**Sähköisen tunnistuspalvelun arviointiohje**

**211/2023 O**

Liikenne- ja viestintäviraston ohje

[Luonnos kappaleisiin 1-4]

1.6.2023

Sisältö

1 Johdanto 5

1.1 Ohjeen tarkoitus 5

1.2 Ohjeen voimaantulo 6

1.3 Säädös- ja standardiviittaukset ja lyhenteet 7

1.4 Tunnistuspalvelun määritelmät 8

1.5 Palvelun tarjoajan yleinen luotettavuus ei sisälly kriteeristöön 9

2 Tunnistuspalvelun arviointi ja tarkastuskertomus 10

2.1 Tarkastuskertomuksen toimittaminen ilmoituksen liitteenä 10

2.1.1 Aloitusilmoitus 11

2.1.2 Muutosilmoitus 11

2.1.3 Määräaikaisarviointi 12

2.2 Tunnistuspalvelun arvioitavat osa-alueet 12

2.3 Tunnistusmenetelmä, tunnistusjärjestelmä ja alihankkijat 14

2.3.1 Määritelmät 14

2.3.2 Arviointi ja alihankkijat 15

2.3.3 Tarkastuskertomus: Kuvaus siitä, minkä osan tunnistusmenetelmästä ja/tai tunnistusjärjestelmästä arviointi kattaa 17

2.3.4 Tarkastuskertomus: Arvioitavan tunnistuspalvelun nimi/nimet 17

2.3.5 Tarkastuskertomus: Tunnistusmenetelmän (tunnistusvälineen) kuvaus 17

2.3.6 Tarkastuskertomus: Tunnistusjärjestelmän kuvaus (järjestelmäarkkitehtuuri) 18

2.4 Tiedot arviointielimestä 19

2.4.1 Tarkastuskertomus: Arviointielimen yksilöinti- ja yhteystiedot 19

2.4.2 Tarkastuskertomus tai ilmoitus: Arviointielimen pätevyys ja riippumattomuus 20

2.5 Arvioinnin toteuttaminen 21

2.5.1 Tarkastuskertomus: Arvioinnin ajankohta ja kesto henkilötyöaikana 21

2.5.2 Tarkastuskertomus: Arviointimenetelmät 21

2.5.3 Tiedot dokumentaatiosta, jota on käytetty vaatimuksenmukaisuuden arvioinnissa 22

2.6 Arvioinnin suhteuttaminen varmuustasoon ja riskeihin 22

2.7 Tarkastuskertomuksen tarkkuus 25

2.8 Poikkeamien raportointi tarkastuskertomuksessa 25

3 Arvioitavat osa-alueet 26

3.1 Tunnistamisen menetelmän ominaispiirteet ja todentamismekanismi 26

3.2 Yhteentoimivuus 27

3.3 Tekniset tietoturvavaatimukset 27

3.4 Poikkeamien havainnointikyky ja hallinta ja häiriöilmoitukset 28

3.5 Tietojen säilyttäminen ja käsittely 29

3.6 Tilaturvallisuus 30

3.7 Riittävät ja pätevät henkilöresurssit 30

3.8 Tietoturvallisuuden hallinta 31

3.9 Tunnistusvälineen hakijan henkilöllisyyden todistaminen ja varmentaminen (ensitunnistaminen) 31

3.10 Huomioita henkilöllisyystodistuksen perusteella ensitunnistamisesta etäyhteydellä 32

3.11 Tunnistusvälineen eli tunnistusmenetelmän elinkaari 34

4 LIITE A: Tarkastuskertomusohjeen muistilista 36

5 LIITE B: Tunnistuspalvelun yleinen arviointikriteeristö 37

5.1 Tunnistamisen menetelmän ominaispiirteet ja todentamismekanismi 37

5.2 Yhteentoimivuus 48

5.3 Tekniset tietoturvavaatimukset 53

5.3.1 Tietoliikenneturvallisuus 54

5.3.2 Tietojärjestelmäturvallisuus 60

5.3.3 Käyttöturvallisuus 66

5.4 Poikkeamien havainnointikyky ja hallinta ja häiriöilmoitukset 70

5.5 Tietojen säilyttäminen ja käsittely 77

5.6 Tilaturvallisuus 84

5.7 Riittävät ja pätevät henkilöresurssit 85

5.8 Tietoturvallisuuden hallinta 87

5.9 Tunnistusvälineen hakijan henkilöllisyyden todistaminen ja varmentaminen (ensitunnistaminen) 91

5.10 Tunnistusvälineen eli tunnistusmenetelmän elinkaari 98

6 LIITE C Mobiilitunnistusratkaisun erityiskriteeristö 104

6.1 Arkkitehtuuri, suunnittelu ja uhkakuvien mallintaminen 104

6.2 Tietojen tallennus ja tietosuoja 105

6.3 Salausvaatimukset 107

6.4 Tunnistaminen, tunnistusmenetelmän ominaispiirteet ja istunnonhallinta 108

6.5 Tietoliikenne 112

6.6 Alustan ja sovelluksen yhteistyö 113

6.7 Ohjelmistokoodin turvallisuus, laatu ja kehitysympäristö 114

6.8 Turvakontrollit ja suojautuminen (EN: Resilience) 115

# 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.

## Ohjeen tarkoitus

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

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 säädetyt 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[[1]](#footnote-1) 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)[[2]](#footnote-2).

