Määräys 72 päivittämisen päivittyvä työsuunnitelma 2020-2021

Sisällys

1 Tunnistus- ja luottamuspalvelumääräyksen Viestintävirasto 72 A/2018 M päivittäminen

1.1 Sidosryhmävalmistelun organisointi työpajoissa

Työpajat ovat avoimia viraston eIDAS-sidosryhmäjakeluihin kuuluville organisaatioille.

Työpajojen sisältöä muutetaan tarvittaessa työn kuluessa. Myös aikataulua voidaan muuttaa tarvittaessa tai järjestää lisää työpajoja erityiskysymyksistä.

Tässä suunnitelmassa esitetään työpajoissa käsiteltävät asiakokonaisuudet, nykyiset asiaan liittyvät säännökset, arvioitavat kysymykset ja lähteitä.

Viimeistään noin 1-2 viikkoa ennen kutakin työpajaa toimitetaan sähköpostitse kustakin aiheesta viraston valmistelumuistio, jossa esitetään muutosvaihtoehtoja ja niiden vaikutusarviointia. Työpajoissa käydään tältä pohjalta läpi teknisiä asioita, toteutettavuutta ja vaikutuksia.

Jokaiselle aiheelle on aikataulutettu jatkotyöpaja, joka pidetään vain tarvittaessa jonkin asian tarkemmalle käsittelylle.

1.2 Täydennetty 26.3.2021, Työpajojen aikataulu (pvm, klo) ja muut työvaiheet

PVM	Määräaika	Toimenpide	Lisätietoja
4.8.2020	15.9.2020	Kuuleminen: Traficomin kysely sidosryhmille määräyksen päivitystarpeista	Kysely lähetetään käytössä olevilla sähköpostijakeluilla ja julkaistaan viraston verkkosivuilla (kielet FI ja EN)
lokakuu - marraskuu 2020		Virkavalmistelu, luonnokset vaikutusarvioinnista ja muutostarpeista	Materiaalia käsitellään teemoittain kokouksissa sidosryhmien kanssa.
7.12.2020		tiedottaminen päivittämisen käynnistämisestä	verkkosivut, sidosryhmäjakelut
ke 16.12.2020 klo 9-11.30	kutsu ja ennakkomateriaali 7.12.2020	1/7 työpaja - työpajojen aiheet ja aikataulu - tunnistus: rajapinnat ja attribuutit	a) määräystyön kokonaisuus ja työsuunnitelma b) tunnistuspalveluiden rajapinnat ja attribuutit
ke 20.1.2021 klo 9-11.30	kutsu ja ennakkomateriaali 11.1.2021	2/7 työpaja - tunnistus: salaus	tunnistusjärjestelmän a) salausvaatimusten sääntelymalli ja tekninen ajantasaisuus, b) osapuolten varmentaminen, avaintenvaihto, sanomatason salaus
tarvittaessa ke 3.2.2021 klo 9-11	*kutsu 20.1.2021*	*tarvittaessa jatkotyöpaja 1. ja 2. työpajan teknisille yksityiskohdille*	*rajapinnat, salaus*
ke 10.2.2021 klo 9-11.30	kutsu ja ennakkomateriaali ~~1.2.2021~~ 3.2.2021	3/7 työpaja - tunnistus: koko tunnistusjärjestelmän tekniset vaatimukset ja arviointi	tunnistusjärjestelmän a) tekniset tietoturvavaatimukset (kokonaisuus) ja varmuustasot, b) häiriötilanteiden hallinta

			c) tietoturvallisuuden hallinta d) vaatimustenmukaisuuden arviointi
~~*tarvittaessa ke 17.2.2021 klo 9-11*~~	~~*kutsu 10.2.2021*~~	~~*tarvittaessa jatkotyöpaja 3. työpajan teknisille yksityiskohdille*~~	~~*tunnistusjärjestelmä*~~
ke 10.3.2021 klo 9-11.30	kutsu ja ennakkomateriaali ~~1.3.2021~~ 3.3.2021	4/7 työpaja - tunnistusmenetelmä, vrt. PSD2 - Blockchain ja SSI	a) tunnistusmenetelmä, todentamistekijät, PSD2-vertailu b) blockchain ja SSI
~~*tarvittaessa ke 17.3.2021 klo 9-11*~~	~~*kutsu 10.3.2021*~~	~~*tarvittaessa jatkotyöpaja 4. työpajan teknisille yksityiskohdille*~~	~~*todentamistekijät ja todentamismekanismi*~~
to 15.4.2021 klo 9-11.30	kutsu ja ennakkomateriaali 1.4.2021	5/7 työpaja - luottamuspalvelut ja akkreditoidut arviointilaitokset	a) hyväksyttyjen luottamuspalveluiden ETSI-standardit b) arviointilaitosten akkreditointi c) arviointikertomukset
tarvittaessa ke 21.4.2021 klo 9-11	*kutsu 15.4.2021*	*tarvittaessa jatkotyöpaja 5. työpajan teknisille yksityiskohdille*	*luottamuspalvelut*
ke 12.5.2021 klo 9-11.30	kutsu ja ennakkomateriaali 3.5.2021	6/7 työpaja ~~— TBD~~ määräyksen tunnistuslukuihin tehdyt muutokset	~~TBD~~ numerot viittaavat määräyksen säännöksiin (§-merkkiä ei enää käytetä) 1. soveltamisala 3. määritelmät 4. tietoturvallisuuden hallinta 5. tekniset tietoturvavaatimukset (kokonaisuus) ja varmuustasot 6. tunnistusmenetelmä, todentamistekijät 7. salausvaatimusten sääntelymalli ja tekninen ajantasaisuus 8. osapuolten varmentaminen, avaintenvaihto 9. sanomatason salaus 11. häiriötilanteiden hallinta 12. tunnistuspalveluiden attribuutit 14. tunnistuspalveluiden rajapinnat 15., 18., 19. vaatimustenmukaisuuden arviointi
tarvittaessa to 20.5.2021 klo 9-11	*kutsu 12.5.2021*	*tarvittaessa jatkotyöpaja 6. työpajan teknisille yksityiskohdille*	

