Tämän tiedon on oltava näky-<br>villä käyttäjän helposti ymmärrettävässä muodossa. | M72B, alakohta 6.2.2                                | Kielen on oltava selkeää, jotta sitä ei se-<br>koiteta istuntoa koskevaan viestiin.                                                                                                                                                                                                                                                               |
| 483. |  | Jos tunnistussovelluksen/lompakon vaste perustuu epäsymmetriseen allekirjoitukseen, käytössä on WYSIWYS-periaate, eli käyttäjälle näytetty tieto on sa-<br>malla myös allekirjoitettava tieto.                     | LoA 2.3.1, korotettu, kohta 2                       |                                                                                                                                                                                                                                                                                                                                                   |
| 484. |  | Sovellus/lompakko ohjaa käyttäjää valitsemaan vah-<br>voja PIN-koodeja.                                                                                                                                            | LoA 2.1.1, korotettu, kohta 2 M72B, alakohta 5.3.g  | LoA 2.1.1 ei kuulu tunnistuslain piiriin, hyväksi havaittu käytäntö                                                                                                                                                                                                                                                                               |

|      |  |                                                                                                                                                                                                                                                                                                                                                             |                                                          |                                                                                                                            |
|------|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| 485. |  | Sovellus/lompakko ei hyväksy PIN-koodeja tai muita käyttäjän muistiin perustuvia salaisuuksia, jotka on helppo arvata.                                                                                                                                                                                                                                      | LoA 2.3.1, korotettu, kohta 2<br>LoA 2.4.6, kohta 1      | Esim. yleisesti heikoiksi tiedettyjä/helposti arvattavia PIN-koodeja ei hyväksytä, kuten 000000, 123456, 999999 jne.       |
| 486. |  | Käyttäjän syötteet, esim. PIN-koodit, validoidaan turvallisesti.                                                                                                                                                                                                                                                                                            | LoA 2.3.1, korotettu, kohta 2<br>M72B, alakohta 5.4.b    |                                                                                                                            |
| 487. |  | Jos sovellus/lompakko käyttää päätelaitteen laitteistotason turvaominaisuuksia, kuten TEE/SE:tä tai vastaavaa, ilmoittaa sovellus käytetyn laitteistotason komponentin ja muut mahdolliset tiedot (tarjoajan) palvelimelle alustuksen yhteydessä, jotta palvelin pystyy havaitsemaan laitteistotason haavoittuvuuksia ja vastaamaan niihin (myös jatkossa). | LoA 2.4.6, kohta 1 ja 4<br>M72B, alakohta 5.4.d          | CVE-2018-11976 → Annetaan palvelimelle mahdollisuus reagoida tunnettuihin laitteistotason komponenttien haavoittuvuuksiin. |
| 488. |  | Jos taustajärjestelmä tai luottava osapuoli havaitsee epäaidon sovelluksen/lompakon, tunnistuksen eteneminen pysäytetään. Eli sovelluksen/lompakon varmenuksen on tapahduttava itse sovelluksessa, ja varmenus on validoitava tarpeen mukaan ennen tunnistuspyynnön etenemistä.                                                                             | LoA 2.4.6, kohta 1 ja 3<br>LoA 2.3.1, korotettu, kohta 1 | HUOMAUTUS: lisätty 19.05.2023.                                                                                             |
| 489. |  | Sovellus/lompakko ja/tai taustajärjestelmä varmistaa, että kerralla ei voi olla useampia aktiivisia tunnistuspyyntöjä, eli edellisten pyyntöjen on oltava hylätyjä/suljettuja ennen uuden pyynnön käynnistämistä.                                                                                                                                           | LoA 2.3.1, korotettu, kohta 2                            |                                                                                                                            |

## C 5 Tietoliikenne

| NRO  | VAR-<br>MUUS-<br>TASO | KRITEERI                                                                                                                                                                                                              | PERUSTE                                                  | Lisätieto / kommentti                                                                                                                                                                                       |
|------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 490. |                       | Sovelluksen/lompakon ja palvelimen välinen verkkoliikenne on suojattu kansainvälisesti tai kansallisesti suositelluilla yhteyskäytännöllä ja suojatut kanavat ovat yhdenmukaisesti käytössä sovelluksessa/lompakossa. | LoA 2.4.6, kohta 2<br>M72B, alakohta 5.3.g               | Tunnistusjärjestelmän <i>sisäisille</i> yhteyksille ei ole määrätty salausvaatimuksia, mutta lähtökohtana voidaan pitää M72B 7 kohdan mukaisia <i>toimijoiden välisiä</i> tietoliikenteen salauskäytäntöjä. |
| 491. |                       | Sovellus/lompakko tarkistaa TLS-salausmenetelmän (tai vastaavan) asetukset/konfiguraation ja varmistaa, että ne noudattavat hyväksi havaittuja käytäntöjä.                                                            | LoA 2.4.6, kohta 2<br>M72B, alakohta 5.3.g, 7.1.3 ja 7.2 | Tunnistusjärjestelmän <i>sisäisille</i> yhteyksille ei ole määrätty salausvaatimuksia, mutta lähtökohtana voidaan pitää M72B 7 kohdan mukaisia <i>toimijoiden välisiä</i> tietoliikenteen salauskäytäntöjä. |

