Ohje

211/2019 O
x.x.2019

Sähköisen tunnistuspalvelun arviointiohje

Liikenne- ja viestintäviraston ohje

211/2019 O

LUONNOS 20.6.2019

Liikenne- ja viestintävirasto

Erik Palmeninaukio 1
PL 313
00059 TRAFICOM
Puhelin 0295 390 100
www.traficom.fi

Sisällys

Liikenne- ja viestintävirasto

Erik Palmeninaukio 1
PL 313
00059 TRAFICOM
Puhelin 0295 390 100
www.traficom.fi

Liikenne- ja viestintävirasto
Erik Palmeninaukio 1
PL 313
00059 TRAFICOM
Puhelin 0295 390 100
www.traficom.fi

Liikenne- ja viestintävirasto

Erik Palmeninaukio 1
PL 313
00059 TRAFICOM
Puhelin 0295 390 100
www.traficom.fi

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 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] noudattamista. Tämä ohje on annettu lain 42 §:n yleisen valtuuden nojalla.

Liikenne- ja viestintävirastolle toimitettavista ilmoituksista on julkaistu erillinen ohje (214/2016 O). EU:lle notifioitavan sähköisen tunnistamisen järjestelmän vaatimusten mukaisuuden arvioinnista säädetään eIDAS-asetuksessa sekä sähköisen tunnistamisen varmuustasoasetuksessa (LOA)[2].

1.2 Ohjeen voimaantulo

Ohje 211/2019 O tulee voimaan x.x.2019

[1] Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta.
[2] Komission täytäntöönpanoasetus (EU) 2015/1502, annettu 8 päivänä syyskuuta 2015, 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 (ETA:n kannalta merkityksellinen teksti)

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.kyberturvallisuus-keskus.fi/fi/sahkoinen-tunnistaminen ja https://www.traficom.fi/fi/saadokset

Versio	Päiväys	Kuvaus/muutos	Tekijä
211/2019 O	x.x.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	2.11.2016	1. julkaistut versiot	Viestintävirasto, Kyberturvallisuuskeskus

215/2016 O Tunnistus- ja luottamuspalveluiden arviointikertomukset			

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[3] (jäljempänä *LOA* tai *varmuustasoasetus*)
  - Tunnistuslaissa viitatut kohdat varmuustasoasetuksesta
  - LOA-guidance, varmuustasoasetuksen epävirallinen soveltamisohje[4]
- Viestintäviraston määräys 72A/2018 M (jäljempänä *M72*)
  - Määräyksellä tarkennetaan eräitä tunnistuslaissa säädettyjä vaatimuksia

Standardiviittaukset[5]:

- ISO/IEC 27001:2013 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.

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0002 Komission täytäntöönpanoasetus on annettu EU:n nk. eIDAS-asetuksen nojalla (Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014 sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta)
[4] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LOA_Guidance_Final_suomeksi.pdf
[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

- OWASP Mobile AppSec Verification v.1.1.3[6]

Varmuustason lyhenteet taulukoissa

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

1.4 Tunnistuspalvelun määritelmät

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.

[6] https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide

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

1.5 Palvelun tarjoajan 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 **tunnistuspalveluntarjoajan oma selvitys**, jonka palveluntarjoaja toimittaa Liikenne- ja viestintäviraston arvioitavaksi. Asiat on listattu määräyksen 72 16 §:ssä.

Liikenne- ja viestintävirastolle tunnistuspalvelun aloitus-, lopetus- ja muutosilmoitusten yhteydessä toimitettavia tietoja on kuvattu tarkemmin ohjeessa **214/2016 O Sähköisten tunnistus- ja luottamuspalveluiden ilmoitukset.**

SÄÄNNÖKSET

M72 16 § Selvitys muiden vaatimusten täyttämisestä

Tunnistuspalveluntarjoajan on osoitettava omalla kirjallisella selvityksellään tai edellä 15 §:ssä tarkoitetulla arvioinnilla seuraavien tunnistuspalveluntarjoajan luotettavuuteen ja tunnistuspalvelusta annettaviin tietoihin liittyvien vaatimusten täyttyminen:

1) julkaistut ilmoitukset ja käyttäjätiedot, kuten tunnistusperiaatteet, sopimusehdot ja hinnastot
2) vakiintunut organisaatio

3) valmius ottaa vahinkoriskejä
4) riittävät taloudelliset varat
5) vastuu alihankkijoista
6) suunnitelma toiminnan päättämisen varalta

2 Tunnistuspalvelun arviointi ja tarkastuskertomus

2.1 Tarkastuskertomuksen toimittaminen ilmoituksen liitteenä

SÄÄNNÖKSET

TunnL 10 § (23.11.2018/1009) 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 palvelun-tarjoajalle.

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

Tunnistuspalveluntarjoajan ja Väestörekisterikeskuksen on hankittava vaatimustenmukaisuuden arvioinnista tarkastuskertomus, joka toimitetaan Viestintävirastolle.

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

2.1.1 Aloitusilmoitus

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

2.1.2 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

2.1.3 Määräaikaisarviointi

Tunnistuspalvelua koskeva tarkastuskertomus toimitetaan Liikenne- ja viestintävirastolle muutosilmoituksen liitteenä, kun edellisen tarkastuskertomuksen hyväksymisestä 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 virasto on hyväksynyt tarkastuskertomuksen. Tunnistuspalveluntarjoajan on toimitettava virastolle uusi tarkastuskertomus viimeistään kahden vuoden kuluttua edellisen tarkastuskertomuksen hyväksymisestä, mikäli se haluaa jatkaa vahvan sähköisen tunnistuspalvelun tarjoamista.

Tarkastuskertomus voi perustua kokonaan tai osittain standardeihin, joiden määrittelemä arviointiväli on vähemmän kuin kaksi vuotta. Tunnistuspalveluntarjoajan vastuulla on huolehtia siitä, että arvioinnit tehdään

tällaisissa tapauksissa standardin määrittelemin määräajoin. Tunnistuspalveluntarjoajan 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 hyväksymisestä.

Tunnistuslain säännökset arviointivelvollisuudesta tulivat voimaan 1.7.2016 ja lain siirtymäsäännöksen mukaan tarkastuskertomus tuli toimittaa Viestintävirastolle viimeistään 31 päivänä tammikuuta 2017. Virasto on julkaissut neuvontamuistion vuoden 2019 uusinta-arvioinneista (dnro 1003/620/2018 *Tulkintamuistio 12/2018 neuvontaa tunnistuspalveluiden vaatimustenmukaisuuden arvioinnista 2019*)

Aloitus- ja muutosilmoitusten vähimmäissisältö on kuvattu Viestintäviraston ohjeessa 214/2016 O.

2.2 Tunnistuspalvelun arvioitavat osa-alueet

Asiat, joiden vaatimustenmukaisuus on arvioitava riippumattomasti, on säädetty tunnistuslaissa ja tarkennettu viraston määräyksessä 72.

Arviointielin voi käyttää tämän ohjeen kriteeristöjä tai muutakin vastaava 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 §:ssä tarkennetaan vaatimusalueet, joista tunnistuspalveluntarjoaja voi esittää oman selvityksen.

Tunnistusmenetelmän eli tunnistusvälineen tarjoajaa koskevat kaikki kohdat.

Tunnistusvälityspalvelua koskevat kohdat 1a)-1d) ja kohta 2g).

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;

[…]

M72 15 § Arviointikriteerit

Tunnistuspalvelun arvioinnin täytyy kattaa vaatimukset, jotka kohdistuvat:

1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän)

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

2) tunnistusmenetelmään eli tunnistusvälineen

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

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

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 §

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.*

2.3.2 Arviointi

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 vahvaan 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.

Tunnistusmenetelmään liittyvistä vaatimuksista merkityksellisiä **tunnistusvälityspalvelun** toiminnassa ovat todentamismekanismin 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 -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

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 järjestelmistä 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 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.

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 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.

2.4 Tiedot arviointielimestä

SÄÄNNÖKSET

TunnL 28 § (29.6.2016/533) 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).

tusjärjestelmään.

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 M72 18 § tai 19 §:n mukainen peruste)

TunnL 42 § (23.11.2018/1009) 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 72 18 § Tunnistuspalvelun ulkoisen arviointielimen vaatimukset

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

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

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

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

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

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

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

Määräys 72 19 § Tunnistuspalvelun sisäisen tarkastuslaitoksen vaatimukset

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

1) IIA:n ammattistandardien (sisäisen tarkastuksen riippumattomuus ja objektiivisuus, ml. organisatorinen riippumattomuus) noudattamisella;

2) ISACA:n standardien ja tietojärjestelmien valvonnan kehikoiden noudattamisella;

3) BIS:in (Bank for International Settlements) sisäistä tarkastusta koskevien ohjeiden noudattamisella;

4) Finanssivalvonnan määräys- ja ohjekokoelman sisäistä tarkastusta koskevien 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.

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

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.

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 tunnistuspalveluntarjoaja 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 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.

2.6 Arvioinnin suhteuttaminen varmuustasoon ja riskeihin

Vahvan sähköisen tunnistamisen luotettavuudelle on säädetty kaksi varmuustasoa, korotettu ja korkea.[7] Arviointikriterien taulukoissa käytettään lyhenteitä S=korotettu (vastaa eIDAS2, substantial) ja H=korkea (vastaa eIDAS3, high).

[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.

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.

…

2.7 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.

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.

Normaalitilanteessa havaitut poikkeamat on korjattu ennen tarkastuskertomuksen toimittamista Liikenne- ja viestintävirastolle. Jos poikkeamia kuitenkin jää, niiden on käytävä yksiselitteisesti ilmi tarkastuskertomuksesta. Tällöin tarkastuskertomukseen on liitettävä tieto siitä, mitä vähäisiä tai muita poikkeamia järjestelmään on jätetty ja millä aikataululla ja miten ne tullaan korjaamaan.

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.

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 Tunnistamisen menetelmän 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
- M72 6 § Tunnistusmenetelmän tietoturvavaatimukset
- M72 7 § Tunnistusjärjestelmän ja rajapintojen salausvaatimukset
- M72 8 § Tietoturvavaatimukset tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa
- M72 9 § Tietoturvavaatimukset asiointipalvelurajapinnassa

- 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.

M72 7 §:n 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 § (29.3.2019/412) Tunnistuspalvelun tarjoajien luottamusverkosto

- VNA 169/2016 Valtioneuvoston asetus vahvan sähköisen tunnistuspalvelun tarjoajien luottamusverkostosta, 1 § Luottamusverkoston tekniset rajapinnat
- M72 12 § Luottamusverkostossa välitettävät vähimmäistiedot
- M72 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 tietoturvavaatimukset

Vaatimuksia tarkastellaan tietoliikenne-, tietojärjestelmä- ja käyttöturvallisuuden kannalta.

Vaatimukset säädetään seuraavissa säännöksissä

- TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset, 1. mom. 4) kohta
- LOA 2.3.1 Todentamismekanismi
- LOA Liite 2.4.6 Tekniset tarkastukset (controls), kohdat 1, 2 ja 3
- M72 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet

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

3.4 Poikkeamien havainnointikyky ja hallinta ja häiriöilmoitukset

Vaatimukset säädetään seuraavissa säännöksissä

- TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset, 1 mom. 4)
- 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
- M72 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet
- M72 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
- M72 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet
- M72 7 § Tunnistusjärjestelmän ja 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 ja
- 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. kohta 4)
- 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

3.7 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

3.8 Tietoturvallisuuden hallinta

Vaatimukset säädetään seuraavissa säännöksissä

- TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset, 1 mom. 5)
- LOA Liite 2.4 Hallinto ja organisointi, johdanto
- LOA Liite 2.4.3 Tietoturvallisuuden hallinta
- LOA Liite 2.4.7 Noudattaminen ja tarkastus
- M72 4 § Tunnistuspalvelun tarjoajan tietoturvallisuuden hallinnan vaatimukset

- 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 72) 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)
- 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
- M72 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

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

- Ensitunnistus perustuu Suomessa hyväksytyn henkilöllisyystodistuksen esittämiseen
- Ensitunnistus sähköisellä tunnistusvälineellä
- Ensitunnistus muuhun tarkoitukseen tehdyn tunnistamisen perusteella
- Poliisin tekemä ensitunnistus

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 digitoitu allekirjoitus, 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 väärennetyn tai väärän henkilön esittämän henkilöllisyystodistuksen uhalta. Huomioon on otettava
  - henkilöllisyystodistuksen aitoustekijöiden havainnointi ja
  - henkilön itsestään toimittaman kuvan tai videon aitouden varmistaminen ja havainnointi.

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.

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 etäensitunnistamisesta

- Jos henkilöllisyystodistuksen voi esittää etäyhteydellä, arvioinnissa on huomioitava perusteellisesti riskit ja suojakeinot, joilla suojaudutaan väärennetyn tai väärän henkilön esittämän henkilöllisyystodistuksen uhalta.

- Huomioon on otettava henkilöllisyystodistuksen aitoustekijöiden havainnointi ja henkilön itsestään toimittaman kuvan tai videon aitouden varmistaminen ja havainnointi.

- On avoin kysymys, miten henkilöllisyystodistuksen aitous voidaan tarkistaa, jos siinä ei ole sirua. 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 layout on oikeanlainen.

- Henkilöllisyystodistuksen sirun käyttäminen muuttaa tilannetta olennaisesti. Passiivinen autentisointi (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.

- Lähes kaikissa passeissa 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. Ominaisuus on jollain aikavälillä tulossa myös EU-henkilökortteihin. US-passit eivät mahdollista tätä lisätodennusta.

- Kun on varmistettu sirun 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 henkilötodistuksen sirulle ei välttämättä ole talletettu todistuksessa olevaa kasvokuvaa, jolloin sitä ei voida lukea situlta ja hyödyntää henkilöä tunnistettaessa. Biometrisessä passissa kuva on talletettu sirulle.

- 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.

- 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.

- Etäyhteyden päässä olevan henkilön videolla havainnoitavien tai kuvana lähettämien ominaisuuksien vertaamisen henkilöllisyystodistuksesta saatuun vertailutietoon on pystyttävä tekemään luotettavasti.

- 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.

3.10 Tunnistusvälineen eli tunnistusmenetelmän elinkaari

Vaatimukset säädetään seuraavissa säännöksissä

- Hakeminen ja rekisteröinti TunnL 7 §, 20 §, M72 6 §
- Myöntäminen, toimittaminen, aktivointi TunnL 20 §, 21 §, LoA 2.2.2
- voimassaolon keskeyttäminen, peruuttaminen ja uudelleen aktivointi TunnL 25 §, 26 § (LoA 2.2.3)
- uusiminen, korvaaminen, TunnL 22 §, LoA 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], jossa käsitellään henkilöllisyyden todentamista ylläpitotilanteissa.

[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

4 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.)
11. Tulokset osa-alueiden arvioinnista (3.1-3.10 soveltuvin osin)

Liikenne- ja viestintävirasto

Erik Palmeninaukio 1
PL 313
00059 TRAFICOM
Puhelin 0295 390 100
www.traficom.fi

5 LIITE B: Tunnistuspalvelun yleinen arviointikriteeristö

5.1 Tunnistamisen menetelmän ominaispiirteet ja todentamismekanismi

1 Tunnistamisen menetelmän ominaispiirteet ja todentamismekanismi

M72 15 § Arviointikriteerit

Tunnistuspalvelun arvioinnin täytyy kattaa vaatimukset, jotka kohdistuvat:
2) tunnistusmenetelmään eli tunnistusvälineen
c) tunnistamisen menetelmän ominaispiirteisiin ja laatimiseen
g) todentamismekanismeihin

NRO	VAR-MUUS-TASO	TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ	SÄÄNNÖKSET	STANDAR-DIVIIT-TAUS	HUOMIOITA
1.	S, H	Tunnistusmenetelmässä käytetään vähintään kahta todentamistekijää eri luokista	**TunnL 8 a § Tunnistusmenetelmässä käytettävät todentamistekijät** 1) tiedossa oloon perustuvaa todentamistekijää, jonka henkilön on osoitettava olevan tiedossaan; 2) hallussapitoon perustuvaa todentamistekijää, jonka henkilön on osoitettava olevan hallussaan; 3) luontaista todentamistekijää, joka perustuu johonkin luonnollisen henkilön fyysiseen ominaisuuteen. […]		

			LOA Liite 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu Sähköisen tunnistamisen menetelmässä käytetään vähintään kahta todentamistekijää eri luokista.		
2.	S,H	Todentamistekijät ovat toisistaan riippumattomia	**LOA Liite 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu** Sähköisen tunnistamisen menetelmä on suunniteltu siten, että sitä voidaan olettaa käytettävän vain, jos se on sen henkilön hallinnassa tai hallussa, jolle se kuuluu.		Todentamistekijöiden riippumattomuuteen toisistaan on syytä kiinnittää erityistä huomiota mobiililaitteella käytettävissä tunnistusmenetelmissä.
3.	S,H	Tunnistusmenetelmän suunnittelussa on otettu huomioon se, että eri todentamistekijöihin kohdistuu erityyppisiä uhkia	**LOA Liite 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu** Sähköisen tunnistamisen menetelmä on suunniteltu siten, että sitä voidaan olettaa käytettävän vain, jos se on sen henkilön hallinnassa tai hallussa, jolle se kuuluu.		
4.	S,H	Tunnistusmenetelmään liittyvät salaiset tiedot eivät tule tunnistuspalveluntarjoajan henkilökunnan tai alihankkijoiden tietoon	**M72A 6 § Tunnistusmenetelmän tietoturvavaatimukset** […] Palveluntarjoajan on varmistettava, etteivät tunnistusvälineeseen liittyvät salaiset tiedot paljastu sen henkilöstölle missään tilanteessa.		Salaisia tietoja ovat tyypillisesti esimerkiksi PIN-koodit tai muut tietoon perustuvat todentamistekijät. Vaatimuksen tarkoitus on huomioida tunnistuspalvelun vilpillisen henkilökunnan riski.