## Ohjeen voimaantulo

Ohje 211/2023 O tulee voimaan x.xx.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> ~~ja~~ [~~https://www.traficom.fi/fi/saadokset~~](https://www.traficom.fi/fi/saadokset)

|  |  |  |  |
| --- | --- | --- | --- |
| Versio | Päiväys | Kuvaus/muutos | Tekijä |
| 211/2023 O | xx.xx.2023 |  | Liikenne- ja viestintävirasto,  Kyberturvallisuuskeskus |
| 211/2019 O | 9.10.2019 | 2. julkaistu yhdistetty versio   * muutettu yleinen kriteeristö karsimalla kriteerejä ja listaamalla ne säädettyjen vaatimusten pohjalta * lisätty kokonaan uusi erityiskriteeristö sähköisessä tunnistamisessa käytettäville mobiilisovelluksille * yhdistetty päivitettynä tunnistuspalvelun tarkastuskertomusta koskeva osa ohjeesta 215/2016 O | Liikenne- ja viestintävirasto, Kyberturvallisuuskeskus |
| 211/2016 O Tunnistuspalvelun auditoinnin mallikriteeristö  215/2016 O Tunnistus- ja luottamuspalveluiden arviointikertomukset | 2.11.2016 | 1. julkaistut versiot | Viestintävirasto, Kyberturvallisuuskeskus |

## 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 viitatut kohdat varmuustasoasetuksesta
  + LoA-guidance, varmuustasoasetuksen epävirallinen soveltamisohje[[3]](#footnote-3)
* Liikenne- ja viestintäviraston määräys M72B/2022 (jäljempänä *M72B*)[[4]](#footnote-4)
  + Määräyksellä tarkennetaan eräitä tunnistuslaissa säädettyjä vaatimuksia

Standardiviittaukset[[5]](#footnote-5):

* ISO/IEC 27001:2013/2017 Information security management
  + 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[[6]](#footnote-6)

Varmuustason lyhenteet taulukoissa

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

## 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.

***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 tunnistusvälinettään 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;

## Palveluntarjoajan yleinen luotettavuus ei sisälly kriteeristöön

Riippumattoman arvioinnin ei tarvitse kattaa palveluntarjoajan yleistä luotettavuutta tai käyttäjille ja luottaville osapuolille tarjottavia tietoja palvelusta (tunnistusperiaatteet, 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 muutosilmoitusten 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 tunnistusperiaatteet, tietosuojaperiaatteet, käyttörajoitukset, sopimusehdot ja hinnastot;**

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

**4) vastuu alihankkijoista; sekä**

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

# Tunnistuspalvelun arviointi ja tarkastuskertomus

## Tarkastuskertomuksen toimittaminen ilmoituksen liitteenä

***SÄÄNNÖKSET***

***TunnL 10 § Tunnistuspalvelun tarjoajan velvollisuus ilmoittaa toiminnan aloittamisesta***

*Suomeen sijoittautuneen tunnistuspalvelun tarjoajan on ennen toimintansa aloittamista tehtävä 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 sisäisen tarkastuslaitoksen laatima tarkastuskertomus riippumattomasta arvioinnista 29 §:n mukaisesti;*

*[…]*

*Tunnistuspalvelun tarjoajan on viipymättä ilmoitettava 2 momentissa tarkoitetuissa tiedoissa tapahtuneista muutoksista kirjallisesti Liikenne- ja viestintävirastolle. Ilmoitus on tehtävä myös toiminnan lopettamisesta sekä toimintojen siirtymisestä toiselle palveluntarjoajalle.*

***TunnL 11 § Muuhun Euroopan talousalueen jäsenvaltioon sijoittautunut tunnistuspalvelun tarjoaja***

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

***TunnL 31 § Tarkastuskertomus***

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

*Tarkastuskertomus on voimassa arvioinnissa käytetyn standardin määrittelemän ajan, kuitenkin enintään 2 vuotta.*

### Aloitusilmoitus

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

### Muutosilmoitus

Tunnistuspalvelua koskeva tarkastuskertomus toimitetaan Liikenne- ja viestintävirastolle ilmoituksen liitteenä, kun ilmoitetaan olennaisesta muutoksesta tunnistusjärjestelmässä.