|      |  |                                                                                                                                                                                                                                                      |                                                               |                                                                                              |
|------|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| 492. |  | Sovellus/lompakko lukitsee päätepisteen sertifikaatin tai julkisen avaimen, eikä muodosta yhteyttä päätepi-<br>teisiin, joilla on eri sertifikaatti tai avain, vaikka se olisi<br>luotetun varmentajan (Certificate Authority) allekirjoit-<br>tama. | LoA 2.4.6, kohta 2                                            |                                                                                              |
| 493. |  | Kriittisissä toiminnoissa, kuten alustuksessa ja käyttä-<br>jän salaisuuden luomisessa, sovellus/lompakko ei luota<br>turvattomiin kommunikointikanaviin (esim. sähköposti,<br>tekstiviesti).                                                        | LoA 1 (määritelmät), kohta 2<br>LoA 2.2.1, korotettu, kohta 2 | Käytännössä sovelluksen personoinnin<br>on perustuttava vahvaan sähköiseen<br>tunnistukseen. |
| 494. |  | Sovellus/lompakko käyttää vain ajantasaisia ohjelmis-<br>tokirjastoja yhteyksien ja tietoturvan toteuttamisessa.                                                                                                                                     | LoA 2.4.6, kohta 1 ja 4                                       |                                                                                              |

## C 6 Alustan ja sovelluksen yhteistyö

| NRO  | VAR-<br>MUUS-<br>TASO | KRITEERI                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | PERUSTE                                           | Lisätieto / kommentti |
|------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|-----------------------|
| 495. |                       | Sovellus/lompakko pyytää päätelaitteelta vain tarvitse-<br>mansa oikeudet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.3.c        |                       |
| 496. |                       | Kaikki ulkopuolisista lähteistä tuleva tieto tarkistetaan<br>ja sanitoidaan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | LoA 2.4.6, kohta 4<br>M72B, alakohta 5.3.c        |                       |
| 497. |                       | Omaa URL-skeemaa tai IPC-mekanismia käytettäessä<br>ei tietoja viedä sovelluksen/lompakon ulkopuolelle.                                                                                                                                                                                                                                                                                                                                                                                                                                                              | LoA 2.4.6, kohta 2<br>M72B, alakohta 5.3.c        |                       |
| 498. |                       | Jos sovelluksessa/lompakossa on tarpeellista näyttää<br>selaimen kautta saatavilla olevaa tietoa (esim. tunnis-<br>tuspalvelimen menetelmien valintaikkuna), käytetään<br>tähän tarkoitukseen ensisijaisesti käyttöjärjestelmän<br>turvallisia ominaisuuksia (katso käyttöjärjestelmän tar-<br>joajan kulloisetkin parhaat käytännöt). WebView:tä<br>käytetään vain, jos muuta turvallisempaa vaihtoehtoa<br>ei ole. Käytetyissä komponenteissa käytetään vain tar-<br>peellisia yhteyskäytäntöjä ja muut suljetaan / varmis-<br>tetaan, että ne eivät ole käytössä. | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.3.c        |                       |
| 499. |                       | JavaScript on oletusarvoisesti deaktivoitu käytetyissä<br>selainkomponenteissa                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.3.c        |                       |
| 500. |                       | Jos käytössä on selaintoiminnon toteuttavia kom-<br>ponentteja, niiden konfiguraatio sallii vain https-yhtey-<br>den.                                                                                                                                                                                                                                                                                                                                                                                                                                                | LoA 2.4.6, kohta 1<br>M72B, alakohta 7.1–2 ja 9.3 |                       |