			Palveluntarjoaja ei saa kopioida tunnistusvälineeseen liittyviä salaisia tietoja.		
5.	S,H	Todentamistekijät on vahvistettu henkilöön liittyväksi	**LOA Liite 1. Sovellettavat määritelmät** 2) todentamistekijällä' tarkoitetaan tekijää, joka on vahvistettu henkilöön kytkeytyväksi ja joka kuuluu johonkin seuraavista luokista […] **LOA Liite 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu** Sähköisen tunnistamisen menetelmä on suunniteltu siten, että sitä voidaan olettaa käytettävän vain, jos se on sen henkilön hallinnassa tai hallussa, jolle se kuuluu.		Esimerkiksi tunnistussovelluksen kytkeminen henkilöön, sirun personointi, tunnuslukulistan tai laitteen kytkeminen henkilöön.
6.	S,H	Todentamismekanismi on suunniteltu siten, että jokaisella tunnistustapahtumalla on yksilöllinen sähköinen todiste	**TunnL 8 a §** […] Jokaisessa tunnistusmenetelmässä on käytettävä sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.3.1 tarkoitettua sellaista dynaamista todentamista, joka muuttuu jokaisessa uudessa henkilön ja hänen henkilöllisyytensä varmentavan järjestelmän välillä tapahtuvassa todentamistapahtumassa.		myös tunnistusvälityspalvelu
7.	S,H	Tunnistustapahtuman sähköinen todiste perustuu henkilöön liitettyihin todentamistekijöihin	**LOA Liite 1. Sovellettavat määritelmät** 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		LOA guidance (otteita) Dynaamisen todentamisen ensisijainen tarkoitus on vähentää esimerkiksi mies välissä (Man in the Middle) -tyyppisten hyökkäysten

			hänen henkilöllisyytensä varmentavan järjestelmän välillä tapahtuvassa todentamisessa;		vaaraa tai riskiä siitä, että aiemmin tallennetun todentamiskerran varmentamistietoja käytetään uudelleen. … 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. … Jos henkilön yksityinen avain on tallennettu etäpalveluna (keskitetysti esimerkiksi tunnistustietojen tarjoajan käyttämälle HSM-laitteelle), yksityisen avaimen käyttämiseen vaadittavan todentamistavan on myös oltava dynaaminen.
8.	H	Käyttäjä voi suojata menetelmän (välineen) ja todentamistekijänsä luotettavasti muiden käytöltä.	**LOA Liite 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu**		Esimerkkejä LOA-guidance: ”Luotettava suojaaminen” tarkoittaa toimenpiteitä, joiden avulla

			Sähköisen tunnistamisen menetelmä on suunniteltu niin, että henkilö, jolle se kuuluu, voi suojata sen luotettavasti muiden käytöltä.		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). Tällä vaatimuksella suojaudutaan toisintamisen, arvaamisen, toiston ja viestinnän väärentämisen muodostamilta uhilta. Edellä mainittujen tekniikoiden lisäksi (ks. Myös LOA-guidance kohta 2.2.1 korkea 1) voidaan käyttää myös seuraavia: ☐ vahvat staattiset salasanat ☐ käyttäjän biometrinen varmentaminen ☐ ympäristön tarkistaminen haitallisen koodin varalta ☐ kaistan ulkopuolella tapahtuva varmentaminen. ☐ Kaikkien salassa pitämiseen 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.
9.	S,H	Tunnistetietoja ei luovuteta luottavalle osapuolelle eli tunnistustapahtumaa ei toteuteta ennen kuin tunnistusväline/menetelmä on varmennettu dynaamisella todentamisella	**LOA Liite 2.3.1 Todentamismekanismi** Henkilön tunnistetietojen luovutusta edeltää sähköisen tunnistamisen menetelmän ja sen voimassaolon luotettava varmentaminen käyttämällä dynaamista todentamista.	A.14.1 Järjestelmien hankkiminen, kehittäminen ja ylläpito/Tietojärjestelmiä koskevat turvallisuusvaatimukset A.14.1.2 sovelluspalvelutapahtumien suojaami-	myös tunnistusvälityspalvelu

				nen julkisissa verkoissa A.14.1.3 sovelluspalvelutapahtumien suojaaminen	
10.	S,H	Tunnistustapahtumassa tallentuvat tunnistetiedot (henkilötiedot) suojataan	**LOA Liite 2.3.1 Todentamismekanismi** Jos henkilön tunnistetiedot tallennetaan osana todentamismekanismia, nämä tiedot on suojattu niiden menetykseltä ja vaarantamiselta, mukaan lukien analyysi verkkoympäristön ulkopuolella. Vrt. M72 7-9 § sanomatason salausvaatimukset jäljempänä		myös tunnistusvälityspalvelu huomioitava kaikki tunnistustapahtumaan osallistuvien tekniset ympäristöt, joissa tunnistetietoja tallentuu
11.	S	Todentamismekanismin turvatoimenpiteet suojaavat vakavuusasteeltaan kohtuulliselta hyökkäykseltä	**TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset** 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;	Arvioinnissa olisi otettava huomioon asiaankuuluvat uhat. Standardissa ISO	yös tunnistusvälityspalvelu todentamismekanismissa on huomioitava myös uhka väärän asiointipalvelun käynnistämästä tunnistuspyynnöstä tai kaappaamasta tunnistusistunnosta (phishing)

			LOA Liite 2.3.1 Todentamismekanismi 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.	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	ks. LOA guidance kohdan 2.3.1 kuvaus s. 24-26 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LOA_Guidance_Final_suomeksi.pdf

				ja toisena esiintyminen. 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.	
12.	H	Todentamismekanismin turvatoimenpiteet suojaavat vakavuusasteeltaan korkean tason hyökkäykseltä	**TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset** 8.1 § 3) tunnistusmenetelmällä voidaan varmistua, että ainoastaan tunnistusvälineen haltija voi käyttää välinettä siten, että sähköisen tunnistamisen varmuustasoasetuksen	ks. yllä	myös tunnistusvälityspalvelu kaikki todentamismekanismiin liittyvät turvallisuusseikat suhteutettuna korkean vakavuustason hyökkäyspotentiaaliin

			liitteen kohdissa 2.2.1 ja 2.3 vähintään korotetulle varmuustasolle säädetyt edellytykset täyttyvät; **LOA Liite 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu** Sähköisen tunnistamisen menetelmä on suojattu toisintamiselta ja väärentämiseltä sekä hyökkäyksiltä, joiden vakavuusaste on korkea (”high”). **LOA Liite 2.3.1 Todentamismekanismi** Todentamismekanismissa 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.		
13.	S,H	Todentamismekanismissa noudatetaan pakollisia salausvaatimuksia **tunnistusvälineen tarjoajan ja tunnistusvälityksen välillä**	**LOA Liite 2.4.6 Tekniset tarkastukset** (controls) 2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät sähköisen viestinnän kanavat on suojattu salakuuntelulta, manipuloinnilta ja toistolta. **M72 7 § Tunnistusjärjestelmän ja rajapintojen salausvaatimukset**	A.10.1.1 salauksen käytön periaatteet A.13.2.3 viestintäturvalli-	myös tunnistusvälityspalvelu

			Tunnistuspalveluntarjoajien välisten ja tunnistuspalveluntarjoajan ja asiointipalvelun välisten rajapintojen liikenne on salattava. Salauksessa, avaintenvaihdossa sekä salaukseen liittyvässä allekirjoituksessa on noudatettava seuraavia menetelmiä: 1) Avaintenvaihto: Avaintenvaihdossa on käytettävä DHE-menetelmiä tai elliptisiä käyriä käyttäviä ECDHE-menetelmiä. Laskutoimituksissa käytetyn äärellisen kunnan (finite field) koon tulee olla DHE-menetelmässä vähintään 2048 bittiä ja ECDHE-menetelmässä vähintään 224 bittiä. 2) Allekirjoitus: Käytettäessä RSA:ta sähköiseen allekirjoitukseen, avaimen pituuden tulee olla vähintään 2048 bittiä. Käytettäessä elliptisen käyrän menetelmää ECDSA:ta alla olevan kunnan koon tulee olla vähintään 224 bittiä. 3) Symmetrinen salaus: Salausalgoritmin on oltava AES tai Serpent. Avaimen pituuden tulee olla vähintään 128 bittiä. Salausmoodin on oltava CBC, GCM, XTS tai CTR. 4) Tiivistefunktiot: Tiivistefunktion on oltava SHA-2, SHA-3 tai Whirlpool. SHA-2:lla tarkoitetaan funktioita SHA224, SHA256, SHA384 ja SHA512.	suus/tietojen siirtäminen: sähköinen viestintä	

			Salausasetukset tulee teknisesti pakottaa edellä lueteltuihin vähimmäistasoihin, jotta yhteyskättelyissä ei päädyttäisi vähimmäistasoja heikompiin asetuksiin. Mikäli yhteyskäytännössä käytetään TLS-protokollaa, tulee käyttää vähintään TLS versiota 1.2 tai uudempaa versiota. TLS versiota 1.1 voi käyttää ainoastaan, jos käyttäjän päätelaite ei tue uudempia versioita. Henkilötietoja sisältävien sanomien eheys ja luottamuksellisuus on suojattava edellä 1 momentissa tarkoitetun liikenteen salauksen lisäksi sanomatasolla 1 momentin mukaisesti. **8 § Tietoturvavaatimukset tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa** Salausmenetelmien tulee täyttää edellä 7 §:n 1 - 4 momentissa määrätyt vaatimukset. Osapuolten tunnistamisessa ja tunnistamisessa tarvittavan tiedon välityksessä tulee käyttää metadataa tai vastaavia menettelyitä, jotka takaavat vastaavan tietoturvatason. Kaikki henkilötiedot tulee salata ja allekirjoittaa sanomatasolla.		

14.	S,H	Todentamismekanismissa noudatetaan pakollisia salausvaatimuksia **tunnistuspalvelun ja asiointipalvelun välillä**	**LOA Liite 2.4.6 Tekniset tarkastukset** (controls) 2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät sähköisen viestinnän kanavat on suojattu salakuuntelulta, manipuloinnilta ja toistolta. **M72 7 § (yllä)** **M72 9 § Tietoturvavaatimukset asiointipalvelurajapinnassa** Tunnistusvälityspalvelun tarjoajan ja asiointipalvelun välisen rajapinnan tulee täyttää edellä 7 §:n 1 - 4 momentissa määrätyt vaatimukset. Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tulee huolehtia henkilötietojen luottamuksellisuudesta ja eheydestä asiointipalvelu- ja käyttäjärajapinnassa.	A.10.1.1 salauksen käytön periaatteet A.13.2.3 viestintäturvallisuus/tietojen siirtäminen: sähköinen viestintä	huom. myös tunnistusvälityspalvelu
15.	S,H	Todentamismekanismissa noudatetaan pakollisia salausvaatimuksia **käyttäjärajapinnassa (selain, mobiili)**	**LOA Liite 2.4.6 Tekniset tarkastukset** (controls) 2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät sähköisen viestinnän kanavat on suojattu salakuuntelulta, manipuloinnilta ja toistolta. **M72 7 § (yllä)** **M72 9 § Tietoturvavaatimukset asiointipalvelurajapinnassa**	A.10.1.1 salauksen käytön periaatteet A.13.2.3 viestintäturvalli-	huom. myös tunnistusvälityspalvelu

			Tunnistusvälityspalvelun tarjoajan ja asiointipalvelun välisen rajapinnan tulee täyttää edellä 7 §:n 1 - 4 momentissa määrätyt vaatimukset. Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tulee huolehtia henkilötietojen luottamuksellisuudesta ja eheydestä asiointipalvelu- ja käyttäjärajapinnassa.	suus/tietojen siirtäminen: sähköinen viestintä	
16.	H	Todentamismekanismissa noudatetaan **suosituksen** mukaisia tiukennettuja/korkean tason salausvaatimuksia tunnistusvälityspalvelun ja tunnistusvälityksen välillä, tunnistuspalvelun ja asiointipalvelun välillä ja käyttäjärajapinnassa (selain, mobiili)	**MPS72 kohta B 7.2 (14.5.2018) suositus** Korkealla varmuustasolla tunnistusjärjestelmässä suositellaan sovellettavaksi määräyksessä 7 §:n 1 momentissa edellytettyjen korotetun varmuustason vaatimusten sijaan seuraavassa esitettyjä suluissa olevia arvoja: 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 (korkealla varmuustasolla 3072) bittiä ja ECDHE-menetelmässä vähintään 224 (korkealla varmuustasolla 256) bittiä.	A.10.1.1 salauksen käytön periaatteet A.13.2.3 viestintäturvallisuus/tietojen siirtäminen: sähköinen viestintä	huom. myös tunnistusvälityspalvelu

			IANA:n IKEv2-määritysten mukaiset DH-ryhmät 14 - 21, 23, 24 ja 26 (korkealla varmuustasolla *15 - 21*) toteuttavat edellä mainitut edellytykset. 2) Allekirjoitus: Käytettäessä RSA:ta sähköiseen allekirjoitukseen, avaimen pituuden tulee olla vähintään 2048 (korkealla varmuustasolla 3072) bittiä. Käytettäessä elliptisen käyrän menetelmää ECDSA:ta, alla olevan kunnan koon tulee olla vähintään 224 (korkealla varmuustasolla 256) bittiä. 3) Symmetrinen salaus: Salausalgoritmin on oltava AES tai Serpent *(*korkealla varmuustasolla *AES tai Serpent)*. Avaimen pituuden tulee olla vähintään 128 (korkealla varmuustasolla 128) bittiä. Salausmoodin on oltava CBC, GCM, XTS tai CTR. 4) Tiivistefunktiot: Tiivistefunktion on oltava SHA-2, SHA-3 tai Whirlpool. SHA-2:lla tarkoitetaan funktioita SHA224, SHA256, SHA384 ja SHA512 (korkealla varmuustasolla *SHA256, SHA384, SHA512 ja SHA-3*)		

5.2 Yhteentoimivuus

2 Yhteentoimivuus

KESKEISET 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.
…

M72 15 § Arviointikriteerit
Tunnistuspalvelun arvioinnin täytyy kattaa vaatimukset, jotka kohdistuvat:
1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän)
d) teknisiin toimenpiteisiin

TunnL 12 a §
…
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.
…

M72 12 § Luottamusverkostossa välitettävät vähimmäistiedot

Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on välitettävä:
1) luonnollista henkilöä koskevassa tunnistustapahtumassa ainakin henkilön yksilöivä tunniste, henkilön etunimi, henkilön sukunimi ja henkilön syntymäaika;

2) oikeushenkilöä koskevassa tunnistustapahtumassa ainakin oikeushenkilöä edustavan luonnollisen henkilön yksilöivä tunniste, henkilön sukunimi, henkilön etunimi ja organisaation yksilöivä tunniste; sekä
3) tieto tunnistusvälineen korotetusta tai korkeasta varmuustasosta.

Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on oltava valmius välittää:
1) tieto siitä, koskeeko tunnistustapahtuma julkisen hallinnon asiointipalvelua vai yksityistä asiointipalvelua;
2) luonnollista henkilöä koskevassa tunnistustapahtumassa etunimi (-nimet) ja sukunimi (-nimet) syntymähetkellä, syntymäpaikka, nykyinen osoite ja sukupuoli;
3) oikeushenkilöä koskevassa tunnistustapahtumassa
a) nykyinen osoite;
b) arvonlisäverotunniste;
c) verorekisterinumero;
d) Euroopan parlamentin ja neuvoston direktiivin 2009/101/EY[9] 3 artiklan 1 kohdassa tarkoitettu tunniste;
e) komission täytäntöönpanoasetuksessa (EU) N:o 1247/2012[10] tarkoitettu oikeushenkilötunnus (LEI);
f) komission täytäntöönpanoasetuksessa (EU) N:o 1352/2013[11] tarkoitettu taloudellisen toimijan rekisteröinti- ja tunnistenumero (EORI-numero); sekä
g) neuvoston asetuksen N:o 389/2012[12] 2 artiklan 12 kohdassa tarkoitettu valmisteveronumero.

[9] Euroopan parlamentin ja neuvoston direktiivi 2009/101/EY, annettu 16 päivänä syyskuuta 2009, niiden takeiden yhteensovittamisesta samanveroisiksi, joita jäsenvaltioissa vaaditaan perustamissopimuksen 48 artiklan toisessa kohdassa tarkoitetuilta yhtiöiltä niiden jäsenten sekä ulkopuolisten etujen suojaamiseksi (EUVL L 258, 1.10.2009, s. 11).
[10] Komission täytäntöönpanoasetus (EU) N:o 1247/2012, annettu 19 päivänä joulukuuta 2012, kauppatietorekistereihin OTC- johdannaisista, keskusvastapuolista ja kauppatietorekistereistä annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 648/2012 mukaisesti annettavien kauppailmoitusten muotoa ja antamistiheyttä koskevista teknisistä täytäntöönpanostandardeista (EUVL L 352, 21.12.2012, s. 20).
[11] Komission täytäntöönpanoasetus (EU) N:o 1352/2013, annettu 4 päivänä joulukuuta 2013, teollis- ja tekijänoikeuksien tullivalvonnasta annetussa Euroopan parlamentin ja neuvoston asetuksessa (EU) N:o 608/2013 säädettyjen lomakkeiden vahvistamisesta (EUVL L 341, 18.12.2013, s. 10).
[12] Neuvoston asetus (EU) N:o 389/2012, annettu 2 päivänä toukokuuta 2012, hallinnollisesta yhteistyöstä valmisteverotuksen alalla ja asetuksen (EY) N:o 2073/2004 kumoamisesta (EUVL L 121, 8.5.2012, s. 1).

M72 14 § Tiedonsiirrossa käytettävä protokolla ja muut vaatimukset

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

M72 25 § Voimaantulo ja siirtymäsäännökset

[…]

Valmius määräyksen 12 §:n 2 momentin mukaisten tietojen välittämiseen tunnistusjärjestelmässä on suunniteltava teknisesti viimeistään 1.10.2018.

NRO	VAR-MUUS TASO	TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ	SÄÄNNÖKSET	STANDAR-DIVIIT-TAUS	HUOMIOITA
17.	S, H	Tunnistuspalvelun tarjoaja tarjoaa luotta-musverkostossa vähintään yhtä yleisesti käytetyn standardin mukaista rajapintaa.	**VNA 169/2016 Valtioneuvoston asetus vahvan sähköisen tunnistuspalvelun tarjoajien luottamusverkostosta** **1 § Luottamusverkoston tekniset rajapinnat** Vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain (617/2009), jäljempänä tunnistuslaki, 12 a §:n 2 momentissa tarkoitettuja teknisiä rajapintoja ovat: 1) tunnistusvälineen tarjoajien välinen rajapinta;		**Soveltaminen:** Liikenne- ja viestintävirasto on laatinut luottamusverkoston yhteistoimintaryhmää kuullen suositusprofiilit SAML ja Open IDConnect -protokollille. 212/2018 S Finnish Trust Network SAML 2.0 Protocol Profile version 1.0 213/2018 S Finnish Trust Network OpenID Connect 1.0 Protocol Profile version 1.0

			2) tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välinen rajapinta; 3) tunnistusvälityspalvelun tarjoajan ja tunnistuspalveluun luottavan osapuolen välinen rajapinta. Luottamusverkostoon kuuluvat tunnistuspalvelun tarjoajat voivat sopia tunnistuslain 12 a §:n 3 momentissa tarkoitetun tunnistetiedon veloituksen välittämiseen tarvittavasta tai muusta luottamusverkoston toiminnassa tarpeellisesta rajapinnasta. Luottamusverkostoon kuuluvan tunnistuspalvelun tarjoajan on tarjottava 1 momentin 1 ja 2 kohdassa tarkoitetuissa rajapinnoissa kummassakin vähintään yhtä yleisesti käytetyn standardin mukaista teknistä rajapintaa.		Suositukset löytyvät viraston verkkosivulta https://www.kybertur-vallisuuskeskus.fi/fi/sahkoinen-tunnistaminen
18.	S,H	Tunnistusvälineen tarjoaja tarjoaa vaatimusten mukaiset tiedot (attribuutit) **luonnollisen henkilön** tunnistamisessa	**M72 12 § Luottamusverkostossa välitettävät vähimmäistiedot** Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on välitettävä: 1) luonnollista henkilöä koskevassa tunnistustapahtumassa ainakin henkilön yksilöivä tunniste, henkilön etunimi, henkilön sukunimi ja henkilön syntymäaika;		

Liikenne- ja viestintävirasto
Erik Palmeninaukio 1
PL 313
00059 TRAFICOM
Puhelin 0295 390 100
www.traficom.fi

			… 3) tieto tunnistusvälineen korotetusta tai korkeasta varmuustasosta.		
19.	S, H	Tunnistusvälineen tarjoajalla on vaadittu suunniteltu **valmius** välittää optionaaliset tiedot **luonnollisen henkilön** tunnistamisessa	**M72 12 § Luottamusverkostossa välitettävät vähimmäistiedot** 2 mom. Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on oltava 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; …		MPS72 12.1 § perustelut, s. 56: Valmius välittää valinnaisia attribuutteja tarkoittaa, että valinnaisten attribuuttien käsittely täytyy suunnitella rajapinnassa ja tunnistusjärjestelmässä siten, että tunnistuspalvelun tarjoajalla on käsitys käyttöönotossa tarvittavista teknisistä toimenpiteistä. Teknistä toteutusta järjestelmiin ei vaadita valinnaisille attribuuteille. Teknisissä konfiguroinneissa tulee kuitenkin huomioida, etteivät tunnistussanomiin sisältyvät valinnaiset attribuutit haittaa tunnistustapahtumia silloinkaan, kun niiden käytöstä ei ole sovittu. Valvontaa varten suunnitelma täytyy käytännössä dokumentoida.