to 10.6.2021 klo 9-11.30	kutsu ja ennakko-materiaali 3.6.2021	7. työpaja - koko määräys	käydään läpi kokonaisuus, tarvittaessa substanssiasioita
kesäkuu-elokuu 2021		virkavalmistelu ja käännökset	FI, SE ja EN
n. syyskuu 2021		kuuleminen: lausuntokierros määräyksestä ja perustelumuisti-osta	FI, SE ja EN
lausunto-kierroksen alkaessa		tiedottaminen lausuntokierrok-sesta	
n. lokakuu 2021		virkavalmistelu: lausuntokooste, mahdolliset muutokset ja niiden käännökset	
n. lokakuu 2021		palautetilaisuus lausuntokierrok-sen tuloksista	FI, EN summary
n. lokakuu 2021 - jou-lukuu 2021		lakisääteinen EU-notifiointi	
n. tammi-kuu-helmi-kuu		uusi määräys voimaan	huom. mahdolliset siirtymä-säännökset arvioidaan valmis-telun aikana

1.3 Päivitystyön kokonaisuus

1.3.1 Vastuuyksikkö

Määräyksen valmistelusta vastaa Liikenne- ja viestintävirastossa Kyberturvallisuuskeskuksen valvontaosaston turvallisuussääntely-yksikkö. Yksikön tehtäviin kuuluu vahvan sähköisen tunnistamisen ja luottamuspalveluiden ohjaus ja valvonta.

Määräyksen antamisesta päättää viraston pääjohtaja Kyberturvallisuuskeskuksen ylijohtajan esittelystä.

1.3.2 Määräystoimivalta

- TunnL (617/2009) 42 § Yleinen ohjaus sekä Liikenne- ja viestintäviraston määräykset
- Määräys tarkentaa ylemmän asteisten säädösten vaatimuksia

1.4 Yleiset linjaukset määräyksen päivittämisestä

Työn painopisteet näkyvät tarkemmin jäljempänä työpajojen kohdalla. Niihin voi antaa palautetta.

✓ **Määräyksen perusrakenne ja lukujako säilytetään**
- Perustelumuistio ja viitteet päivitetään.
- Perustelumuistion rakenne muuttuu täysin viraston uuden mallin mukaiseksi ja sisältöä karsitaan.

✓ **Vaatimusmuutoksia harkitaan**
- Vaatimuksia ja perusteluja selvennettävä ja ajantasaistettava joiltain osin

- Erityisesti attribuuteissa, salausvaatimuksissa ja luottamuspalveluiden standardiviitteiden täydennyksissä

✓ **Vaikuttavuus, kyselyyn saatujen vastausten mukaan**
- Määräyksen koettu jonkin verran edistäneen oman palvelun turvallisuuden kehittämistä.
- Salausvaatimusten jäykkyyttä kritisoitu
- Rajapintasuositusten vapaaehtoisuus aiheuttanut ylimääräistä työtä yhteensovittamisessa
- Avaintenhallinnan käytäntöjen ohjauksen puuttuminen nostettu ongelmana esille
- Kyselyssä arvioita, että kaikki eivät tee häiriöilmoituksia

✓ **Muu tekninen ohjaus viraston antamat ohjeet ja suositukset**
- käytetään pääpiirteissään samoissa asioissa kuin tähänkin asti
- Salausvaatimuksissa harkitaan viittausta NCSA:n tai SOGIS MRA:n dokumenttiin
- DVV toivonut rajat ylittävän julkisen sektorin tunnistuksen erillistä ohjetta

✓ **Valvovalta viranmaiselta toivotut operatiiviset palvelut**
- eivät kuulu säädettyihin tehtäviin (toisin kuin esimerkiksi .FI-verkkotunnushallinnolla)

✓ **Uhkat, fraud.**
- Muutosvalmistelussa SPname-attribuutti ja tietoliikenteen osapuolten varmentaminen liittyvät uhkien ja fraudin torjuntaan.