|      |  |                                                                                                                                                                                     |                                                                   |                                                                                                                                                                                                                                                                                              |
|------|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 501. |  | Natiivimetodit on estetty, jos alustan ohjelmistoversio on todettu haavoittuvaksi.                                                                                                  | LoA 2.4.6, kohta 1 M72B, alakohta 5.3.) ja 5.4.d                  | Esim. vanhemman Android-käyttöjärjestelmäversion toteutus JavaScriptin kohdalla voi olla turvaton                                                                                                                                                                                            |
| 502. |  | Jos sovelluksen/lompakon natiivimetodit ovat avoimia selaintoiminnallisuuden toteuttaville komponenteille, varmistetaan, että ajetaan vain sovelluspakettiin kuuluvaa JavaScriptiä. | LoA 2.4.6, kohta 1 M72B, alakohta 5.3.c                           |                                                                                                                                                                                                                                                                                              |
| 503. |  | Selaintoiminnon toteuttavilta komponenteilta on pääsy kielletty / estetty paikallisiin resursseihin.                                                                                | LoA 2.4.6, kohta 1 M72B, alakohta 5.3.c)                          |                                                                                                                                                                                                                                                                                              |
| 504. |  | Käytössä on turvalliset API:t, jos käytetään objektien serialisointia.                                                                                                              | LoA 2.4.6, kohta 1 ja 3 LoA 2.4.6, korotettu M72B, alakohta 5.3.c |                                                                                                                                                                                                                                                                                              |
| 505. |  | Sovellus/lompakko suojaa itseään näytön peittokuvaan perustuvilta hyökkäyksiltä (overlay attack).                                                                                   | LoA 2.4.6, kohta 1                                                | Overlay-tyyppisten hyökkäysten riskienhallintakeinot riippuvat käytetystä alustasta ja sen tarjoamista ominaisuuksista. Esim. Android API-versio 9 lähtien voidaan tätä riskiä jo osittain hallita. Sovellus/lompakko käyttää alustan tarjoamia turvakontrolleja täysimääräisesti hyväkseen. |
| 506. |  | Selainkomponentin välimuisti, tietovarasto ja ladatut resurssit poistetaan ennen selainkomponentin tuhoamista.                                                                      | LoA 2.4.6, kohta 1 ja 3 M72B, alakohta 5.4.b                      |                                                                                                                                                                                                                                                                                              |
| 507. |  | Varmistetaan, että sovellus/lompakko estää kolmannen osapuolen näppäimistöjen käytön arkaluonteisten tietojen syötössä.                                                             | LoA 2.4.6, kohta 1–2                                              | Poikkeuksena esim. ne käyttötapaukset, joissa kolmannen osapuolen näppäimistön käyttäminen on edellytys tunnistussovelluksen käytölle. Nämä tulee erikseen tunnistaa ja dokumentoida.                                                                                                        |

## C 7 Ohjelmistokoodin turvallisuus, laatu ja kehitysympäristö

| NRO  | VAR-<br>MUUS-<br>TASO | KRITEERI                                                                                                                                           | PERUSTE            | Lisätieto / kommentti |
|------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-----------------------|
| 508. |                       | Sovellus/lompakko on allekirjoitettu ja provisioitu voimassa olevalla ja luotetulla varmenteella, ja yksityinen avain on asianmukaisesti suojattu. | LoA 2.4.6, kohta 1 |                       |

|      |  |                                                                                                                                                                |                                                          |                                                                                                           |
|------|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| 509. |  | Sovellus/lompakko on luotu release mode -tilassa, eli esim. tilassa, jossa virheenkorjaus on tehty vaikeamaksi.                                                | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.3.c               |                                                                                                           |
| 510. |  | Sovelluksen/lompakon kehityksessä käytetään vain hyväksi havaittuja ohjelmistokehityksen/koodauksen tietoturvakäytäntöjä.                                      | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.3.c               | Esimerkiksi kaikki käytettävä Javascript tulee enkoodata ja sanitoida XSS-hyökkäysriskin pienentämiseksi. |
| 511. |  | Virheenkorjaussymbolit on poistettu binääreistä                                                                                                                | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.3.c               |                                                                                                           |
| 512. |  | Virheenkorjauskoodi ja -viestit on poistettu.                                                                                                                  | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.3                 |                                                                                                           |
| 513. |  | Testaus- tai kehitysaikaiset asetukset, lokien kerääminen (verbose logging) ja konfiguraatiot on poistettu julkaisuversiosta.                                  | LoA 2.4.6, kohta 1 ja 4<br>M72B, alakohta 5.3.c ja 5.4.d |                                                                                                           |
| 514. |  | Kaikki sovelluksen/lompakon käyttämät kolmannen osapuolen komponentit on tunnistettu, ja ne tarkistetaan säännöllisesti tunnettujen haavoittuvuuksien varalta. | LoA 2.4.6, kohta 4<br>M72B, alakohta 5.4.d               |                                                                                                           |
| 515. |  | Sovellus/lompakko huomaa poikkeukset ja käsittelee ne asianmukaisesti.                                                                                         | LoA 2.4.6, kohta 4<br>M72B, alakohta 5.3.f ja 5.4.d      |                                                                                                           |
| 516. |  | Sovellus/lompakko tai palvelin minimoi virheviestien sisältämän tiedon.                                                                                        | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.3.c               |                                                                                                           |
| 517. |  | Turvakontrollien virheenkäsittely oletusarvoisesti epäpääsyn virhetilanteessa.                                                                                 | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.3.c               |                                                                                                           |
| 518. |  | Muistia varataan, vapautetaan ja käytetään turvallisesti.                                                                                                      | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.3.c               |                                                                                                           |
| 519. |  | Alustan / kehitysympäristön tarjoamat tietoturvaominaisuudet ovat käytössä.                                                                                    | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.3.c               |                                                                                                           |