20.	S, H	Tunnistusvälineen tarjoaja tarjoaa vaatimusten mukaiset tiedot (attribuutit) **oikeushenkilön** tunnistamisessa	**M72 12 § Luottamusverkostossa välitettävät vähimmäistiedot** Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on välitettävä: … 2) oikeushenkilöä koskevassa tunnistustapahtumassa ainakin oikeushenkilöä edustavan luonnollisen henkilön yksilöivä tunniste, henkilön sukunimi, henkilön etunimi ja organisaation yksilöivä tunniste; sekä 3) tieto tunnistusvälineen korotetusta tai korkeasta varmuustasosta.		vain, jos ryhdytään tarjoamaan oikeushenkilön vahvaa sähköistä tunnistusta
21.	S, H	Tunnistusvälineen tarjoajalla on vaadittu suunniteltu valmius välittää optionaaliset tiedot **oikeushenkilön** tunnistamisessa	**M72 12 § Luottamusverkostossa välitettävät vähimmäistiedot** Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on oltava valmius välittää: 1) tieto siitä, koskeeko tunnistustapahtuma julkisen hallinnon asiointipalvelua vai yksityistä asiointipalvelua;		

			… 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 1247/2012 tarkoitettu oikeushenkilötunnus (LEI); f) komission täytäntöönpanoasetuksessa (EU) N:o 1352/2013 tarkoitettu taloudellisen toimijan rekisteröinti- ja tunnistenumero (EORI-numero); sekä g) neuvoston asetuksen N:o 389/2012 2 artiklan 12 kohdassa tarkoitettu valmisteveronumero.		

5.3 Tekniset tietoturvavaatimukset

3 Tekniset tietoturvavaatimukset

KESKEISET SÄÄNNÖKSET

M72A 15 § Arviointikriteerit
Tunnistuspalvelun arvioinnin täytyy kattaa 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 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.

M72 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet

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

1) tietoliikenneturvallisuus
    a) verkon rakenteellinen turvallisuus
    b) tietoliikenneverkon vyöhykkeistäminen
    c) suodatussäännöt vähimpien oikeuksien periaatteilla
    d) suodatuksen ja valvontajärjestelmien hallinnointi koko elinkaaren ajan
    e) hallintayhteydet
2) tietojärjestelmäturvallisuus
    a) pääsyoikeuksien hallinta
    b) järjestelmien käyttäjien tunnistaminen
    c) järjestelmien koventaminen
    d) haittaohjelmasuojaus
    e) turvallisuuteen liittyvien tapahtumien jäljitys
    f) poikkeamien havainnointikyky ja toipuminen
    g) kansainvälisesti tai kansallisesti suositellut salausratkaisut muutoin kuin 7 §:ssä säädetyltä osin

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

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

5.3.1 Tietoliikenneturvallisuus

3.1 Tietoliikenneturvallisuus

nro	var-muus-taso	TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ	Säännökset	Standar-diviittaus	huomioita

22.	S,H	Tietoliikenneturvallisuus: tunnistusjärjestelmän **tietoliikenneyhteydet, hallintayhteydet, prosessit** (tunnistuspalvelun tuotantoon ml. hallintaan liittyvien osaprosessien tietoliikenne) ja niiden **suojauskäytännöt** on **tunnistettu ja dokumentoitu** Tunnistusjärjestelmän tietoliikenneyhteyksien vyöhykkeistäminen ja suodatussäännöstöt on toteutettava vähimpien oikeuksien (least privilege) ja monitasoisen suojaamisen (defence in depth) periaatteiden mukaisesti	**M72A 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet** Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän 4) tietoliikenneturvallisuus a) verkon rakenteellinen turvallisuus b) tietoliikenneverkon vyöhykkeistäminen **LOA Liite 2.4.6 Tekniset tarkastukset** (controls) 2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät sähköisen viestinnän kanavat on suojattu salakuuntelulta, manipuloinnilta ja toistolta.	A.8.1.1 Suojattavan omaisuuden luetteloiminen A.13.1 viestintäturvallisuus/verkon turvallisuuden hallinta: A.13.1.1 verkon hallinta A.13.1.3 ryhmien eriyttäminen verkossa	Tunnistusjärjestelmän kokonaisarkkitehtuurissa huolehditaan tietoliikenneturvallisuudesta. Huom. suunnittelussa on huolehdittava myös kaikista relevanteista tietoliikenneyhteyksistä alihankkijoihin (infra, ohjelmistot, käyttöpalvelut, korttitehdas jne. jne.) Ilmoitukseen/**tarkastuskertomukseen** on liitettävä 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
23.	S, H	Tietoliikenneturvallisuus:	**M72A 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet**	A.8.1.1 Suojatta-	

		Tunnistusjärjestelmän **tietoliikennelaitteet** (vanhassa kriteeristössä oli *Käytössä oleva omaisuus*) **ja -järjestelmät** on tunnistettu ja dokumentoitu.	Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän 1) tietoliikenneturvallisuus a) verkon rakenteellinen turvallisuus	van omaisuuden luetteloiminen	
24.	S, H	Tietoliikenneturvallisuus: **Tuotantoverkko** tulee olla **eriytettynä** ylläpito- ja hallinnointiverkosta. Ylläpito- ja hallinnointiverkon tulee olla eriytettynä muusta toimistoverkosta. Käytössä on tuotannosta eriytetty kehitysympäristö.	**M72A 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet** Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän 1) tietoliikenneturvallisuus a) verkon rakenteellinen turvallisuus b) tietoliikenneverkon vyöhykkeistäminen	A.12.1.4 Käyttöturvallisuus: Kehitys-, testaus- ja tuotantoympäristöjen erottaminen	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, luottamuksellisuudelle ja käytettävyydelle.
25.	S,H	Tietoliikenneturvallisuus: Tunnistusjärjestelmän tietoliikenneyhteyksillä **huolehditaan suodatuksista** vähimpien oikeuksien periaatteilla	**M72A 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet** Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän 1) tietoliikenneturvallisuus c) suodatussäännöt vähimpien oikeuksien periaatteilla	A.13.1.1-3 viestintäturvallisuus/verkon turvallisuuden hallinta:	

				A.13.1.1 verkon hallinta A.13.1.2 Verkkopalvelujen turvaaminen A.13.1.3 Ryhmien eriyttäminen verkossa ks. myös pääsynhallinta	
26.	S, H	Tietoliikenneturvallisuus: Tuotantoverkon **yhteyksien julkiseen verkkoon** tulee olla riskiperusteisia, vain palvelun toiminnallisuudet mahdollistavia yhteyksiä.	**M72A 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet** Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän 1) tietoliikenneturvallisuus a) verkon rakenteellinen turvallisuus c) suodatussäännöt vähimpien oikeuksien periaatteilla	ks. ed. rivi	Kaikki muut kuin toiminnalle tarpeelliset yhteydet on nimenomaisesti kielletty tai suljettu.

27.	S, H	Tietoliikenneturvallisuus: Tunnistuspalveluiden ja luottavien osapuolten **kryptografinen avainmateriaali** tai **metadata** vaihdetaan turvallisesti	**M72A 8 § Tietoturvavaatimukset tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa** Osapuolten tunnistamisessa ja tunnistamisessa tarvittavan tiedon välityksessä tulee käyttää metadataa tai vastaavia menettelyitä, jotka takaavat vastaavan tietoturvatason. vrt. **M72A 7-9 § sanomatason salausvaatimus** vrt. **LOA 2.4.6 Tekniset tarkastukset** 1. Käytössä on oikeasuhteiset tekniset tarkastukset palvelujen turvallisuuteen kohdistuvien riskien hallitsemiseksi ja käsiteltävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi. 2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät sähköisen viestinnän kanavat on suojattu salakuuntelulta, manipuloinnilta ja toistolta. vrt. **LOA 2.3.1 Todentamismekanismi** Todentamismekanismissa toteutetaan turvatoimenpiteitä sähköisen tunnistamisen menetelmän varmentamiseksi siten, että on erittäin epätodennäköistä, että viestin arvaaminen, salakuuntelu, toisto tai manipulointi hyökkäyksessä, jonka vakavuusaste on korkeampaa perustasoa (”enhanced-basic”), voi heikentää todentamismekanismeja.	A.10.1.2 Salauksenhallinta: salausavainten hallinta	vrt. PSD2/RTS eIDAS art45 tai eSeal varmennevaatimus osapuolen tunnistamiselle Pitäisikö olla avaintenhallintakäytäntöjen määrittely eri varmuustasoille? Ensimmäinen avaintenvaihto ja uusimiset voisi olla tarpeen suunnitella eri tavalla käytännön syistä erityisesti luottavien osapuolten kanssa; molempien pitäisi kuitenkin olla turvallisia. Ohjeessa 211/2016 oli seuraavia informatiivisia huomioita: politiikassa huomioidaan salausavaimien suojaus koko niiden elinkaaren ajalla Salausavaintenhallinnan prosessit ja käytännöt ovat dokumentoituja ja asianmukaisesti toteutettuja 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)
28.	H	Tietoliikenneturvallisuus: Tunnistuspalveluiden ja luottavien osa-puolten kryptografinen avainmateriaali tai metadata vaihdetaan turvallisesti	vrt. yllä sekä **LOA 2.3.1 Todentamismekanismi** Todentamismekanismissa 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.	A.10.1.2 Salauksenhallinta: salausavainten hallinta	pitäisikö olla avaintenhallintakäytäntöjen määrittely eri varmuustasoille?? Ensimmäinen avaintenvaihto ja uusimiset voisi olla tarpeen suunnitella eri tavalla käytännön syistä erityisesti luottavien osapuolten kanssa; molempien pitäisi kuitenkin olla turvallisia.
29.	S,H	Tietoliikenneturvallisuus: Tunnistusjärjestelmän tietoliikenneyhteyksien **suodatusten ja valvontajärjestelmien hallinnoinnista** huolehditaan	Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän 1) tietoliikenneturvallisuus d) suodatuksen ja valvontajärjestelmien hallinnointi koko elinkaaren ajan	A.13.1 viestintäturvallisuus/verkon turvallisuuden hallinta:	

Liikenne- ja viestintävirasto

Erik Palmeninaukio 1
PL 313
00059 TRAFICOM
Puhelin 0295 390 100
www.traficom.fi

				A.13.1.1 verkon hallinta	
30.	S	Tietoliikenneturvallisuus/hallinta: Tunnistusjärjestelmän etäkäytössä ja hallinnassa on **arvioitu ja minimoitu** sähköpostin tai web-selailun kautta aiheutuvat tietoturvauhat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvauhat.	**M72A 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet** Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän 1) tietoliikenneturvallisuus e) hallintayhteydet 3) käyttöturvallisuus c) etäkäyttö ja -hallinta Tuotantoverkko ja sen edellä 1 momentin 1) e) ja 3) c) alakohdissa tarkoitetut hallintayhteydet ja etäkäyttö- ja etähallinta on toteutettava siten, että organisaation muiden palveluiden kuten sähköpostin tai web-selailun kautta aiheutuvat tietoturvauhat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvauhat on a) korotetulla varmuustasolla erityisesti arvioitu ja minimoitu	A.9.4. Järjestelmien ja sovellusten pääsynhallinta: A.9.4.1 Tietoihin pääsyn rajoittaminen A.9.4.4 Ylläpito-ja hallintasovellukset A.13.1.3 verkon turvallisuuden hallinta: Ryh-	MPS72: internetiä ja toimistoverkkoa pidetään ei-luotettuna verkkona, ellei toimistoverkko kuulu vaatimustenmukaisuuden arvioinnin piiriin. Tiedonsiirtokanavan täytyy siis olla etäkäytössä suojattu ja toimistoverkon aiheuttamat riskit täytyy huomioida. Korotetun varmuustason vaatimukset ovat tavanomaisia ja ne katetaan jo esimerkiksi ISO 27001 -vaatimusten kautta, jos sovelletaan sitä.

				mien eriyttäminen verkossa	
31.	H	Tietoliikenneturvallisuus/hallinta: Tunnistusjärjestelmän (tuotantoverkon) etäkäytössä ja etähallinnassa on **estetty** sähköpostin tai web-selailun kautta aiheutuvat tietoturvauhat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvauhat	**M72A 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet** Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän 1)tietoliikenneturvallisuus e) hallintayhteydet 3) käyttöturvallisuus c) etäkäyttö ja -hallinta **M72A 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet** Tuotantoverkko ja sen edellä 1 momentin 1) e) ja 3) c) alakohdissa tarkoitetut hallintayhteydet ja etäkäyttö- ja etähallinta on toteutettava siten, että organisaation muiden palveluiden kuten sähköpostin tai web-selailun kautta aiheutuvat tietoturvauhat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvauhat on … b) korkealla varmuustasolla kokonaisuutena arvioiden estetty. **MPS72 soveltamisohje:**	ks. ed. rivi	

			Korkealla varmuustasolla 2 momentin 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. Korkealla varmuustasolla edellytetty kokonaisarvio tarkoittaa sitä, että jos käytettään muuta kuin edellä kuvattua kovennettua työasemaa, otetaan toteutuksessa huomioon tuotantojärjestelmän eriyttäminen ja muut järjestelyt, joilla tietoturvauhkat 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-proxya. Välttämättömien tiedostojen siirrossa koneelta toiselle on myös huomioitava haittaohjelmien riski mm. pitämällä huolta siitä, että käytetään vain luotettavia lähteitä ja varmistetaan tietoturvallisuus (eheys) kaikilla tarpeellisilla menetelmillä.		

5.3.2 Tietojärjestelmäturvallisuus

3.2 Tietojärjestelmäturvallisuus

NRO	VAR-MUUS-TASO	TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ	SÄÄNNÖKSET	STANDAR-DIVIIT-TAUS	HUOMIOITA
32.	S, H	Tietojärjestelmäturvallisuus: Tunnistusjärjestelmän **tietojärjestelmät ja prosessit** (tunnistuspalvelun tuotantoon ml. hallintaan liittyvät tietojärjestelmiä käyttävät prosessit) on **tunnistettu ja dokumentoitu.** Tunnistusjärjestelmän tietojärjestelmät on **luokiteltu** huomioiden niissä käsiteltävä tieto ja niiden mahdollistamat toiminnot. Järjestelmien luokittelussa tulee huomioida suojattavan tiedon koko elinkaari. Hallintaan käytettävä tietojenkäsittelyympäristöön on erotettu muista ympäristöistä	**M72A 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet** Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän 2) tietojärjestelmäturvallisuus a) pääsyoikeuksien hallinta b) järjestelmien käyttäjien tunnistaminen	A.8.1.1 suojattavan omaisuuden hallinta, vastuu suojattavasta omaisuudesta: suojattavan omaisuuden luetteloiminen A.8.2.1 Suojattavan omaisuuden hallinta: tietojen luokittelu	Luokittelu: mm. laitteiden, ohjelmistojen ja muu omaisuuden hyväksytty käyttö tulee olla määriteltynä

Liikenne- ja viestintävirasto

Erik Palmeninaukio 1
PL 313
00059 TRAFICOM
Puhelin 0295 390 100
www.traficom.fi

33.	S, H	Tietojärjestelmäturvallisuus: Tunnistusjärjestelmän **pääsyoikeudet** on määritelty ja dokumentoitu. Pääsyoikeudet **perustuvat** tietojärjestelmien luokitteluun ja henkilön/käyttäjän tehtäviin. Pääsy tulee myöntää vain tehtävien mukaisesti (vähimpien oikeuksien periaate).	**M72A 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet** Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän 2) tietojärjestelmäturvallisuus a) pääsyoikeuksien hallinta b) järjestelmien käyttäjien tunnistaminen	A.9.1.1 pääsynhallinnan liiketoiminnalliset vaatimukset: pääsynhallintapolitiikka A.9.1.2 pääsy verkkoihin ja verkko verkkopalveluihin A.9.4.1 järjestelmien ja sovellusten pääsynhallinta: tietoihin pääsyn rajoittaminen	Pääsyoikeuksien hallinnoinnin avulla rajoitetaan pääsy tietoon ja tiedonkäsittely-ympäristöihin suunnitelmallisesti ja dokumentoidusti

Liikenne- ja viestintävirasto

Erik Palmeninaukio 1
PL 313
00059 TRAFICOM
Puhelin 0295 390 100
www.traficom.fi

34.	S, H	Tietojärjestelmäturvallisuus: Tunnistusjärjestelmän tietojärjestelmien **käyttäjät tunnistetaan** tunnetulla ja turvallisena pidetyllä tekniikalla/menetelmällä.	**M72A 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet** Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän 2) tietojärjestelmäturvallisuus a) pääsyoikeuksien hallinta b) järjestelmien käyttäjien tunnistaminen	A.9.4.2 järjestelmien ja sovellusten pääsynhallinta: turvallinen kirjautuminen	esim. varmenteet, 2FA pääsääntöisesti muu kuin salasana, mutta jos mukana salasana, kunnolliset salasanapituudet ja yksilölliset (ei yhteiskäyttöiset) salasanat ja käyttäjätunnukset
35.	S, H	Tietojärjestelmäturvallisuus: Pääsyoikeuksia valvotaan ja niiden **ajantasaisuudesta** huolehditaan.	**M72A 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet** Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän 2) tietojärjestelmäturvallisuus a) pääsyoikeuksien hallinta b) järjestelmien käyttäjien tunnistaminen	A.9.2 pääsyoikeuksien hallinta A.9.2.1 Käyttäjien rekisteröinti ja poistaminen A.9.2.3 Ylläpito-oikeuksien hallinta	