Toiminnan olennaisissa muutostilanteissa täytyy tehdä arviointi ja toimittaa muutosta koskeva muutosilmoitus sekä tarkastuskertomus ennen muutoksen tuotantoon 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.

### 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 määrittelemin 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.

## 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 tunnistuspalveluntarjoaja 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 palvelulleen 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):*
2. *tietoturvallisuuden hallintaan;*
3. *tietojen säilyttämiseen ja käsittelyyn;*
4. *tiloihin ja henkilökuntaan;*
5. *teknisiin toimenpiteisiin; ja*
6. *yhteentoimivuuteen luottamusverkostossa; sekä*
7. *tunnistusmenetelmään eli tunnistusvälineen:*
8. *hakemiseen ja rekisteröintiin;*
9. *hakijan henkilöllisyyden todistamiseen ja varmentamiseen;*
10. *tunnistusmenetelmän ominaispiirteisiin ja laatimiseen;*
11. *myöntämiseen, toimittamiseen ja aktivointiin;*
12. *voimassaolon keskeyttämiseen, peruuttamiseen ja uudelleen aktivointiin;*
13. *uusimiseen ja korvaamiseen; ja*
14. *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.*

## Tunnistusmenetelmä, tunnistusjärjestelmä ja alihankkijat

### 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 §***

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

### 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 tunnistustapahtumien 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 kertakäyttösalasana.
* 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 vääriin käsiin, jos puhelin on toisen hallussa fyysisesti tai tietoturvaloukkauksen takia. Miten on estetty se, että matkapuhelimeen ei tallennu esimerkiksi kopiota tai murrettavissa olevaa tiivistettä 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.

### 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 järjestelmistä on tarkastettu ne kaikki osat, joissa tunnistuspalvelua tuotetaan.

### 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.

### Tarkastuskertomus: Tunnistusmenetelmän (tunnistusvälineen) kuvaus

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

Kuvausten täytyy olla teknisesti niin tarkkoja, että niiden perusteella pystyy päättelemään, 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.

### 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 selvitä 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.

## 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.

### 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.

### 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 säädetyistä 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 tunnistusjärjestelmän arviointiin edellyttää sitä, että osoitetaan myös, miten ja miltä osin 18.1 kohdassa tarkoitetut säännökset, ohjeet tai standardit kohdistuvat tunnistusjärjestelmälle 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 tunnistusjärjestelmän arviointiin edellyttää sitä, että osoitetaan myös, miten ja miltä osin 19.1 kohdassa tarkoitettujen säännösten, ohjeiden tai standardien mukaisesti organisoitu sisäinen tarkastus kohdistuu tunnistusjärjestelmälle asetettuihin vaatimuksiin.*

## Arvioinnin toteuttaminen

### 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 vähimmäiskestoa. 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 tunnistusjärjestelmä, ja kaikki tässä ohjeessa luetellut osa-alueet, ja mukana tulee olla myös tekniset näytteenotot tai arvioinnit.

### 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.

### 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 salassapitosäännösten 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.

### 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.

## Arvioinnin suhteuttaminen varmuustasoon ja riskeihin

Vahvan sähköisen tunnistamisen luotettavuudelle on säädetty kaksi varmuustasoa, korotettu ja korkea.[[7]](#footnote-7) Arviointikriteerien taulukoissa käytettään 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 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 (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 olettamukset 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 tulevissa 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.

[…]

## Tarkastuskertomuksen tarkkuus

Tarkastuskertomuksesta tulee käydä ilmi, miten vaatimusten täyttyminen on arvioitu.

**Tarkastuskertomuksessa tulee olla sanallinen kuvaus siitä, minkä käytännön seikkojen ja havaintojen perusteella kunkin vaatimuksen täyttyminen 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.**

## 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 toimenpide-ehdotus 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.

## 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.

# 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.

## 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 tietoturvavaatimukset
* 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 todentamismekanismia ja menetelmän kykyä suojata varmuustason edellyttämällä tasolla tietoturvauhkilta 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.

## 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.

## Tekniset tietoturvavaatimukset

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 tietoturvavaatimukset

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 tietoturvauhkien 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
* Tietoliikenneyhteyksien vyöhykkeistäminen
* Tietoliikennelaitteet- ja järjestelmät
* Tuotanto-, ylläpito- ja hallinnointiverkkojen sekä kehitysympäristön eriyttäminen
* Suodatukset
* Yhteydet julkiseen verkkoon
* Tietojärjestelmien luokittelu
* Pääsyoikeudet ja käyttäjien tunnistus
* Vaaralliset työyhdistelmät
* Kovennukset
* Salausratkaisut
* Kryptografisen materiaalin turvallisuus
* Etätyöasemien erityiset vaatimukset
* Haittaohjelmat
* Muutostenhallinta
* Ohjelmistohaavoittuvuudet
* Varmuuskopiointi