## C 8 Turvakontrollit ja suojautuminen (EN: Resilience)

| NRO  | VAR-MUUS-TASO | KRITEERI                                                                                                            | PERUSTE                                    | Lisätieto / kommentti                                                 |
|------|---------------|---------------------------------------------------------------------------------------------------------------------|--------------------------------------------|-----------------------------------------------------------------------|
| 520. |               | Sovellus/lompakko käyttää useampaa tässä kappaleessa esitettyä puolustusmekanismia.                                 | LoA 2.4.6, kohta 1                         | Ohjelmiston kykyä vastustaa hyökkäyksiä on arvioitava kokonaisuutena. |
| 521. |               | Sovelluksessa/lompakossa on useampi kuin yksi toiminto, joka pyrkii huomaamaan rootatun tai jailbreakatun laitteen. | LoA 2.4.6, kohta 4<br>M72B, alakohta 5.3.f |                                                                       |

|      |  |                                                                                                                                                                                                                                        |                                                                                  |  |
|------|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|--|
| 522. |  | Havaintomekanismit saavat aikaan erityyppisiä reaktioita, mm. viivästettyjä ja piilotettuja reaktioita.                                                                                                                                | LoA 2.4.6, kohta 4<br>M72B, alakohta 5.3.f ja 6.1                                |  |
| 523. |  | Sovellus/lompakko lähettää viestin palvelinpään toteutukselle huomautessaan ajoympäristöksi rootatun tai jailbreakatun laitealustan, tai sovellus itse voi päättää mitä tehdä huomautessaan ympäristön olevan rootattu/jailbreakattu.  | LoA 2.4.6, kohta 4<br>M72B, alakohta 5.3.f                                       |  |
| 524. |  | Sovellus/lompakko pyrkii estämään virheenkorjaukseen pyrkivät yritykset ja reagoi huomautessaan virheenkorjaukseen käytetyn ratkaisun liittyneen sovellukseen. Tämän on katettava kaikki käytettävissä olevat virheenkorjauskäytännöt. | LoA 2.4.6, kohta 1<br>M72B, alakohta 5.3.c                                       |  |
| 525. |  | Sovellus/lompakko huomaa ja reagoi, jos sovelluksen ajoympäristössä (sandbox) ajonaikaiset tiedostot tai kriittiset tiedot/tiedostot muuttuvat.                                                                                        | LoA 2.4.6, kohta 4<br>M72B, alakohta 5.3.f                                       |  |
| 526. |  | Sovellus/lompakko huomaa ja reagoi yleisesti käytettyihin työkaluihin, joilla pyritään selvittämään sovelluksen lähdekoodia (reverse engineering).                                                                                     | LoA 2.4.6, kohta 4<br>M72B, alakohta 5.3.f                                       |  |
| 527. |  | Sovellus/lompakko huomaa ja reagoi, jos sitä ajetaan emulaattorissa.                                                                                                                                                                   | LoA 2.4.6, kohta 4<br>M72B, alakohta 5.3.f                                       |  |
| 528. |  | Sovellus/lompakko tarkkailee muistiavaruuden koodin ja tiedon manipulointia ja reagoi siihen asianmukaisesti.                                                                                                                          | LoA 2.4.6, kohta 4<br>M72B, alakohta 5.3.f                                       |  |
| 529. |  | Sovellukselle/lompakolle tärkeät tai olennaiset osiot on soveltuvalta osin salattu tietojärjestelmätasolla. Analysoimalla ei saada selville sovellukselle/lompakolle tärkeitä tai olennaisia osioita.                                  | LoA 2.4.6, kohta 1 ja 3<br>LoA 2.4.6, korotettu<br>M72B, alakohta 5.3.c ja 5.4.b |  |
| 530. |  | Sovelletaan sovellustason hyötykuorman salausta.                                                                                                                                                                                       | LoA 2.4.6, kohta 1–4<br>M72B, alakohta 5.3.g                                     |  |

## Viitteet

Kriteerit, joille tämä ohje perustuu:

TunnL – Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009)

LoA – Komission täytäntöönpanoasetus (EU) 2015/1502 teknisten vähimmäiseritelmien ja -menettelyjen vahvistamisesta sähköisen tunnistamisen menetelmien varmuustasoja varten sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 8 artiklan 3 kohdan mukaisesti

M72B – Määräys sähköisistä tunnistus- ja luottamuspalveluista (M72B/2022) <https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen>

OWASP - OWASP Mobile Application Security Verification Standard, MASVS versio 1.4.2