				A.9.2.5 pääsyoikeuksien uudelleenarviointi A.9.2.6 pääsyoikeuksien poistaminen ja muuttaminen	
36.	S,H	Tietojärjestelmäturvallisuus: Henkilöstön **tehtävät ja toiminnot on määriteltävä** siten, ettei yksi henkilö pysty omalla toiminnallaan tahattomasti tai tahallisesti aiheuttamaan vakavaa turvallisuuspoikkeamaa (vaaralliset työyhdistelmät).	**M72A 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet** Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän 2) tietojärjestelmäturvallisuus a) pääsyoikeuksien hallinta b) järjestelmien käyttäjien tunnistaminen		Esimerkiksi vilpillisen tai huolimattoman työntekijän mahdollisuutta myöntää tunnistusmenetelmä vaatimusten vastaisesti voidaan ehkäistä tehtävien määrittelyllä tai muilla kontrolleilla, jotka vähentävät erehdyksen ja väärinkäytöksen riskiä. Arvioinnissa on huomioitava tunnistusmenetelmän varmuustason mukaisesti kohtuullinen tai korkea hyökkäyspotentiaali, kuten muissakin kohdissa

37.	S,H	Tietojärjestelmäturvallisuus: Tunnistusjärjestelmän **kovennuksista** huolehditaan; käytössä on menettelytapa, jolla järjestelmät asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus. Tunnistusjärjestelmässä käytetään **vain** sen toiminnan kannalta **tarvittavia** palveluita, toimintoja, prosesseja, laitteita ja komponentteja. Niiden käyttö on määritelty siten, että asennuksesta on poistettu kaikki tarpeettomat oikeudet ja toiminnot/elementit.	**M72A 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet** Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän 2) tietojärjestelmäturvallisuus c) järjestelmien koventaminen	A.12.5. tuotantokäytössä olevien ohjelmistojen hallinta	ks. myös tietoliikenne Ohjeessa 211/2016 oli seuraavia kriteereitä, jotka ovat tässä mukana informatiivisina: Kovennettu asennus sisältää vain sellaiset komponentit ja palvelut, sekä käyttäjien ja prosessien oikeudet, jotka ovat välttämättömiä toimintavaatimusten täyttämiseksi ja turvallisuuden varmistamiseksi Käyttöön on otettu vain käyttövaatimusten ja tietojen käsittelyn kannalta olennaiset toiminnot, laitteet ja palvelut
38.	S, H	Tietojärjestelmäturvallisuus: Tunnistusjärjestelmässä huolehditaan **haittaohjelmien** aiheuttamien haittojen ja uhkien havaitsemisesta, ennaltaehkäisystä, estämisestä ja korjaamisesta.	**M72A 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet** Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän 2) tietojärjestelmäturvallisuus d) haittaohjelmasuojaus	A.12.2 haittaohjelmilta suojautuminen A.12.6. teknisten haavoittuvuuksien hallinta	Ks. myös poikkeamien havainnointikyky

39.	S, H	Tietojärjestelmäturvallisuus: Tunnistusjärjestelmässä käytetään kaikilta osin suositeltavia **salausratkaisuja**.	**M72A 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet** Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän 2) tietojärjestelmäturvallisuus g) kansainvälisesti tai kansallisesti suositellut salausratkaisut muutoin kuin määräyksen 72 7 §:ssä säädetyltä osin	A.10.1 salauksen käytön periaatteet A.18.1.5 salaustekniikan hallintaa koskevat säädökset	MPS72:ssa mainitaan lähteinä seuraavia: SOGIS-MRA NCSA-FI NIST Enisa SANS Ohjeessa 211/2016 oli seuraavia huomioita, jotka ovat tässä mukana informatiivisina: 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)
40.	S,H	Tietojärjestelmäturvallisuus: Salaustekninen aineisto on suojattu koko elinkaaren ajan	**LOA 2.4.6 Tekniset tarkastukset** 3) Pääsy arkaluonteiseen salaustekniseen aineistoon, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, rajoitetaan tiukasti niihin tehtäviin ja sovelluksiin, jotka edellyttävät tällaista pääsyä. On	A.8.2.1 tiedon luokittelu A.10.1.1 salauksen	Ohjeessa 211/2016 oli seuraavia huomioita, jotka ovat tässä mukana informatiivisina:

			varmistettava, ettei tällaista aineistoa koskaan tallenneta pysyväisluonteisesti ilmitekstinä. Arkaluonteinen salaustekninen aineisto, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, on suojattu luvattomalta käsittelyltä. **M72A 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet** Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän 2) tietojärjestelmäturvallisuus a) pääsyoikeuksien hallinta b) järjestelmien käyttäjien tunnistaminen g) kansainvälisesti tai kansallisesti suositellut salausratkaisut muutoin kuin 7 §:ssä säädetyltä osin 3) käyttöturvallisuus b) salassa pidettävän aineiston käsittely-ympäristö	käytön periaatteet A.10.1.2 salausavainten hallinta	Salaiset avaimet ovat vain valtuutettujen käyttäjien ja prosessien käytössä Salausavaintenhallinnan prosessit ja käytännöt ovat dokumentoituja ja asianmukaisesti toteutettuja 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)

5.3.3 Käyttöturvallisuus

3.3 Käyttöturvallisuus

NRO	VAR-MUUS TASO	TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ	SÄÄNNÖKSET	STANDAR-DIVIIT-TAUS	HUOMIOITA
41.	**S,H**	Käyttöturvallisuus: Tunnistusjärjestelmän **muutostenhallinta** on suunniteltua ja huolellista.	**M72A 5 § Tunnistusjärjestelmän tekniset tietoturva-toimenpiteet** Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän 3) käyttöturvallisuus a) muutosten hallinta	A.12.1.2 käyttötur-valli-suus/toi-mintaoh-jeet ja vel-vollisuudet: muutok-senhallinta A.14.2.2 järjestel-mien hank-kiminen, kehittämi-nen ja ylläpito/kehi-tys- ja tuki-prosessien turvalli-suus: jär-jestelmään tehtävien	Muutosten hallintaan määriteltynä selkeät prosessit

				muutosten hallintamenettelyt A.14.2.3 sovellusten tekninen katselmointi käyttöalustan muutosten jälkeen A.14.2.4 ohjelmistopakettien muutoksia koskevat rajoitukset	
42.	S,H	Käyttöturvallisuus: Tunnistusjärjestelmän **ohjelmistohaavoittuvuuksien** hallinta on suunnitelmallista. Tunnistusjärjestelmässä huolehditaan **ohjelmistohaavoittuvuuksien** aiheuttamien	**M72A 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet** Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän 3) käyttöturvallisuus c) ohjelmistohaavoittuvuuksien hallinta	A.12.5.1 käyttöturvallisuus: ohjelmistojen asentaminen tuo-	Ohjeessa 211/2016 oli seuraavia huomioita, jotka ovat tässä mukana informatiivisina: Organisaatiolla tulee olla menetelmä yleisten haavoittuvuuksien seurantaan

		haittojen ja uhkien havaitsemisesta, ennaltaehkäisystä, estämisestä ja korjaamisesta.		tantokäytössä oleviin järjestelmiin A.12.6.1 käyttöturvallisuus: teknisten haavoittuvuuksien hallinta A.14.2. järjestelmien hankkiminen, kehittäminen ja ylläpito/kehitys- ja tukiprosessien turvallisuus A.14.2.1 turvallisen	Tunnistusjärjestelmässä käytettävien ohjelmistojen tulee noudattaa turvallisen ohjelmoinnin periaatteita.

				kehittämisen politiikka A.14.2.2 järjestelmään tehtävien muutosten hallintamenettelyt A.14.2.3 sovellusten tekninen katselmointi käyttöalustan muutosten jälkeen A.14.2.4 ohjelmistopakettien muutoksia	

				koskevat rajoitukset A.14.2.5 turvallisen järjestelmän suunnittelun periaatteet A.14.2.6 turvallinen kehitysympäristö A.14.2.7 ulkoistettu kehittäminen A.14.2.8 järjestelmän turvallisuustestaus	

				A.14.2.9 järjestelmän hyväksymistestaus	
43.	S,H	Käyttöturvallisuus: Tunnistusjärjestelmän **varmuuskopioinnista** huolehditaan suunnitelmallisesti. Varmuuskopioinnissa huomioidaan tiedon luokittelu (henkilötiedot, salaustekniset tiedot jne.), järjestelmien palautettavuus ja varmuuskopioiden säilytys.	**M72A 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet** Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän 3) käyttöturvallisuus d) varmuuskopiointi	A.12.3.1 tietojen varmuuskopiointi	Ohjeessa 211/2016 oli seuraavia huomioita, jotka ovat tässä mukana informatiivisina: Varmuuskopioiden fyysinen sijoituspaikka on riittävän eriytetty varsinaisesta järjestelmästä.

5.4 Poikkeamien havainnointikyky ja hallinta ja häiriöilmoitukset

4 Poikkeamien havainnointikyky ja hallinta ja häiriöilmoitukset

KESKEISET SÄÄNNÖKSET

M72A 15 § Arviointikriteerit
Tunnistuspalvelun arvioinnin täytyy kattaa 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 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.
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 salassapitosäännösten estämättä ilmoitettava ilman aiheetonta 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 tarkoitetussa ilmoituksessa on kerrottava niistä toimista, joita eri tahoilla on käytettävissään uhkien tai häiriöiden torjumiseksi sekä näistä toimenpiteistä aiheutuvista arvioiduista kustannuksista.

…

Vaatimuksia on tarkennettu M72 5 §:ssä ja 11 §:ssä

Liikenne- ja viestintävirasto

Erik Palmeninaukio 1
PL 313
00059 TRAFICOM
Puhelin 0295 390 100
www.traficom.fi

NRO	VAR-MUUS-TASO	TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ	SÄÄNNÖKSET	STANDAR-DIVIIT-TAUS	HUOMIOITA
44.	S, H	Tunnistusjärjestelmän poikkeamien havaitsemiseen on **kyvykkyys** ja ennalta **määritellyt prosessit**. Määrittelyissä huomioidaan järjestelmän tietoliikenneyhteyksien ja tietojärjestelmien komponenttien ja prosessien tärkeys/kriittisyys/luokittelu ja se, että turvallisuuteen liittyvät/vaikuttavat tapahtumat kyetään jäljittämään myös jälkikäteen. Tunnistusjärjestelmässä kerätään ja tallennetaan **tapahtumalokeja** ja¨rjestelma¨n toiminnasta ja tietoturvaan vaikuttavista/liittyvista¨ tapahtumista ja poikkeamista.	**M72 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet** Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän 1) tietoliikenneturvallisuus d) suodatuksen ja valvontajärjestelmien hallinnointi koko elinkaaren ajan 2) tietojärjestelmäturvallisuus e) turvallisuuteen liittyvien tapahtumien jäljitys f) poikkeamien havainnointikyky ja toipuminen	A.12.4.1 käyttöturvallisuus: tapahtumien kirjaaminen A.12.4.2 käyttöturvallisuus: lokitietojen suojaaminen A.12.4.3 käyttöturvallisuus: pääkäyttäjä- ja operaattorilokit	

Liikenne- ja viestintävirasto

Erik Palmeninaukio 1
PL 313
00059 TRAFICOM
Puhelin 0295 390 100
www.traficom.fi

				A.16.1 tietoturvahäiriöiden hallinta/tietoturvahäiriöiden ja tietoturvallisuuden parannusten hallinta A. 16.1.1 vastuut ja menettelyt A.16.1.6 tietoturvahäiröistä oppiminen	
45.	S, H	Tunnistusjärjestelmän **hallintalokit** on määritelty ja eriytetty muista lokeista. Niiden eheydestä on huolehdittu.	**Tunnistusjärjestelmän tietoturvallisuuden ylläpitämistä koskevat vaatimukset säädetään TunnL 8 §:ssä ja LoA 2.4.6 kohdassa.** **M72 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet** Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän	A.12.4.1 käyttötur-vallisuus: tapahtumien kirjaaminen	hallintalokeihin tallennetaan tiedot tunnistusjärjestelmässä tehtävistä muutoksista

			1) tietoliikenneturvallisuus d) suodatuksen ja valvontajärjestelmien hallinnointi koko elinkaaren ajan 2) tietojärjestelmäturvallisuus e) turvallisuuteen liittyvien tapahtumien jäljitys f) poikkeamien havainnointikyky ja toipuminen	A.12.4.2 käyttöturvallisuus: lokitietojen suojaaminen A.12.1.4 kehitys-, testaus- ja tuotantoympäristöjen erottaminen	
46.	S, H	Tunnistusjärjestelmän toimintaa, muutoksia ja tapahtumalokeja **monitoroidaan** poikkeamien ja tietoturvaloukkausten havaitsemiseksi. Tunnistusjärjestelmän **poikkeamat ja häiriöt käsitellään ja analysoidaan** ja niiden vaikuttavuus/vakavuus luokitellaan suunnitelmallisesti.	**M72 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet** Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän 1) tietoliikenneturvallisuus d) suodatuksen ja valvontajärjestelmien hallinnointi koko elinkaaren ajan 2) tietojärjestelmäturvallisuus f) poikkeamien havainnointikyky ja toipuminen	A.16.1 tietoturvahäiriöiden hallinta/tietoturvahäiriöiden ja parannusten hallinta: A.16.1.2 tietoturvatapahtumien raportointi	Ohjeessa 211/2016 oli seuraavia huomioita, jotka ovat tässä mukana informatiivisina: Kaikki havainnot käsitellään ja niiden vaikuttavuus luokitellaan sovittujen menetelmien mukaan

Liikenne- ja viestintävirasto

Erik Palmeninaukio 1
PL 313
00059 TRAFICOM
Puhelin 0295 390 100
www.traficom.fi

				A.16.1.3 tietoturva-heikkouk-sien rapor-tointi A.16.1.4 tietoturva-tapahtu-mien arvi-ointi ja niitä koskevien päätösten tekeminen	
		Tunnistusjärjestelmän poikkeamien ja häiri-öiden edellyttämät **korjaavat toimenpiteet** ovat suunnitelmallisia ja tehokkaita. Toiminnan jatkuvuussuunnittelu sisältää en-nalta¨ ehka¨isevia¨ ja korjaavia toimenpi-teita¨, joilla minimoidaan merkitta¨vien toi-mintaha¨irio¨iden tai poikkeuksellisten tapah-tumien vaikutukset.	**M72 5 § Tunnistusjärjestelmän tekniset tietoturva-toimenpiteet** Tunnistusjärjestelmä on suunniteltava¸ toteutettava ja yl-läpidettävä siten, että huomioidaan järjestelmän 1) tietoliikenneturvallisuus d) suodatuksen ja valvontajärjestelmien hallinnointi koko elinkaaren ajan 2) tietojärjestelmäturvallisuus f) poikkeamien havainnointikyky ja toipuminen	A.16.1. tie-toturvahäi-riöiden hal-linta/tieto-turvahäiri-öiden ja pa-rannusten hallinta: A.16.1.5 tietoturva-häiriöihin	Saatavuusvaatimukset (SLA) ovat sopimusasia, huomioitava syrji-mättömyys

				vastaaminen	
47.	S, H	Häiriönhallintaprosesseissa on huomioitu **ilmoitusvelvollisuus muille luottamusverkostoon kuuluville tunnistuspalveluille.**	**TunnL 16 § Tunnistuspalvelun tarjoajan velvollisuus ilmoittaa toimintaan ja tietojen suojaamiseen kohdistuvista uhkista tai häiriöistä** Tunnistuspalvelun tarjoajan on salassapitosäännösten estämättä ilmoitettava ilman aiheetonta viivästystä …tunnistuspalveluunsa muille luottamusverkostossa toimiville sopimuspuolilleen …palvelun toimivuuteen, tietoturvaan tai sähköisen henkilöllisyyden käyttöön kohdistuvista merkittävistä uhkista tai häiriöistä. … Tunnistuspalvelun tarjoaja voi salassapitosäännösten estämättä ilmoittaa kaikille luottamusverkoston jäsenille 1 momentissa tarkoitetuista uhkista ja häiriöistä sekä palvelun tarjoajista, joiden on syytä epäillä tavoittelevan oikeudetonta taloudellista hyötyä, antavan merkityksellisiä totuudenvastaisia tai harhaanjohtavia tietoja tai käsittelevän henkilötietoja lainvastaisesti. **Soveltaminen:** Luottamusverkoston yhteistoimintaryhmässä on laadittu yhteinen käytäntö keskinäisistä häiriöilmoitustilanteista ja ilmoituskynnyksistä.	A.16.1.2 tietoturvahäiriöiden hallinta/tietoturvahäiriöiden ja parannusten hallinta: tietoturvatapahtumien raportointi	Vastuut poikkeamatilateisiin ja sidosryhmäviestintään on määritelty

48.	S, H	Häiriönhallintaprosesseissa on huomioitu **ilmoitusvelvollisuus käyttäjille ja luottaville osapuolille.**	**TunnL 16 § Tunnistuspalvelun tarjoajan velvollisuus ilmoittaa toimintaan ja tietojen suojaamiseen kohdistuvista uhkista tai häiriöistä** Tunnistuspalvelun tarjoajan on…ilmoitettava ilman aiheetonta 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 arvioiduista kustannuksista.	A.16.1.2 tietoturvahäiriöiden hallinta/tietoturvahäiriöiden ja parannusten hallinta: tietoturvatapahtumien raportointi	Vastuut poikkeamatilateisiin ja sidosryhmäviestintään on määritelty Luottavilla osapuolilla tarkoitetaan asiointipalveluita
49.	S, H	Häiriönhallintaprosesseissa on huomioitu **ilmoitusvelvollisuus Liikenne- ja viestintävirastolle**	**TunnL 16 § Tunnistuspalvelun tarjoajan velvollisuus ilmoittaa toimintaan ja tietojen suojaamiseen kohdistuvista uhkista tai häiriöistä** Tunnistuspalvelun tarjoajan on salassapitosäännösten estämättä ilmoitettava ilman aiheetonta 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 arvioiduista kustannuksista.	A.16.1.2 tietoturvahäiriöiden hallinta/tietoturvahäiriöiden ja parannusten hallinta: tietoturvatapahtumien raportointi	Vastuut poikkeamatilateisiin ja sidosryhmäviestintään on määritelty

			M72 11 § Tunnistuspalveluntarjoajan häiriöilmoitukset Viestintävirastolle Viestintävirastolle tunnistus- ja luottamuspalvelulain 16 §:n mukaisesti tehtävässä merkittävää uhkaa tai häiriötä koskevassa ilmoituksessa on annettava vähintään seuraavat tiedot: 1) tunnistusväline tai välityspalvelu, johon häiriö vaikuttaa; 2) kuvaus häiriöstä ja sen tiedossa olevista syistä; 3) kuvaus häiriön vaikutuksista, mukaan lukien vaikutus uusien tunnistusvälineiden myöntämiseen, käyttäjiin, luottaviin osapuoliin, muihin luottamusverkoston toimijoihin ja rajat ylittävään käyttöön; 4) kuvaus korjaustoimenpiteistä; sekä 5) kuvaus häiriöstä tiedottamisesta luottaville osapuolille, tunnistusvälineiden haltijoille, luottamusverkostolle ja tieto ilmoittamisesta muille viranomaisille. Häiriön merkittävyyden arvioinnissa merkittävyyttä lisää se, että häiriö liittyy sähköisen henkilöllisyyden virheellisyyteen tai väärinkäyttöön tai tietoturvauhkaan tai -häiriöön, joka vaarantaa tunnistamisen eheyden ja luotettavuuden. Merkittävyyttä lisää myös se, että häiriöllä on vaikutuksia luottamusverkostoon.		