## 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 tietoturvavaatimukset
* 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

## 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 tietoturvavaatimukset
* 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 jäljitettävyys ja palautettavuus
* tiedon elinkaaren hallinta mukaan lukien tiedon säilytysajat ja hävittäminen

## 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 ympäristötapahtumilta (palo, lämpö, kaasu, pöly, tärinä, vesi)
* Suojautuminen luvattomalta pääsyltä (murto)
* Sähkönsaannin katkokset
* Suojautuminen ilkivallalta
* Vyöhykkeistäminen
* Rakenteellinen suojaus
* Kulunvalvonta
* Turvallisuusjärjestelmien laatu
* Luvattomat laitteet ja yhteydet

## Riittävät ja pätevät henkilöresurssit

Vaatimukset säädetään seuraavissa säännöksissä

* TunnL 13 § Tunnistuspalvelun 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 tunnistuspalvelun 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

## 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 Tunnistuspalvelun tarjoajan tietoturvallisuuden hallintajärjestelmä
* LoA Liite, 1. Sovellettavat määritelmät  
  4. 'tietoturvallisuuden hallintajärjestelmällä' tarkoitetaan prosesseja ja menettelyjä, joiden tarkoituksena on pitää tietoturvallisuuteen 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

## 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

## 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
  + 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 käytettävissä 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
  + henkilöllisyystodistuksen aitoustekijöiden havainnointi ja
  + 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 kuvatietoon 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.
* Väestötietojärjestelmästä tulee hakea vertailutiedot, millä varmistetaan, että esitetty henkilöllisyystodistus on aito ja se on voimassa, ja henkilöllisyystodistusta esittävä henkilö on sen omistaja.
* Jos on mahdollisuus käyttää myös muun maan väestötietojärjestelmää ja rekisteriä, jossa on tiedot henkilöllisyystodistusten ja passien voimassaolosta, voidaan etätunnistus suorittaa myös niiden perusteella.
* 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 henkilöllistystodistuksen esittäjä on paikalla esittämishetkellä eikä kysymyksessä ole väärennetty tallenne. Esimerkiksi henkilö tekee pyydetyt sattumanvaraiset eleet reaaliaikaisesti. Elävyyden havainnointia varten tulee olla henkilöstölle riittävä koulutus ja kattavat ohjeet. Elävyyden havainnointi koneellisesti tulee perustua sattumanvaraisiin tapahtumiin tai pyyntöihin, jotka on kohdennettu etäensitunnista tekevälle 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 tarkoitetut sormenjäljet tarvittavine lisätietoineen siten kuin EU:n passiasetuksessa säädetään. Tekniseen osaan voidaan tallettaa myös 5 §:n 1 momentissa tarkoitetut tiedot. Passinhaltijan oikeudesta tarkastaa passin tekniseen osaan hänestä talletetut tiedot säädetään EU:n passiasetuksessa.   
    
  Passin turvatekijöistä ja biometrisistä tunnisteista säädetään EU:n passiasetuksessa. Biometrisen tunnisteen 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 biometristen tietojen sisällyttäminen henkilökortteihin […] ovat tärkeitä askelia tehtäessä niiden käytöstä unionissa turvallisempaa. Tällaisten **biometristen 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 tunniste**, 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 […] biometristen 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 luottaisiin, 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 tulkinnassaan 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 biometristen 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.

## 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 neuvontamuistion[[8]](#footnote-8), jossa käsitellään henkilöllisyyden todentamista ylläpitotilanteissa.

## 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.

# 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

1. Arvioinnin ajankohta ja kesto henkilötyöaikana (2.5.1)
2. Arviointimenetelmät (2.5.2)
3. Tiedot dokumentaatiosta, jota on käytetty arvioinnissa (2.5.3)
4. Kuvaus siitä, minkä osan tunnistusmenetelmästä ja/tai tunnistusjärjestelmästä arviointi kattaa (2.3.3)
5. Arvioitavan tunnistuspalvelun nimi/nimet (2.3.4)
6. Tunnistusmenetelmän (tunnistusvälineen) kuvaus (2.3.5)
7. Tunnistusjärjestelmän kuvaus (järjestelmäarkkitehtuuri) (2.3.6)
8. Poikkeamat (2.8-2.9)
9. Tulokset osa-alueiden arvioinnista (3.1-3.12 soveltuvin osin)

1. Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014 sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta. [↑](#footnote-ref-1)
2. 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 [↑](#footnote-ref-2)
3. <https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LOA_Guidance_Final_suomeksi.pdf> [↑](#footnote-ref-3)
4. 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 [↑](#footnote-ref-4)
5. 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> [↑](#footnote-ref-5)
6. <https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide> [↑](#footnote-ref-6)
7. 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. [↑](#footnote-ref-7)
8. 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> [↑](#footnote-ref-8)