Liikenne- ja viestintävirasto

Erik Palmeninaukio 1
PL 313
00059 TRAFICOM
Puhelin 0295 390 100
www.traficom.fi

			MPS72 soveltamisohje ilmoituskynnyksestä Liikenne- ja viestintävirastolle, 11 §:n perustelut: Pykälän 2 momentissa määritellään yleisellä tasolla niitä tekijöitä, jotka ovat olennaisia häiriön merkittävyyden eli ilmoituskynnyksen kannalta. Tällaisia merkittäviä häiriöitä ovat muun muassa: - tunnistusvälineen myöntäminen väärälle henkilölle - sellaiset sulkulistojen toimivuuteen liittyvät häiriöt, joissa ajantasaista sulkulistaa ei ole saatavilla - tunkeutumiset palveluntarjoajan järjestelmiin - tunnistusvälineen tarjoajan varmenteiden allekirjoitusavaimien paljastumiset - tunnistusvälineiden vakavat väärinkäytökset kuten tapaukset, jotka liittyvät tunnusten ketjuttamiseen - vakavat sisäiset väärinkäytökset. Sähköisen henkilöllisyyden virheitä tai väärinkäytöksiä pidetään merkittävinä hyvin matalalla kynnyksellä, samoin esimerkiksi haavoittuvuuksia tai virheitä, jotka vaarantavat tunnistamistiedon oikeellisuuden. Sen sijaan käytettävyys- tai laatuongelmien ilmoituskynnys on lähtökohtaisesti korkeampi ja niiden merkittävyyttä lisää lähinnä se, että ongelma vaikuttaa muihin luottamusverkoston toimijoihin.		

5.5 Tietojen säilyttäminen ja käsittely

5 Tietojen säilyttäminen ja käsittely

M72A 15 § Arviointikriteerit
Tunnistuspalvelun arvioinnin täytyy kattaa vaatimukset, jotka kohdistuvat:
1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän)
b) tietojen säilyttämiseen
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 tietosuojaan 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) 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 tietoturvallisuusuhat

Liikenne- ja viestintävirasto

Erik Palmeninaukio 1
PL 313
00059 TRAFICOM
Puhelin 0295 390 100
www.traficom.fi

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. Arkaluonteinen salaustekninen aineisto, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, on suojattu luvattomalta käsittelyltä.					
NRO	**VAR-MUUS-TASO**	**TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ**	**SÄÄNNÖKSET**	**STANDAR-DIVIIT-TAUS**	**HUOMIOITA**
50.	S, H	Tunnistusjärjestelmään ja tunnistamiseen liittyvien **tietojen hallinta on suunnitelmallista** ja perustuu **tietojen luokitteluun.**	**LOA Liite 2.4.4 Tietojen säilyttäminen** 1. Asiaankuuluvat tiedot kirjataan ja säilytetään käyttämällä tehokasta tiedonhallintajärjestelmää ottaen huomioon sovellettava lainsäädäntö ja tietosuojaan ja tietojen säilyttämiseen liittyvät hyvät käytännöt. **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. Arkaluonteinen salaustekninen aineisto, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, on suojattu luvattomalta käsittelyltä.	A.8.2.1 suojattavan omaisuuden hallinta/tietojen luokittelu: tiedon luokittelu A.18.1.4 vaatimustenmukaisuus/lainsäädäntöön ja sopimuksiin sisälty-	Luokittelussa huomioidaan esim. salaustekniset tiedot, tunnistustapahtumatiedot, henkilötiedot, liikesalaisuudet ja järjestelmien turvallisuuteen vaikuttavat tiedot.

				vien vaatimusten noudattaminen: tietosuoja ja henkilötietojen suojaaminen	
51.	S, H	Tiedonhallinnan suunnittelussa on huomioitu tiedon koko **elinkaari**. Tietojen **säilytysajat** on määritelty.	**LOA Liite 2.4.4 Tietojen säilyttäminen** 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 tietoturvalouk-kausten tutkimista varten ja säilytetään siihen asti, kun tiedot hävitetään turvallisesti.	A.18.1.4 vaatimustenmukaisuus/lainsäädäntöön ja sopimuksiin sisältyvien vaatimusten noudattaminen: tietosuoja ja henkilötietojen suojaaminen	Huomioon on otettava mm. turvallisuuteen liittyvien tapahtumien jäljitettävyys ja tunnistuslain 24 §:ää *vastaavien* käsittelyperusteiden aiheuttamat tarpeet. Ohjeessa 211/2016 oli seuraavia huomioita, jotka ovat tässä mukana informatiivisina: Lokeille pitää määritellä säilöntään riittävän pitkä aika jälkikäteen tapahtuvaa selvitystä varten
52.	S, H	Tunnistuslain **24 §:ssä säädetyistä erityisistä tallennusvelvollisuuksista** on huolehdittu.	**TunnL 24 § Tunnistustapahtumaa ja tunnistusvälinettä koskevien tietojen tallentaminen ja käyttö** Tunnistuspalvelun tarjoajan on tallennettava:	A.12.4.1 käyttöturvallisuus:	"*…ainoastaan laskee liikkeelle tunnistusvälineitä*" tarkoittaa säännöksessä VRK:n varmenteen kaltaista tunnistuspalvelua, jossa

			1) yksittäisen tunnistustapahtuman ja sähköisen allekirjoittamisen tapahtuman todentamiseksi tarvittavat tiedot; 2) tiedot 18 §:ssä tarkoitetuista tunnistusvälineen käyttöön liittyvistä estoista ja käyttörajoituksista; 3) varmenteen osalta 19 §:ssä tarkoitetun varmenteen tietosisältö. Tunnistusvälineen tarjoajan on tallennettava tarvittavat tiedot 17 ja 17 a §:ssä tarkoitetusta hakijan ensitunnistamisesta ja siinä käytetystä asiakirjasta tai sähköisestä tunnistamisesta. Edellä 1 momentin 1 kohdassa tarkoitetut tiedot on säilytettävä viiden vuoden ajan tunnistustapahtumasta. Muut 1 ja 2 momentissa tarkoitetut tiedot on säilytettävä viiden vuoden ajan vakituisen asiakassuhteen päättymisestä. Tunnistustapahtuman yhteydessä syntyneet henkilötiedot on hävitettävä tunnistustapahtuman jälkeen, jollei tallentaminen ole välttämätöntä yksittäisen tunnistustapahtuman todentamiseksi. Tunnistuspalvelun tarjoaja saa käsitellä tallennettuja tietoja ainoastaan palvelun toteuttamiseksi ja ylläpitämiseksi, laskutusta varten, omien oikeuksiensa turvaamista varten riitatilanteissa, väärinkäytöstilanteiden selvittämisessä sekä tunnistuspalvelua käyttävän palvelun-	tapahtumien kirjaaminen	tunnistusvälineen myöntäjä ei välitä tunnistussanomia tunnistustapahtumassa

			tarjoajan tai tunnistusvälineen haltijan pyynnöstä. Tunnistuspalvelun tarjoajan on tallennettava tieto käsittelyn ajankohdasta, syystä ja käsittelijästä. Jos palveluntarjoaja ainoastaan laskee liikkeelle tunnistusvälineitä: 1) 1 momentin 1 kohtaa ja 4 momenttia ei sovelleta siihen; 2) 3 momentissa tarkoitettu viiden vuoden tallennusaika lasketaan tunnistusvälineen voimassaolon päättymisestä.		
53.	S, H	Tunnistuslain **24 §:n erityisvaatimus** tallennettavaksi säädettyjen tietojen käsittelyyn liittyvien tietojen tallentamisesta.	**Tunnistustapahtumiin ja tunnistuspalveluun liittyvästä käsittelystä säädetään TunnL 24 §:ssä.** **TunnL 24 §** **…** Tunnistuspalvelun tarjoaja saa käsitellä tallennettuja tietoja ainoastaan palvelun toteuttamiseksi ja ylläpitämiseksi, laskutusta varten, omien oikeuksiensa turvaamista varten riitatilanteissa, väärinkäytöstilanteiden selvittämisessä sekä tunnistuspalvelua käyttävän palveluntarjoajan tai tunnistusvälineen haltijan pyynnöstä. Tunnistuspalvelun tarjoajan on tallennettava tieto käsittelyn ajankohdasta, syystä ja käsittelijästä.	A.12.4.1 käyttöturvallisuus: tapahtumien kirjaaminen A. A.12.4.3 Pääkäyttäjä- ja operaattorilokit	huomioitava käsittelytietojen jäljitettävyys ja lokien eheyden turvaaminen

54.	S, H	Tunnistusjärjestelmässä **käsiteltävien ja säilytettävien tietojen eheydestä ja luottamuksellisuudesta on huolehdittu teknisillä toimenpiteillä.**	**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 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. Arkaluonteinen salaustekninen aineisto, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, on suojattu luvattomalta käsittelyltä. **M72 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet** Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän 3) käyttöturvallisuus	A.9.1.1 pääsynhallintapolitiikka A.9.1.2 pääsy verkkoihin ja verkkopalveluihin A.10.1.1 salauksen käytön periaatteet A.12.4.2 käyttöturvallisuus: lokitietojen suojaaminen	tiedon salaus ja/tai pääsynhallinta eriyttäminen tarvittaessa (vrt. erityisesti salaustekninen aineisto) varmuuskopiointi/palautettavuus suosituksessa salausvaatimuksille määritelty avaintenvaihto voi olla relevantti tunnistuspalvelun ja sen alihankkijan välillä, vaikka se ei ole relevantti levysalauksessa

			b) salassa pidettävän aineiston käsittely-ympäristö d) varmuuskopiointi **M72 7 § Tunnistusjärjestelmän ja rajapintojen salausvaatimukset** […] Salauksessa, avaintenvaihdossa sekä salaukseen liittyvässä allekirjoituksessa on noudatettava seuraavia menetelmiä: **1) Avaintenvaihto:** Avaintenvaihdossa on käytettävä DHE -menetelmiä tai elliptisiä käyriä käyttäviä ECDHE -menetelmiä. Laskutoimituksissa käytetyn äärellisen kunnan (finite field) koon tulee olla DHE -menetelmässä vähintään 2048 bittiä ja ECDHE -menetelmässä vähintään 224 bittiä. **2) Allekirjoitus**: Käytettäessä RSA:ta sähköiseen allekirjoitukseen, avaimen pituuden tulee olla vähintään 2048 bittiä. Käytettäessä elliptisen käyrän menetelmää ECDSA:ta alla olevan kunnan koon tulee olla vähintään 224 bittiä. **3) Symmetrinen salaus**: Salausalgoritmin on oltava AES tai Serpent. Avaimen pituuden tulee olla vähintään 128 bittiä. Salausmoodin on oltava CBC, GCM, XTS tai CTR.		

			4) Tiivistefunktiot: Tiivistefunktion on oltava SHA-2, SHA-3 tai Whirlpool. SHA-2:lla tarkoitetaan funktioita SHA224, SHA256, SHA384 ja SHA512. […] Tunnistusjärjestelmässä säilytettävien tietojen eheydestä ja luottamuksellisuudesta on huolehdittava. Jos tiedon suojaaminen perustuu ainoastaan niiden salaukseen, sovelletaan edellä 1 momentissa allekirjoittamisen, symmetrisen salaamisen ja tiivistefunktioiden vaatimuksia. **MPS72 soveltamisohje**: Jos suojattavia tietoja säilytetään järjestelmissä siten, että niiden luottamuksellisuutta ja/tai eheyttä suojataan ainoastaan tai pääasiassa kryptografisin menetelmin, on käytettävä 1 momentissa määriteltyjä menetelmiä lukuun ottamatta avaintenvaihdon vaatimuksia. Ne eivät sovellu, koska levysalauksessa ei tyypillisesti käytetä avaintenvaihtoa. Vaihtoehtoisesti voidaan hyödyntää esimerkiksi huolellista pääsynhallintaa.		
55.	H	Tietojen käsittelyssä ja säilyttämisessä noudatetaan **suosituksen** mukaisia tiukennettuja/korkean tason salausvaatimuksia.	**MPS72 kohta B 7.2 suositus** Korkealla varmuustasolla tunnistusjärjestelmässä suositellaan sovellettavaksi määräyksessä 7 §:n 1 momentissa edellytettyjen korotetun varmuustason vaatimusten sijaan seuraavassa esitettyjä suluissa olevia arvoja:	ks. yllä	avaintenvaihto voi olla relevantti tunnistuspalvelun ja sen alihankkijan välillä

			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 (korkealla varmuustasolla **3072**) bittiä ja ECDHE-menetelmässä vähintään 224 (korkealla varmuustasolla **256**) bittiä. IANA:n IKEv2-määritysten mukaiset DH-ryhmät 14 - 21, 23, 24 ja 26 (korkealla varmuustasolla ***15 - 21***) toteuttavat edellä mainitut edellytykset. 2) **Allekirjoitus**: Käytettäessä RSA:ta sähköiseen allekirjoitukseen, avaimen pituuden tulee olla vähintään 2048 (korkealla varmuustasolla 3072) bittiä. Käytettäessä elliptisen käyrän menetelmää ECDSA:ta, alla olevan kunnan koon tulee olla vähintään 224 (korkealla varmuustasolla 256) bittiä. 3) **Symmetrinen salaus**: Salausalgoritmin on oltava AES tai Serpent *(korkealla varmuustasolla AES tai Serpent)*. Avaimen pituuden tulee olla vähintään 128 (korkealla varmuustasolla 128) bittiä. Salausmoodin on oltava CBC, GCM, XTS tai CTR. 4) **Tiivistefunktiot**: Tiivistefunktion on oltava SHA-2, SHA-3 tai Whirlpool. SHA-2:lla tarkoitetaan funktioita		

			SHA224, SHA256, SHA384 ja SHA512 (korkealla varmuustasolla *SHA256, SHA384, SHA512 ja SHA-3*)		
56.	S, H	Kaikki **laitteet ja välineet**, jotka sisältävät henkilötietoja, salattuja tietoja tai muita arkaluonteisia tietoja, säilytetään, kuljetetaan ja hävitetään turvallisella ja varmalla tavalla.	**LOA Liite 2.4.6 Tekniset tarkastukset** (controls) 5) Kaikki laitteet ja välineet, jotka sisältävät henkilötietoja, salattuja tietoja tai muita arkaluonteisia tietoja, säilytetään, kuljetetaan ja hävitetään turvallisella ja varmalla tavalla.	A.8.3 Suojattava omaisuus/tietovälineiden käsittely A.11.2.6 toimitilojen ulkopuolelle vietyjen laitteiden ja suojattavan omaisuuden turvallisuus A.11.2.7 laitteiden turvallinen käytöstä	hallinta, hävittäminen, siirtäminen

				poistami-nen ja kier-rättäminen	

5.6 Tilaturvallisuus

6. Tilaturvallisuus

M72A 15 § Arviointikriteerit
Tunnistuspalvelun arvioinnin täytyy kattaa 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 varmuustasoasetuksen liitteen kohdassa 2.4.5 säädetyllä tavalla;

NRO	VAR-MUUS TASO	TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ	SÄÄNNÖKSET	STANDAR-DIVIIT-TAUS	HUOMIOITA
57.	S, H	**Tilaturvallisuus**	**LOA Liite 2.4.5 Tilat ja henkilökunta**	A.11.1 fyy-sinen tur-vallisuus ja	Kaikki tunnistuspalvelun tuotan-toon liittyvät/vaikuttavat tilat, myös alihankkijat

		Tunnistusjärjestelmän tilat on jaettu turvavyöhykkeisiin käsiteltävän tiedon luottamuksellisuus ja kriittisyys huomioiden.	3. Palvelun tarjoamiseen käytetyt tilat ovat jatkuvasti seurattuja ja suojattuja ympäristötapahtumien aiheuttamilta vahingoilta, luvattomalta käytöltä ja muilta tekijöiltä, jotka voivat vaikuttaa palvelun turvallisuuteen. 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.	ympäristön turvallisuus/turva-alueet: A.11.1.1 fyysinen turva-alue	Mahdollinen Katakrin täyttäminen oletusarvoisesti riittävä, jos tunnistusjärjestelmän tuottaminen ko. tiloissa. Muiden standardien kattavuutta ei ole selvitetty.
58.	S, H	Tunnistuspalvelun tuotannossa käytettävät laitteistot **on suojattu** murtoa, ilkivaltaa, paloa, lämpöä, kaasuja, pölyä, tärinää, vettä ja sähkönkäytön katkoksia vastaan. Suojauksen vahvuudessa on huomioitu turvavyöhykkeet. Tiloissa on toteutettu tarkoituksenmukainen **kulunvalvonta**/pääsynvalvonta jolla varmistutaan siitä, että vain asianomaisilla henkilöillä on pääsy. Tietojen fyysiseen suojaamiseen tarkoitetut turvallisuusjärjestelmät ja laitteet ovat yleisesti käytettyjen teknisten standardien tai vaatimusten mukaisia.	**LOA Liite 2.4.5 Tilat ja henkilökunta** 3. Palvelun tarjoamiseen käytetyt tilat ovat jatkuvasti seurattuja ja suojattuja ympäristötapahtumien aiheuttamilta vahingoilta, luvattomalta käytöltä ja muilta tekijöiltä, jotka voivat vaikuttaa palvelun turvallisuuteen. 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.11.1.2 kulunvalvonta A.11.1.3 toimistojen, tilojen ja laitteistojen suojaus, A.11.1.4 suojaus ulkoisia ja ympäristön	

				aiheuttamia uhkia vastan A.11.2.1 laitteiden sijoitus ja suojaus A.11.2.3 kaapeloinnin turvallisuus	
59.	S, H	Turvavyöhykkeillä huolehditaan siitä, ettei niillä ole **asiaankuulumattomia** laitteita tai yhteyksiä.	**LOA Liite 2.4.5 Tilat ja henkilökunta** 3. Palvelun tarjoamiseen käytetyt tilat ovat jatkuvasti seurattuja ja suojattuja ympäristötapahtumien aiheuttamilta vahingoilta, luvattomalta käytöltä ja muilta tekijöiltä, jotka voivat vaikuttaa palvelun turvallisuuteen. 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	

5.7 Riittävät ja pätevät henkilöresurssit

7. Riittävät ja pätevät henkilöresurssit **M72A 15 § Arviointikriteerit** Tunnistuspalvelun arvioinnin täytyy kattaa vaatimukset, jotka kohdistuvat: 1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän) c) […] ja henkilökuntaan					
NRO	**VAR-MUUS TASO**	**TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ**	**SÄÄNNÖKSET**	**STANDAR-DIVIIT-TAUS**	**HUOMIOITA**
60.	S, H	**Henkilökunnan riittävyys ja pätevyys** Tunnistuspalvelun tuotanto-organisaatiolla on käytössään riittävä asiantuntemus ja henkilöstöresurssit tietoturvallisuuden ja tietosuojan varmistamiseksi.	**TunnL 13 § Tunnistuspalvelun tarjoajan yleiset velvollisuudet** Tunnistuspalvelun tarjoajan tunnistamiseen liittyvien … henkilökunnan ja alihankintana käyttämien palvelujen tulee täyttää sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdissa …ja 2.4.5 vähintään korotetulle varmuustasolle säädetyt vaatimukset. **LOA Liite 2.4.5 Tilat ja henkilökunta** Vaatimukset, jotka koskevat tiloja ja henkilöstöä sekä tarvittaessa alihankkijoita, jotka suorittavat tämän asetuksen	A.7.2.2 Henkilöstö-turvalli-suus/työ-suhteen ai-kana: Tie-toturvatie-toisuus, -opastus ja -koulutus	Arviointi - henkilöresurssien riittävyys toiminnan luonteeseen nähden (24/7/365) - tekniset valvontajärjestelyt huomioidaan, ei tarkkoja vaatimuksia henkilöstömäärälle tai päivystykselle - tarpeellisten osa-alueiden osaamisesta (tekninen, oikeudellinen mm. henkilötietojen käsittelyn takia)

			soveltamisalaan kuuluvia tehtäviä. Kunkin vaatimuksen noudattaminen on suhteutettava siihen, minkä tasoinen riski tarjottavaan varmuustasoon liittyy. 1. Käytössä on menettelyt, joilla varmistetaan, että henkilöstöllä ja alihankkijoilla on riittävä koulutus, pätevyys ja kokemus taidoissa, joita he tarvitsevat suorittaakseen tehtävänsä. 2. Käytössä on riittävästi henkilöstöä ja alihankkijoita, jotta palvelua voidaan toteuttaa ja resursoida asianmukaisesti sen toimintaperiaatteiden ja menettelyjen mukaisesti.		
61.	S, H	Tunnistusjärjestelmään alihankitut palvelut ja toiminnot on tunnistettu ja dokumentoitu. Alihankkijoiden henkilöstöresurssien pätevyys ja riittävyys on varmistettu.	**ks. ed. rivi**	ks. ed. rivi A.15.1.1 Toimittajasuhteiden tietoturvapolitiikka A.15.2.1 toimittajien palvelujen seuranta ja katselmointi	Tiedot tunnistusjärjestelmän alihankkijoista (toimistojärjestelmät, käyttöpalvelut, ohjelmistot, infra…) ja vähintään yleisellä tasolla arvio näiden henkilöresursseista.

Liikenne- ja viestintävirasto

Erik Palmeninaukio 1
PL 313
00059 TRAFICOM
Puhelin 0295 390 100
www.traficom.fi

5.8 Tietoturvallisuuden hallinta

8. Tietoturvallisuuden hallinta

M72A 15 § Arviointikriteerit
Tunnistuspalvelun arvioinnin täytyy kattaa vaatimukset, jotka kohdistuvat:
1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän)
a) tietoturvallisuuden hallintaan

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

NRO	VAR-MUUS TASO	TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ	SÄÄNNÖKSET	STANDAR-DIVIIT-TAUS	HUOMIOITA
62.	S, H	Tunnistuspalvelun tarjoajalla on käytössä tehokas **tietoturvallisuuden hallintajärjestelmä** tunnistusjärjestelmän (ml. organisatoriset ja tekniset toimet) tunnistuspalvelun toiminnan tietoturvaan liittyvien riskien hallintaa ja valvontaa varten.	**LOA Liite 2.4.3 Tietoturvallisuuden hallinta** Käytössä on tehokas tietoturvallisuuden hallintajärjestelmä tietoturvaan liittyviä riskien hallintaa ja valvontaa varten. Tietoturvallisuuden hallintajärjestelmässä noudatetaan vakiintuneita standardeja tietoturvaan liittyviä riskien hallintaa ja valvontaa varten.	A.5 tietoturvapolitiikat	ISO 27001 noudattaminen ilman merkittäviä poikkeamia osoittaa tietoturvallisuuden hallinnan vaatimuksen täyttämisen.
63.	S, H	Tietoturvallisuuden hallintajärjestelmä perustuu yleisesti tunnettuun standardiin tai standardeihin	**M72A 4 § Tunnistuspalvelun tarjoajan tietoturvallisuuden hallinnan vaatimukset** Tunnistuspalveluntarjoajan on käytettävä tunnistusjärjestelmän tietoturvallisuuden hallinnassa ISO/IEC 27001 -standardia tai muuta yleisesti tunnettua vastaavaa tietoturvallisuuden hallinnan standardia. Tietoturvallisuuden hallinta voi perustua myös useamman standardin yhdistelmään.		MPS72 4 §:n perusteluissa mäppäys ISO27001:een.

64.	S, H	Tietoturvallisuuden hallintajärjestelmä kattaa tunnistusjärjestelmään vaikuttavat olennaiset sisäiset ja ulkoiset tekniset, oikeudelliset ja hallinnolliset vaatimukset ja tarpeet.	**M72A 4 § Tunnistuspalvelun tarjoajan tietoturvallisuuden hallinnan vaatimukset** Tietoturvallisuuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osa-alueet 1) tunnistuspalveluntarjoajan toimintaympäristö kokonaisuutena;	4 organisaation toimintaympäristö	Tunnistuspalvelussa tulee mm. noudattaa ajantasaisia lainsäädäntöjä ja määräyksiä, kuten tunnistus- ja luottamuspalvelulakia, määräystä 72 ja yleistä tietosuoja-asetusta.
65.	S, H	Tietoturvallisuuden hallintajärjestelmä kattaa hallinnan johtamisen, organisoinnin ja ylläpidon. Käytössä on ajantasainen ja johdon hyväksymä **tietoturvapolitiikka**. Turvallisuusperiaatteet ja politiikat ovat organisaation ja suojattavien kohteiden kannalta kattavat ja tarkoituksenmukaiset. Henkilökunnan ja alihankkijoiden tietoturvallisuuteen liittyvät vastuut on kuvattu.	**M72A 4 § Tunnistuspalvelun tarjoajan tietoturvallisuuden hallinnan vaatimukset** Tietoturvallisuuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osa-alueet 2) tietoturvallisuuden hallinnan johtaminen, organisointi ja ylläpito;	5 johtajuus 9.2 sisäinen auditointi 9.3 johdon katselmus 10 hallintajärjestelmän parantaminen A.5.1.1 Tietoturvapolitiikat	

				A.6.1.1 Tietoturva-roolit ja -vastuut A.15.1.1 toimittaja-suhteiden tietoturva-politiikka	
66.	S, H	Tietoturvallisuuden hallintajärjestelmä kattaa tunnistuspalvelun tarjontaan liittyvien tietoturvallisuusriskien hallinnan. Riskienhallinta on säännöllinen ja jatkuva, dokumentoitu prosessi. Tunnistetut riskit luokitellaan ja priorisoidaan. Riskienhallintaprosessi tunnistaa tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen kohdistuvat riskit. Riskienhallintaprosessia ja sen tuloksia hyödynnetään tunnistuspalvelun/tunnistusjärjestelmän turvatoimien suunnittelussa.	Tietoturvallisuuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osa-alueet 3) tunnistuspalvelun tarjontaan liittyvien tietoturvallisuusriskien hallinta;	MPS72 viittaus: 6 suunnittelu	mitigointi on myös osa tietoturvatoimenpiteitä, jotka ovat edellä

67.	S, H	Tietoturvallisuuden hallintajärjestelmä kattaa tietoturvallisuuden resursoinnin, pätevyysvaatimukset, henkilöstön tietoisuuden tieto-turvallisuudesta, viestinnän ja dokumentoinnin sekä dokumentoidun tiedon hallinnan. Ajantasaiset tietoturvaohjeet ja käytännöt ovat kaikkien sähköisen tunnistamisen tehtäviin osallistuvien saatavilla ja tiedossa Henkilöstön turvallisuuskoulutus on säännöllistä ja dokumentoitua. Koulutuksen tehokkuutta seurataan	Tietoturvallisuuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osa-alueet 4) tietoturvallisuuden resursointi, pätevyys, henkilöstön tietoisuus tieto-turvallisuudesta, viestintä ja dokumentointi sekä dokumentoidun tiedon hallinta;	MPS72: 7 tukitoiminnot	
68.	S, H	Tietoturvallisuuden hallintajärjestelmässä huolehditaan tunnistuspalvelun tarjonnan suunnittelusta ja ohjauksesta siten, että tunnistuspalvelulle säädetyt tietoturvavaatimukset täyttyvät.	Tietoturvallisuuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osa-alueet 5) tunnistuspalvelun tarjonnan suunnittelu ja ohjaus tietoturvavaatimusten täyttämiseksi; ja	MPS72: 8 toiminta A.18.1.1 vaatimustenmukaisuus/lainsäädäntöön ja sopimuksiin sisältyvien vaatimusten nou-	tunnistuspalvelulle säädetyt vaatimukset soveltuvin osin tietosuojasääntely soveltuvin osin luottamusverkoston sopimussääntely

				dattaminen: sovellettavien lakisääteisten ja sopimuksellisten vaatimusten yksilöiminen	
69.	S, H	Tietoturvallisuuden hallintajärjestelmä kattaa tietoturvallisuuden hallinnan tehokkuuden ja toimivuuden säännöllisen arvioinnin.	Tietoturvallisuuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osa-alueet 6) tietoturvallisuuden hallinnan tehokkuuden ja toimivuuden arviointi.	MPS72: 9.1 seuranta, mittaus, analysointi, arviointi	Miten hyvin tietoturvallisuuden hallinta tehoaa/vaikuttaa niihin tekijöihin, prosesseihin ja ongelmiin, jotka vaikuttavat tunnistusjärjestelmän tietoturvallisuuteen

5.9 Tunnistusvälineen hakijan henkilöllisyyden todistaminen ja varmentaminen (ensitunnistaminen)

9. Tunnistusvälineen hakijan henkilöllisyyden todistaminen ja varmentaminen (ensitunnistaminen)

M72A 15 § Arviointikriteerit
Tunnistuspalvelun arvioinnin täytyy kattaa 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 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 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

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 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 tarkoitetun vaatimustenmukaisuuden arviointilaitoksen vahvistuksen perusteella.

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.

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

LOA Liite 1 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)

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.

LOA Liite 1 2.1.3 Henkilöllisyyden todistaminen ja varmentaminen (oikeushenkilö)

LOA Liite 1 2.1.4 Luonnollisten ja oikeushenkilöiden sähköisen tunnistamisen menetelmien välinen kytkös

MÄÄRITELMÄT

TunnL 2 § Määritelmät

7) ensitunnistamisella tunnistusvälineen hakijan henkilöllisyyden todentamista välineen hankkimisen yhteydessä;

Liikenne- ja viestintävirasto

Erik Palmeninaukio 1
PL 313
00059 TRAFICOM
Puhelin 0295 390 100
www.traficom.fi

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;					
NRO	**VAR-MUUS-TASO**	**TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ**	**SÄÄNNÖS**	**STAN-DARDI**	**HUOMIOITA**
Tapa 1: Ensitunnistus perustuu Suomessa hyväksytyn henkilöllisyystodistuksen esittämiseen					
70.	S, H	Henkilöllisyyden todistaminen perustuu tunnistuslaissa hyväksyttyihin henkilöllisyystodistuksiin. Muiden kuin laissa lueteltujen valtioiden myöntämien henkilöllisyystodistuksen hyväksyminen on selkeästi määritelty.	**TunnL 17 §** 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.		Jos käytössä on henkilöllisyystodistuksiin perustuva ensitunnistaminen
71.	S, H	Henkilöllisyystodistus esitetään ja sen aitous tarkistetaan **paikan päällä**. Henkilöstö tuntee henkilöllisyystodistusten aitoustekijät ja pystyy tarkistamaan ne.	**TunnL 17 § Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen** Ensitunnistamisessa luonnollisen henkilön tunnistaminen tulee tehdä henkilökohtaisesti tai sähköisesti siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen		

		Varmistetaan, että henkilöllisyystodistus on sen esittävän henkilön oma.	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. **LOA Liite 1 2.1.2** 1. Henkilöllä on varmennettu olevan hallussaan sen jäsenvaltion hyväksymä todiste ilmoitetusta henkilöllisyydestä, jossa sähköisen tunnistamisen menetelmää haetaan ja todiste on tarkastettu sen varmistamiseksi, että se on aito; tai luotettavasta lähteestä tiedetään sen olevan olemassa ja liittyvän todelliseen henkilöön ja 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; tai 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;		
72.	S	Henkilöllisyystodistus esitetään ja sen aitous tarkistetaan **etäyhteydellä**. Henkilöstö tuntee henkilöllisyystodistusten aitoustekijät ja pystyy tarkistamaan ne. Varmistetaan, että henkilöllisyystodistus on sen esittävän henkilön oma. Etäyhteyden luotettavuusvaatimuksissa huomioidaan korotetun tason hyökkäyspotentiaali.	**TunnL 17 § Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen** 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 tunnistusvälineeseen. **LOA Liite 1 2.1.2** 1. Henkilöllä on varmennettu olevan hallussaan sen jäsenvaltion hyväksymä todiste ilmoitetusta henkilöllisyydestä, jossa sähköisen tunnistamisen menetelmää haetaan ja todiste on tarkastettu sen varmistamiseksi, että se on aito; tai luotettavasta lähteestä tiedetään sen olevan olemassa ja liittyvän todelliseen henkilöön ja		ks. tämän ohjeen kohta 3.9

			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; tai 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;		
73.	H	Henkilöllisyystodistus esitetään ja sen aitous tarkistetaan etäyhteydellä. Henkilöllisyystodistuksen aitous tarkistetaan sen myöntäjän sähköisen allekirjoituksen perusteella henkilöllisyystodistuksen sirulta. Varmistetaan, että henkilöllisyystodistus on sen esittävän henkilön oma vertaamalla	**LOA Liite 1 2.1.2 korkea** 1. Sama kuin tasolla ”korotettu”, minkä lisäksi yhden kohdissa a–c mainituista vaihtoehdoista on täytyttävä: a) 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		ks. tämän ohjeen kohta 3.9

		esittäneen henkilön ominaisuuksia henkilöllisyystodistuksesta saatuun sähköisesti allekirjoitettuun vertailutietoon. Etäyhteyden luotettavuusvaatimuksissa huomioidaan korkean tason hyökkäyspotentiaali.	tarkistetaan sen määrittämiseksi, onko se luotettavan lähteen mukaan voimassa; ja hakijalla todetaan olevan ilmoitettu henkilöllisyys vertaamalla yhtä tai useampaa henkilön fyysistä ominaisuutta luotettavaan lähteeseen;		
74.	S, H	Tieto passin tai henkilökortin voimassaolosta tarkistetaan käytettävissä olevista poliisin tietojärjestelmästä tai kansainvälisistä luotettavista lähteistä.	**LOA Liite 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)** Menettelyt 1 ja 2, osavaatimus ja on ryhdytty toimiin sen riskin minimoimiseksi, että henkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riskisiitä, että todiste on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt; **TunnL 7 b § Tieto passin tai henkilökortin voimassaolosta** Tunnistuspalvelun tarjoajalla on oikeus saada salassapitosäännösten estämättä rajapinnan kautta tai muutoin säh-		Ei pakolliseksi säädetty vaatimus, mutta vaikuttaa riskiarviointiin ja voi vaikuttaa korvausvastuuseen. Korkealla varmuustasolla lähtökohtaisesti välttämätön.

			köisesti poliisin tietojärjestelmässä oleva tieto ensitunnistamisessa käytettävän passin tai henkilökortin voimassaolosta.		
75.	S, H	Henkilön olemassaolo tarkistetaan väestötietojärjestelmästä	**TunnL 7 § Väestötietojärjestelmän tietojen käyttäminen** 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.		Koskee kaikkia ensitunnistusmenettelyjä.
Tapa 2: Ensitunnistus sähköisellä tunnistusvälineellä					
76.	S	Henkilöllisyyden todistaminen perustuu tunnistuslaissa hyväksyttyihin vahvoihin sähköisiin tunnistusvälineisiin.	**TunnL 17 § Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen** 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 tunnistusvälineeseen.		Jos käytössä on vahvaan sähköiseen tunnistamiseen perustuva ensitunnistaminen. Tunnistuslain mukaisesti hyväksytyt korotetun varmuustason tunnistusvälineet ovat Liikenne- ja viestintäviraston rekisterissä.

			LOA Liite 1 2.1.2 4. Jos sähköisen tunnistamisen menetelmiä myönnetään sellaisen voimassa olevan ilmoitetun sähköisen tunnistamisen menetelmän perusteella, 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 tarkoitetun vaatimustenmukaisuuden arviointilaitoksen tai vastaavan elimen vahvistama.		
77.	H	Henkilöllisyyden todistaminen perustuu tunnistuslaissa hyväksyttyihin vahvoihin sähköisiin tunnistusvälineisiin. Korkean varmuustason tunnistusvälineen myöntäminen sähköisen tunnistuksen perusteella on mahdollista vain korkean varmuustason välineellä.	**LOA liite 1 2.1.2 korkea** 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 ja		Jos käytössä on vahvaan sähköiseen tunnistamiseen perustuva ensitunnistaminen. Tunnistuslain mukaisesti hyväksytyt korkean varmuustason tunnistusvälineet ovat Liikenne- ja viestintäviraston rekisterissä.

			on ryhdytty toimiin sen osoittamiseksi, että sen menettelyn tulokset, jossa ilmoitettu sähköisen tunnistamisen menetelmä aiemmin myönnettiin, ovat edelleen voimassa.		
Tapa 3: Ensitunnistus muuhun tarkoitukseen tehdyn tunnistamisen perusteella ("aikaisempi asiakkuus")					
78.	S, H	Henkilöllisyyden varmentamisessa luotetaan menettelyyn, jolla henkilöllisyys on todistettu ja varmennettu aikaisemmin muuta kuin vahvan sähköisen tunnistusvälineen myöntämistä varten. Menettely perustuu muuhun sääntelyyn kuin tunnistuslakiin tai eIDAS-asetukseen ja sitä valvoo viranomainen. Menettely tarjoaa vastaavan varmuuden kuin tunnistussääntelyn mukainen henkilöllisyystodistuksen esittämiseen perustuva tai sähköisellä tunnistusmenetelmällä tunnistamiseen perustuva menettely.	**TunnL 17 § Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen** 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 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 tarkoitetun vaatimustenmukaisuuden arviointilaitoksen vahvistuksen perusteella.		Tämän kohdan mukaisen ensitunnistusmenettelyn käyttö edellyttää Liikenne- ja viestintäviraston nimenomaista vahvistusta. Menettelyä koskevaan ilmoitukseen täytyy liittää arviointi vaatimustenmukaisuudesta.

			LOA Liite 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö) 3. Jos julkisen tai yksityisen tahon samassa jäsenvaltiossa aiemmin muuhun tarkoitukseen kuin sähköisen tunnistamisen menetelmien myöntämiseen käyttämät menettelyt tarjoavat vastaavan varmuuden kuin 2.1.2. kohdassa esitetyt menettelyt varmuustasolla ”korotettu”, rekisteröinnistä vastaavan tahon ei tarvitse toistaa kyseisiä aiempia menettelyjä edellyttäen, että tällaisen vastaavantasoisen varmuuden on vahvistanut Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 765/2008 (1) 2 artiklan 13 kohdassa tarkoitettu vaatimustenmukaisuuden arviointilaitos tai vastaava elin;		
Tapa 4: Poliisin tekemä ensitunnistus					
79.	S, H	Ensitunnistamisen tekee tarvittaessa poliisi.	**TunnL 17 §** Jos tunnistusvälineen hakijan henkilöllisyyttä ei voida luotettavasti todentaa, hakemukseen liittyvän ensitunnistamisen tekee poliisi. **LOA Liite 1 2.1.2 korkea** 3. 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.		

5.10 Tunnistusvälineen eli tunnistusmenetelmän elinkaari

10. Tunnistusvälineen eli tunnistusmenetelmän elinkaari

M72A 15 § Arviointikriteerit
Tunnistuspalvelun arvioinnin täytyy kattaa 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	VAR-MUUS-TASO	TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ	SÄÄNNÖKSET	STAN-DARDI	HUOMIOITA

80.	S, H	Tunnistusvälinettä ei liitetä henkilöön eli personoida ennen ensitunnistamista.	**M72A 6 § Tunnistusmenetelmän tietoturvavaatimukset** 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. […]		
81.	S, H	Luonnollisen henkilön henkilötiedot tarkistetaan väestötietojärjestelmästä tunnistusvälinettä myönnettäessä ja säännöllisesti tunnistusvälineen voimassaolon aikana.	**TunnL 7 § Väestötietojärjestelmän tietojen käyttäminen** 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. […] **Ks. M72A 12 § Luottamusverkostossa välitettävät vähimmäistiedot**		Säännöllisen tarkistamisen tiheyttä ei ole säädetty. Hyvä vakiintunut käytäntö on tarkistus viikottain. vrt. (ei viittausta tunnistuslaissa eli muodollisesti sovelletaan vain, jos menetelmä notifioidaan) **LOA 2.1.1 Hakemus ja rekisteröinti** 3. Kerätään asiaankuuluvat tunnistetiedot, jotka tarvitaan henkilöllisyyden todista

82.	S, H	**Tunnistusvälineen myöntäminen, toimittaminen, aktivointi** Tunnistusvälineen luovutus- tai toimitusmenettelyssä varmistetaan, ettei tunnistusväline joudu oikeudettomasti toisen haltuun.	**TunnL 20 § Tunnistusvälineen myöntäminen** 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. […] vrt. (Kohtaan LOA 2.1.1 ei ole viittausta tunnistuslaissa eli muodollisesti sitä sovelletaan vain, jos menetelmä notifioidaan) **LOA 2.1.1 Hakemus ja rekisteröinti** 1. Varmistetaan, että hakija on tietoinen sähköisen tunnistamisen menetelmien käyttöön liittyvistä ehdoista ja edellytyksistä. 2. Varmistetaan, että hakija on tietoinen sähköisen tunnistamisen menetelmiin liittyvistä suositelluista varotoimista. **TunnL 21 § Tunnistusvälineen luovuttaminen hakijalle** Tunnistusvälineen tarjoajan on luovutettava tunnistusväline sen hakijalle siten kuin sopimuksessa on sovittu. Tunnistuspalvelun tarjoajan on varmistettava, ettei tun-		sopimusehdot (mm. TunnL 15 §) kuuluvat toimijan itse selvitettäviin asioihin, eivät kuulu auditoinnin piiriin 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. Ks. LOA-guidance: Mahdollisia mekanismeja ovat esimerkiksi seuraavat: • henkilökohtainen toimitus • toimitus kirjattuna kirjeenä • sellaisen aktivointimenettelyn käyttö, josta voidaan kohtuudella olettaa, että vain henkilöllä on menetelmän aktivointiin tarvittavat tiedot (esimerkiksi oletus-PIN-

			nistusväline joudu oikeudettomasti toisen haltuun välinettä luovutettaessa siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.2.2 vähintään korotetulle varmuustasolle säädetyt vaatimukset täyttyvät. **LOA Liite 2.2.2 Myöntäminen, toimittaminen ja aktivointi** Sähköisen tunnistamisen menetelmän myöntämisen jälkeen se toimitetaan käyttäen mekanismia, jonka kautta se voidaan olettaa toimitettavan vain sen henkilön haltuun, jolle se kuuluu.		koodi, joka toimitetaan erillään tunnistamismenetelmästä). Tasolla ”korotettu” on käytettävä useita todentamistekijöitä. Aktivointikoodeja ei välttämättä tarvita. Tason ”korotettu” vaatimukset voidaan täyttää monenlaisilla myöntämis-, toimitus- ja aktivointitapojen yhdistelmillä: • 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”. • Sähköisen tunnistamisen menetelmä ja aktivointikoodi toimitetaan erikseen postitse henkilön varmennettuun osoitteeseen. • Sähköisen tunnistamisen menetelmä toimitetaan postitse hakijan osoitteeseen.

					• Sähköisen tunnistamisen menetelmä annetaan käyttöön, kun hakijan henkilöllisyys on varmennettu.
83.	H	**Tunnistusvälineen myöntäminen, toimittaminen, aktivointi** Tunnistusväline luovutus- tai toimitusmenettelyssä varmistetaan, ettei tunnistusväline joudu oikeudettomasti toisen haltuun.	**LOA Liite 2.2.2 Myöntäminen, toimittaminen ja aktivointi** **korkea** Aktivointiprosessi varmistaa, että sähköisen tunnistamisen menetelmä on toimitettu vain sen henkilön haltuun, jolle se kuuluu.		
84.	S, H	**Tunnistusvälineen voimassaolon keskeyttäminen, peruuttaminen ja uudelleen aktivointi** Tunnistusvälineen tarjoajalla on 24/7 -sulkupalvelu käyttäjille sekä sulkulista luottaville osapuolille tai mahdollisuus teknisesti estää käyttäjän kadonneeksi tai varastetuksi ilmoittaman tunnistusvälineen käyttö.	**TunnL 25 § Tunnistusvälineen peruuttamista tai käytön estämistä koskeva ilmoitus** Tunnistusvälineen haltijan on ilmoitettava tunnistusvälineen tarjoajalle tai tämän nimeämälle muulle taholle tunnistusvälineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä ilman aiheetonta viivytystä havaittuaan asian. 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.		vrt. (kohtaan LOA 2.2.3 ei ole viittausta tunnistuslaissa eli sitä sovelletaan vain, jos menetelmä notifioidaan) **LOA Liite 2.2.3 Voimassaolon keskeyttäminen, peruuttaminen ja uudelleenaktivointi** 1. Sähköisen tunnistamisen menetelmän voimassaolo on mahdollista keskeyttää ja/tai peruuttaa viivytelemättä ja tehokkaasti. 2. Käytössä ovat toimenpiteet, joilla estetään voimassaolon luvaton keskeyttäminen, peruuttaminen ja/tai uudelleenaktivointi.

			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 tarkoitetun ilmoituksen. Todistusta on pyydettävä 18 kuukauden kuluessa ilmoituksesta. 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. […] **26 § Tunnistusvälineen tarjoajan oikeus peruuttaa tai estää tunnistusvälineen käyttö** Sen lisäksi, mitä 25 §:ssä säädetään, tunnistusvälineen tarjoaja voi peruuttaa tunnistusvälineen tai estää sen käytön, jos: 1) tunnistusvälineen tarjoajalla on syytä epäillä, että joku muu kuin se, jolle tunnistusväline on myönnetty, käyttää sitä;		3. Uudelleenaktivoinnin ehtona on, että ennen voimassaolon keskeyttämistä tai peruuttamista asetetut varmuusvaatimukset täyttyvät edelleen.

Liikenne- ja viestintävirasto

Erik Palmeninaukio 1
PL 313
00059 TRAFICOM
Puhelin 0295 390 100
www.traficom.fi

			2) tunnistusväline sisältää ilmeisen virheellisyyden; 3) tunnistusvälineen tarjoajalla on syytä epäillä, että tunnistusvälineen käytön turvallisuus on vaarantunut; 4) tunnistusvälineen haltija käyttää tunnistusvälinettä olennaisesti sopimusehtojen vastaisella tavalla; 5) tunnistusvälineen haltija on kuollut. Tunnistusvälineen tarjoajan tulee ilmoittaa haltijalle niin pian kuin mahdollista tunnistusvälineen peruuttamisesta tai käytön estämisestä ja sen ajankohdasta sekä siihen johtaneista syistä. Tunnistusvälineen tarjoajan on palautettava mahdollisuus käyttää tunnistusvälinettä tai annettava haltijalle uusi väline välittömästi 1 momentin 2 ja 3 kohdassa tarkoitetun syyn poistuttua.		
85.	S, H	**Tunnistusvälineen uusiminen ja korvaaminen**	**TunnL 22 § Tunnistusvälineen uusiminen** Tunnistusvälineen tarjoaja saa toimittaa tunnistusvälineen haltijalle uuden välineen ilman nimenomaista pyyntöä vain, jos aikaisemmin annettu tunnistusväline on korvattava uudella. Tunnistusvälineen uusimisessa tulee		TunnL 8 §:n ja LOA 2.2.1 mukaisen varmistusvaatimuksen, että ainoastaan tunnistusvälineen haltija voi käyttää välinettä, täytyy toteutua myös kaikissa tilanteissa, joissa osa tai kaikki todentamistekijät tai aktivointikoodit luovute-

			noudattaa sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.2.4 vähintään korotetulle varmuustasolle säädettyjä vaatimuksia. **LOA Liite 2.2.4 Uusiminen ja korvaaminen** 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.		taan uudelleen uusimisen/korvaamisen tai uudelleenaktivoinnin yhteydessä. 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
86.	H	**Tunnistusvälineen uusiminen ja korvaaminen**	**LOA Liite 2.2.4 Uusiminen ja korvaaminen** **Korkea:** 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.		

			Jos uusiminen tai korvaaminen perustuu voimassa olevaan sähköisen tunnistamisen menetelmään, tunnistetiedot varmennetaan luotettavasta lähteestä.		

6 LIITE C Mobiilitunnistusratkaisun erityiskriteeristö

Yleistä

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

Kriteeristön ensimmäinen versio on laadittu **pääsääntöisesti varmuustasolle korotettu**. Kriteeristöä voidaan tulevaisuudessa päivittää ja huomioida myös korkea varmuustaso, kun soveltamisesta saadaan kokemusta Suomessa ja kun eIDAS-sääntelyn vaatimusten tulkinnasta syntyy yhtenäisiä käytäntöjä Euroopassa.

6.1 Arkkitehtuuri, suunnittelu ja uhkakuvien mallintaminen

Kriteeri	Peruste	Lisätieto / kommentti
400. Kaikki sovelluksen komponentit on tunnistettu, luokiteltu ja ne ovat tarpeellisia	LOA 2.4.6, kohta 1 TunnL 8.1 § 4)	
401. Turvakontrollit on toteutettu sekä sovellukseen että palvelimeen	LOA 2.4.6, kohta 1 M72A 5.1 § 2c)	
402. Korkean tason arkkitehtuuri on määritelty itse sovellukselle ja siihen liittyville (ulkoisille) palveluille ja tietoturva on arkkitehtuurissa huomioitu	LOA 2.4.6, kohta 1 TunnL 8.1 § 4)	

403. Sovelluksessa käsiteltävä arkaluontoiset tiedot on selvästi tunnistettu	LOA 2.4.4, kohta 1 LOA 2.4.6, kohta 1 ja 3	
404. Sovellukseen ja sen käyttämiin palveluihin liittyvät uhkakuvat ja mahdolliset vastatoimet on tunnistettu	LOA 2.3.1, korotettu, kohta 2 LOA 2.3.1, korkea	Arvioidaan hyökkäyspotentiaalia kohtuullinen (korotettu) tai korkea (korkea)
405. Kaikilla turvakontrolleilla on keskitetty toteutus	LOA 2.4.6, kohta 1	
406. Salausavainten hallintaan on tarkkaan määritelty menetelmätapa, joka pohjautuu kansainvälisesti hyväksyttyyn ajantasaiseen standardiin	LOA 2.4.6, kohta 3 LOA 2.4.6, korotettu	
407. Mobiilisovellus ilmoittaa palvelimelle käytössä olevan käyttöjärjestelmäversion ja sovellusversion numeron, ja palvelinpäästä löytyy mekanismi, joka estää toiminnan liian vanhoilla ohjelmistoversiolla.	LOA 2.4.6, kohta 1 M72A 5.1 § 2c)	
408. Vanhentunut mobiilisovellus kehottaa käyttäjää käyttöjärjestelmän ja / tai mobiilisovelluksen päivitykseen, jotta transaktio voidaan suorittaa.	(LOA 2.1.1, kohta 2)	Suositeltava käytäntö / Best practise (BP). LOA 2.1.1 ei sisälly tunnistuslakiin.
409. Tietoturvallisia käytäntöjä noudatetaan koko sovelluksen elinkaaren ajan	LOA 2.4.6, kohta 1 ja 4 TunnL 8.1 § 4)	

6.2 Tietojen tallennus ja tietosuoja

Kriteeri	Peruste	Lisätieto / kommentti
410. Alustan tarjoamia turvapalveluita / -ominaisuuksia hyödynnetään täysimittaisesti sovelluksen tallentaessa arkaluonteista tietoa.	LOA 2.4.6., kohta 1, kohta 3	
411. Käyttäjää informoidaan selkeästi minkä tasoista tunnistusta ollaan tekemässä [Tälle vaatimukselle oikea paikka, yhdessä sovittu Best practise, esim. millä graafisilla elementeillä tms.]	LOA 2.1.1, kohta 2	Suositeltava käytäntö
412. Mitään luottamuksellista tietoa ei tallenneta sovellusympäristön tai alustan tarjoaman salaisuuksien tallennusta varten tarkoitetun ominaisuuden ulkopuolelle	LOA 2.4.6, kohta 1 M72A 5.1 § 3b)	
413. Mitään arkaluonteista tietoa ei kirjoiteta sovelluksen lokeihin	LOA 2.4.6, kohta 1 M72A 5.1 § 3b)	
414. Mitään arkaluonteista tietoa ei jaeta ulkoisten tahojen kanssa, ellei se ole ennalta määritelty arkkitehtuurissa	LOA 2.4.6, kohta 1 M72A 5.1 § 3b)	
415. Välimuistia ei käytetä tekstinsyöttökentissä, jotka saattavat sisältää arkaluonteista tietoa	LOA 2.4.6, kohta 1 M72A 5.1 § 3b)	
416. Arkaluontaista tietoa tai salaisuuksia (salasana, PIN -koodi) ei missään vaiheessa paljasteta käyttöliittymän kautta	LOA 2.4.6, kohta 1 M72A 5.1 § 3b)	
417. Leikepöytää ei käytetä tietoelementtien kohdalla, jotka saattavat sisältää arkaluonteista tietoa	LOA 2.4.6, kohta 1 M72A 5.1 § 3b)	
418. Arkaluonteista tietoa ei jaeta käytettäessä IPC -mekanismeja	LOA 2.4.6, kohta 1 M72A 5.1 § 3b)	

Kriteeri	Peruste	Lisätieto / kommentti
419. Tunnistukseen käytettyä / käytettyjä salaisuuksia ei missään vaiheessa tallenneta eikä siirretä sovelluksessa käytetyn tietovaraston ulkopuolelle.	LOA 2.4.6, matala, kohta 3 LOA 2.4.6, korotettu M72A 5.1 § 3b)	
420. Sovelluksen siirtyessä taustalle, arkaluonteinen tieto poistetaan käyttöliittymäkomponenteista	LOA 2.4.6, kohta 1 M72A 5.1 § 3b)	
421. Sovellus ei pidä arkaluonteista tietoa muistissa tarpeettoman pitkään, ja kun tietoa ei enää tarvita, poistetaan se muistista välittömästi	LOA 2.4.6, kohta 1 M72A 5.1 § 3b)	
422. Sovellus suosittelee loppukäyttäjälle minimitason laiteturvallisuuden käyttöönottoa (puhelimen PIN-koodisuojaus ja/tai biometrinen puhelimen avausmekanismi tai vastaavat)	LOA 2.1.1, kohta 2	Suositeltava käytäntö
423. Käyttäjälle kerrotaan parhaista käytännöistä, joita käyttäjän tulisi noudattaa henkilökohtaisen tiedon käsittelyssä	LOA 2.1.1, kohta 2	Suositeltava käytäntö

6.3 Salausvaatimukset

Kriteeri	Peruste	Lisätieto / kommentti
424. Sovellus ei luota pelkästään symmetrisiin salausmenetelmiin ja kovakoodattuihin avaimiin ainoana salauskeinona	M72A 5.1 § 2g M72A 7 §	
425. Käyttötapauksiin soveltuvat ja hyväksi havaitut salausmenetelmät ovat käytössä	M72A 5.1 § 2g	
426. Sovellus ei käytä vanhentuneita tai huonoiksi todettuja salauskäytäntöjä tai algoritmeja	M72A 5.1 § 2g	
427. Salausavaimia ei uudelleenkäytetä	LOA 2.4.6, kohta 1 TunnL 8.1 § 4)	
428. Käytetty satunnaislukugeneraattori on tarpeeksi turvallinen ja laadukas	LOA 2.4.6, kohta 1 TunnL 8.1 § 4)	
429. Käytössä on allekirjoituslaskuri, eli palvelin pystyy mahdollisesti huomaamaan sovelluksen kloonausyrityksen	LOA 2.3.1, korotettu, kohta 2 LOA 2.3.1, korkea	
430. Sovellus ei sisällä / käytössä ei ole mitään kovakoodattuja käyttäjätunnuksia tai salasanoja.	LOA 2.4.6, kohta 1 M72A 6.2 ja 6.3	
431. Sovelluksen kehitysaikaiset mahdollisesti heikommat salauskäytännöt, tunnisteet ja varmenteet on poistettu tuotantoon menevästä versiosta.	LOA 2.4.6, kohta 1 ja 3 LOA 2.4.6, korkea M72A 5.1 § 2g	

6.4 Tunnistaminen, tunnistusmenetelmän ominaispiirteet ja istunnonhallinta

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

Kriteeri	Peruste	Lisätieto / kommentti
432. Sovelluksen yksilöinnissä rekisteröintivaiheen aikana varmistutaan siitä että sovellus kytketään tunnistusvälineen haltijaan.	LOA 1 (määritelmät), kohta 2 LOA 2.2.1, kohta 2	
433. Tunnistuksen toteuttava salaisuus on suojattu väärinkäyttöä vastaan, ja salaisuuteen pääsee käsiksi vain ennalta määritellyllä, turvallisella tavalla	LOA 2.4.6, kohta 3 LOA 2.4.6, korotettu M72A 6 § 3	Esim. yksityinen avain.
434. Salaisuudet / tunnistusavaimet ovat yksilöllisiä	M72A 5.1 § 2g)	
435. Tunnistuksen toteuttavat asymetriset salaisuudet luodaan päätelaitteessa (avainpari, muu salainen avain / salaisuus)	M72A 5.1 § 2g) M72A 5.1 § 3b)	vrt RTS
436. Jos tunnistuksen toteuttavat salaisuudet luodaan laitteen ulkopuolella, provisioidaan ne turvallisesti käytettävään laitteeseen	LOA 2.4.6, kohta 2 LOA 2.4.6, korotettu M72A 5.1 § 3b)	vrt. RTS
437. Tunnistus ei saa pohjautua pelkästään jaettuun salaisuuteen	LOA 2.2.1, korotettu, kohta 2	
438. 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 M72A 6 § 3	

Kriteeri	Peruste	Lisätieto / kommentti
439. Sovellus ei tallenna pysyvästi tunnistetietoja / kredentiaaleja selväkielisinä missään vaiheessa (salasana, PIN-koodit, käyttäjätunnukset jne)	LOA 2.2.1, korotettu, kohta 2 LOA 2.2.1, korkea, kohta 2 LOA 2.3.1, korotettu, kohta 2 LOA 2.3.1, korkea, kohta 2 LOA 2.4.6, kohta 3	
440. Jos sovellus lähettää palvelimelle viestejä, joiden palvelinpäässä tapahtuva validointi johtaa tunnistukseen, tulee kyseiset viestit lähettää turvallisesti käyttäen ajantasaisia ja hyväksyttyjä salauskäytäntöjä (esim. Mutual / 2-way TLS 1.2 tai uudempi)	LOA 2.4.6, kohta 2 M72A 5.1 § 2g) M72A 7 § 1-4	
441. Jos sovelluksen ja palvelimen välillä vaihdetaan henkilötietoa, suojataan tämä tieto myös sanomatason salauksella.	LOA 2.4.6, kohta 2 LOA 2.4.6, korotettu M72A 5.1 § 2g)	
442. Jos sovellus perustuu, tai sen osana on kertakäyttösalasanoihin perustuva menetelmä, tulee kertakäyttösalasanan (OTP) luonnissa käyttää hyväksi havaittuja ja standardeihin perustuvia ratkaisuja	M72A 5.1 § 2g)	
443. Tunnistukseen käytetyn salaisuuden tallennukseen käytetään mahdollisuuksien mukaan alustan tarjoamia palveluita / laitteisto-ominaisuuksia, kuten laitteistotason turvaosiota tai käyttöjärjestelmän tarjoamia palveluita arkaluonteisen tiedon tallennukseen (esim. keychain)	M72A 5.1 § 2c) M72A 5.1 § 3b)	
444. Tieto virheellisestä syötteestä lähetetään jokaisen kerran jälkeen palvelimelle. Palvelin seuraa virheellisten syötteiden määrää ja sovellus lukittuu automaattisesti X virheellisen syötteen jälkeen. Jos	LOA 2.4.6, kohta 1 M72A 5.1 § 2f)	vrt. RTS ja SCA *[entä avaus? Tai käyttöjärjestelmätasolle tallennetut tunnisteet kuten sormenjälki?].*

Kriteeri	Peruste	Lisätieto / kommentti
verkkoyhteyttä ei ole, eikä viestejä saada lähetettyä palvelimelle turvallisesti, sovellus itse noudattaa samaa logiikkaa. (PSD2 5 virheen sääntö)		
445. Sovelluksen 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 LOA 2.3.1, korkea	
446. Jos käytössä on istuntotunnisteet, käytetään satunnaisia istuntotunnisteita	LOA 2.3.1, korotettu, kohta 2 LOA 2.3.1, korkea	
447. (Ohjelmisto/OAuth) Token-pohjaiseen teknologiaan ratkaisussa varmistetaan että token on allekirjoitettu hyväksyttävällä ja turvallisella algoritmilla	LOA 2.4.6, kohta 2 M72A 7.1 § 2	
448. Istunnon tai tokenin voimassaoloaika määritellään palvelinpäässä	LOA 2.4.6, kohta 1 & 4	
449. Valtuutuspolitiikat, joiden perusteella myönnetään pääsy kohdesovellukseen/palveluun, määritellään (tunnistus)palvelinpäässä	LOA 2.4.6, kohta 1 & 4	
450. 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
451. Jos biometrista todentamistekijää käytetään ja alustan ominaisuuksien takia rekisteröityneitä henkilöitä ei pystytä erottelemaan, on käyttäjää selkeästi ohjeistettava poistamaan muiden henkilöiden	LOA 2.2.1, korotettu, kohta 1 LOA 2.1.1, kohta 2 LOA 1 (määritelmät), kohta 2	LOA 2.1.1. Ei kuulu tunnistuslain piiriin, hyväksi havaittu käytäntö

Kriteeri	Peruste	Lisätieto / kommentti
biometriset tunnisteet/salaisuudet, jotka kuuluvat muille laitteen käyttäjille		
452. Jos sovelluksessa 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 omina kokonaisuuksinaan.	LOA 1 (määritelmät), kohta 2 LOA 2.2.1, korotettu, kohta 2 LOA 2.2.4, korotettu	Todentamistekijöiden riippumattomuus varmistettava. Tarkoittaa esim. yhden todentamistekijän kategorian vaihtoa, tai uuden lisäämistä, jolloin käytössä olisi kolmesta kategoriasta todentamistekijöitä.
453. 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 LOA 2.2.1, korotettu, kohta 2 LOA 2.3.1, korotettu, kohta 2	
454. Biometrisen todentamistekijän toteutuksessa käytetään ainoastaan alustan tarjoamia rajapintoja	LOA 2.4.6, kohta 1 M72A 5.1 § 2c)	
455. Biometristä tekijää hyödynnettäessä itse biometristä tallennetta (sormenjälki, kasvokuva, iiris skannaus jne) ei siirretä sovelluksen ulkopuolelle.	LOA 2.2.1, korotettu, kohta 2 LOA 2.3.1, korotettu, kohta 2	
456. Rekisteröintivaiheessa käytettävää arkaluonteista tai henkilötietoa voidaan siirtää palvelinpäähän arvioitavaksi ainoastaan käyttäen turvallisia keinoja.	LOA 2.4.6, kohta 2	

Kriteeri	Peruste	Lisätieto / kommentti
457. Käyttäjällä tulee olla mahdollisuus väliaikaisesti sulkea salaisuus a) yhdestä laitteesta b) useammasta laitteesta c) kaikista laitteista kerralla.	LOA 2.2.3, korotettu, kohta 1	
458. Väliaikaisesti suljetun salaisuuden avaamiseksi vaaditaan aina tunnistus vähintään samalla tasolla kuin sovelluksen käyttöönotossa	LOA 2.2.3, korotettu, kohta 3	
459. 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	
460. Laitekohtainen salaisuuden väliaikainen sulkeminen ja salaisuuden poistaminen tulee olla myös mahdollista palvelinpäässä.	LOA 2.2.3, korotettu, kohta 1 ja 2	
461. Tunnistus sidotaan haluttuun tapahtumaan tai selainistuntoon, eli tunnistussovelluksessa näytetään selkeästi tieto mitä ollaan tekemässä.		Esim. RTS, dynaaminen yhdistäminen. EU 2018/389
462. Tunnistussovellus toteuttaa myös ns. binding messagen jossa käyttäjälle muodostuu mahdollisuus ymmärrettävästi yhdistää mobiililaitteessa tapahtuva tunnistus esim. selainistuntoon.	LOA 2.3.1, korotettu, kohta 2	
463. Jos tunnistussovelluksen vaste perustuu epäsymmetriseen allekirjoitukseen on käytössä WYSIWYS -periaate, eli käyttäjälle näytetty tieto on samalla myös allekirjoitettavat tieto.	LOA 2.3.1, korotettu, kohta 2	
464. Sovellus ohjaa käyttäjää valitsemaan vahvoja PIN-koodeja	LOA 2.1.1, korotettu, kohta 2 M72A 5.1 § 2g)	LOA 2.1.1 ei kuulu tunnistuslain piiriin, hyväksi havaittu käytäntö

Kriteeri	Peruste	Lisätieto / kommentti
465. Sovellus ei hyväksy helposti arvattavia PIN-koodeja tai muita käyttäjän muistiin perustuvia salaisuuksia	LOA 2.3.1, korotettu, kohta 2 LOA 2.4.6, kohta 1	
466. Käyttäjän syötteet, esim. PIN -koodit, validoidaan turvallisesti	LOA 2.3.1, korotettu, kohta 2 M72A 5.1 § 3b)	
467. Jos sovellus hyväksikäyttää päätelaitteen laitteistotason turvaominaisuuksia, kuten TEE:tä tai vastaavaa, ilmoittaa sovellus käytetyn laitteistotason komponentin ja muut mahdolliset tiedot palvelimelle alustuksen yhteydessä, jotta palvelin pystyy päättelemään onko käytössä laitteistotasolla haavoittuvainen järjestelmä (myös jatkossa).	LOA 2.4.6, kohta 1 M72A 5.1 § 3d)	Uusi, 29.4.2019: CVE-2018-11976 → Annetaan palvelimelle mahdollisuus reagoida jos on tiedossa että laitteistotason komponentti on haavoittuvainen.

6.5 Tietoliikenne

Kriteeri	Peruste	Lisätieto / kommentti
468. Sovelluksen ja palvelimen välinen verkkoliikenne on suojattu kansainvälisesti tai kansallisesti suositelluilla yhteyskäytännöllä ja suojatut kanavat ovat yhdenmukaisesti käytössä sovelluksessa	LOA 2.4.6, kohta 2 M72A 5.1 § 2g)	Tunnistusjärjestelmän *sisäisille* yhteyksille ei ole määrätty salausvaatimuksia, mutta lähtökohtana voidaan pitää M72A 7

Kriteeri	Peruste	Lisätieto / kommentti
		§:n mukaisia *toimijoiden välisiä* tietoliikenteen salauskäytäntöjä.
469. Sovellus tarkistaa TLS (tai vastaava) salausmenetelmän asetukset ja varmistaa että ne noudattavat hyväksi havaittuja käytäntöjä	LOA 2.4.6, kohta 2 M72A 5.1 § 2g)	Tunnistusjärjestelmän *sisäisille* yhteyksille ei ole määrätty salausvaatimuksia, mutta lähtökohtana voidaan pitää M72A 7 §:n mukaisia *toimijoiden välisiä* tietoliikenteen salauskäytäntöjä.
470. Sovelluksessa on käytössä hard-fail certificate pinning.	LOA 2.4.6, kohta 2	
471. Kriittisissä toiminnoissa, kuten alustuksessa ja käyttäjän salaisuuden luomisessa sovellus ei luota turvattomiin kommunikointikanaviin (Esim. sähköposti, SMS)	LOA 1 (määritelmät), kohta 2 LOA 2.2.1, korotettu, kohta 2	Käytännössä sovelluksen personoinnin on perustuttava vahvaan sähköiseen tunnistukseen.
472. Sovellus käyttää vain ajantasaisia ohjelmistokirjastoja yhteyksien ja tietoturvan toteuttamisessa	LOA 2.4.6, kohta 1 ja 4	

6.6 Alustan ja sovelluksen yhteistyö

Kriteeri	Peruste	Lisätieto / kommentti
473. Sovellus pyytää päätelaitteelta vain tarvitsemansa oikeudet	LOA 2.4.6, kohta 1 M72A 5.1 § 2c)	
474. Kaikki sovelluksen ulkopuolelta / ulkopuolisista lähteistä tuleva tieto tarkistetaan ja sanitoidaan (sanitize?).	LOA 2.4.6, kohta 4 M72A 5.1 § 2c)	
475. Omaa URL skeemaa tai IPC mekanismeja käytettäessä ei tietoja viedä sovelluksen ulkopuolelle, ellei sitä toteuteta turvallisesti	LOA 2.4.6, kohta 2 M72A 5.1 § 2c)	
476. WebView -komponenteissa käytetään vain tarpeellisia yhteyskäytäntöjä, ja muut suljetaan / varmistetaan että ne eivät ole käytössä	LOA 2.4.6, kohta 1 M72A 5.1 § 2c)	
477. JavaScript on oletusarvoisesti deaktivoitu WebView komponenteissa	LOA 2.4.6, kohta 1 M72A 5.1 § 2c)	
478. Natiivimetodit ovat estetty, jos alustan ohjelmistoversio on todettu haavoittuvaksi	LOA 2.4.6, kohta 1 M72A 5.1 § 2c) ja 3d)	Esim. vanhemman Android -käyttöjärjestelmäversion toteutus JavaScriptin kohdalla voi olla turvaton
479. Jos sovelluksen natiivimetodit ovat avoimia WebView –komponenteille, varmistetaan että ajetaan vain sovelluspakettiin kuuluvaa JavaScriptiä	LOA 2.4.6, kohta 1 M72A 5.1 § 2c)	
480. WebView -komponenteilta on pääsy kielletty / estetty paikallisiin resursseihin	LOA 2.4.6, kohta 1 M72A 5.1 § 2c)	
481. Käytössä on turvalliset API:t jos käytetään objektien serialisointia	LOA 2.4.6, kohta 1 ja 3 LOA 2.4.6, korotettu	

Kriteeri	Peruste	Lisätieto / kommentti
	M72A 5.1 § 2c)	

6.7 Ohjelmistokoodin turvallisuus, laatu ja kehitysympäristö

Kriteeri	Peruste	Lisätieto / kommentti
482. Sovellus on allekirjoitettu ja provisioitu voimassaolevalla ja luotetulla varmenteella	LOA 2.4.6, kohta 1	
483. Sovellus on luotu release mode:ssa, eli esim. moodissa, jossa virheenkorjaus on tehty vaikeammaksi	LOA 2.4.6, kohta 1 M72A 5.1 § 2c)	
484. Sovelluskehityksessä käytetään hyväksi havaittuja ohjelmistokehityksen / koodauksen tietoturvakäytäntöjä.	LOA 2.4.6, kohta 1 M72A 5.1 § 2c)	Esimerkiksi kaikki käytettävä Javascript tulee enkoodata ja sanitoida XSS hyökkäysriskin pienentämiseksi.
485. Virheenkorjaussymbolit on poistettu binääreistä	LOA 2.4.6, kohta 1 M72A 5.1 § 2c)	
486. Virheenkorjauskoodi ja –viestit on poistettu	LOA 2.4.6, kohta 1 M72A 5.1 § 2c)	
487. Kaikki kolmannen osapuolen käytetyt komponentit on tunnistettu ja tunnetut haavoittuvuudet selvitetty ja analysoitu	LOA 2.4.6, kohta 4 M72A 5.1 § 3d)	
488. Sovellus huomaa ja käsittelee asianmukaisesti poikkeukset	LOA 2.4.6, kohta 4	

Kriteeri	Peruste	Lisätieto / kommentti
	M72A 5.1 § 2f) ja 3d)	
489. Sovellus tai palvelin minimoi virheviestien sisältämän tiedon	LOA 2.4.6, kohta 1 M72A 5.1 § 2c)	
490. Turvakontrollien virheenkäsittely oletusarvoisesti evää pääsyn virhetilanteessa	LOA 2.4.6, kohta 1 M72A 5.1 § 2c)	
491. Muistia varataan, käytetään ja vapautetaan turvallisesti	LOA 2.4.6, kohta 1 M72A 5.1 § 2c)	
492. Alustan / kehitysympäristön tarjoamat tietoturvaominaisuudet ovat käytössä	LOA 2.4.6, kohta 1 M72A 5.1 § 2c)	

6.8 Turvakontrollit ja suojautuminen (EN: Resilience)

Kriteeri	Peruste	Lisätieto / kommentti
493. Sovellus käyttää useampaa tässä kappaleessa esitettyä puolustusmekanismia	LOA 2.4.6, kohta 1	Ohjelmiston kykyä vastustaa hyökkäyksiä on arvioitava kokonaisuutena.
494. Sovelluksessa on useampi kuin yksi toiminto jotka pyrkivät huomaamaan rootatun tai jailbreakatun laitteen.	LOA 2.4.6, kohta 4 M72A 5.1 § 2f)	

Kriteeri	Peruste	Lisätieto / kommentti
495. Sovellus lähettää viestin palvelinpään toteutukselle huomatessaan ajoympäristöksi rootatun tai jailbreakatun laitealustan tai sovellus itse voi päättää mitä tehdä huomatessaan ympäristön olevan rootattu / jailbreakattu.	LOA 2.4.6, kohta 4 M72A 5.1 § 2f)	
496. Sovellus pyrkii estämään virheenkorjaukseen pyrkivät yritykset ja reagoi jos huomaa virheenkorjaukseen käytetyn ratkaisun liittyneen sovellukseen.	LOA 2.4.6, kohta 1 M72A 5.1 § 2c)	
497. Sovellus pyrkii huomaamaan ja reagoi jos sovelluksen ajoympäristössä (sandbox) ajonaikaiset tiedostot tai kriittiset tiedot / tiedostot muuttuvat	LOA 2.4.6, kohta 4 M72A 5.1 § 2f)	
498. Sovellus huomaa ja reagoi yleisesti käytettyihin työkaluihin, joilla pyritään selvittämään sovelluksen lähdekoodia (reverse engineering)	LOA 2.4.6, kohta 4 M72A 5.1 § 2f)	
499. Sovellus huomaa ja reagoi jos sitä ajetaan emulaattorissa	LOA 2.4.6, kohta 4 M72A 5.1 § 2f)	
500. Sovellus tarkkailee ja huomatessaan muistiavaruuden muutoksia / manipulointia ja reagoi asianmukaisesti	LOA 2.4.6, kohta 4 M72A 5.1 § 2f)	
501. Sovellukselle tärkeät / olennaiset osiot on soveltuvilta osin salattuja tietojärjestelmätasolla. Analysoimalla ei saada selville sovellukselle tärkeitä / olennaisia osioita	LOA 2.4.6, kohta 1 ja 3 LOA 2.4.6, korotettu M72A 5.1 § 3b) M72A 5.1 § 2c)	