✓ **PSD2 ja eIDAS.**
- PSD2-vaatimuksia tarkastellaan referenssinä tunnistusmenetelmän vaatimusten kohdalla
- Määräystyön yhteyteen ei ole suunniteltu perusteellista Liikenne- ja viestintäviraston ja Finanssivalvonnan tekemää yhteistarkastelua
- Jos toimijoilla on tarve saada asioita käsittelyyn, niistä tarvitaan aloitetta ja tietoa toimijoilta

✓ **Blockchain ja SSI.**
- julkisen ja yksityisen sektorin yhteistyön politiikkaratkaisut eivät kuulu valvontaviranomaisen toimivaltaan tai tehtäviin
- Määräystyön yhteydessä varataan tilaisuus käsitellä lohkoketjuteknologian ja SSI -lompakkototeutusten suhdetta tunnistuksen teknisiin vaatimuksiin ja arviointivaatimuksiin
- virasto ei ole tässä vaiheessa tekemässä omaa teknistä yksityiskohtaista arviota, mutta seuraa tarkasti eIDAS-asetuksen uudelleenarviointia ja EU-tason hankkeita

2 1/7 työpaja: 16.12.2020 Tunnistuspalvelurajapinnat ja attribuutit

2.1 Määräyksen nykyiset säännökset

- *3 § Määritelmät*
- M72 Luku 3 Tietojen välittäminen luottamusverkostossa
- *12 § Luottamusverkostossa välitettävät vähimmäistiedot*
- *13 § Rajat ylittävän tunnistamisen edellyttämät tiedot*
- *14 § Tiedonsiirrossa käytettävä protokolla ja muut vaatimukset*

2.2 Pohjamateriaali, lähteet, referenssit

1) Liikenne- ja viestintäviraston kysely 4.8.2020 tunnistus- ja luottamuspalvelumääräyksen 72 ja muun teknisen ohjauksen muutostarpeista
2) Liikenne- ja viestintäviraston valmistelumuistio 2020-2021 rajapinnat ja attribuutit (jaetaan 1-2 viikkoa ennen työpajaa)
3) Päivitettävät Liikenne- ja viestintäviraston rajapintasuositukset 212/2021 (SAML) ja 213/2021 (OpenIDConnect)
4) Mahdollisesti ETSI MSS -standardi
5) Komission yhteentoimivuuspäätös EU 2015/1501 (M72 12 §:n attribuutit vastaavat (EU) 2015/1501 määriteltyjä pakollisia ja valinnaisia tietoja)

6) Onko muita lähteitä?

2.3 Arvioitavat kysymykset

2.3.1 Onko tarpeellista lisätä (luonnollisen henkilön) pakollisia tai valinnaisia attribuutteja (12 §)?

- Liittyvätkö tarpeet tunnistamisen turvallisuuteen vai yhteentoimivuuteen?
- Miten huomioidaan se, että eIDAS-asetuksen muuttaminen voi jollain aikavälillä lisätä tai muuttaa rajat ylittävän tunnistamisen attribuutteja, esim. kansallisuus?
- Toteuttaako attribuutit tunnistusvälineen tarjoaja vai tunnistusvälityspalvelu?

2.3.2 Ensitunnistamisen attribuutit

- Määritelläänkö ensitunnistuksen ketjuttamisessa tarvittavia attribuutteja pakolliseksi?
- Mitkä attribuutit ovat saatavilla tai tarpeellisia? Esim. tarjotun ensitunnistuksen oma perusta (kuten tieto henkilöllisyystodistuksesta tai ketjutuksesta)?

2.3.3 Muut attribuutit ("rikastaminen") tai tunnistuksen pseudonymisointi/köyhdyttäminen

- Mitä pseudonymisointi tai tunnistuksen köyhdyttäminen edellyttäisi? Voiko tarjontaa edistää jollakin yhteisellä määrittelyllä?
- Mitä rikastamisen tai köyhdyttämisen edellyttäisi teknisesti tunnistusvälineen tarjoajalta tai tunnistusvälityspalvelulta? Vaikuttaako köyhdyttäminen tunnistusvälineen tarjoajaan?

2.3.4 Rajapintaprotokollat ja tekninen yhteentoimivuus (14 §)

- Miten 14 §:n informatiivista protokollasäännöstä voisi tarkentaa?
- Millä tarkkuudella rajapintavaatimukset laaditaan määräykseen suhteessa niihin protokolliin, joiden pohjalta laaditaan rajapintasuositukset (SAML, Open ID Connect). Miten huomioidaan mahdollisten muiden protokollien käyttö.
- Miten huomioidaan ETSI MSS -protokolla, jota ei arvioitu 2016 määräystyössä?
- Miten IPv6-tukea voidaan edistää?

2.3.5 Vaikutus asiointipalvelurajapintaan

- Liittyykö tunnistusvälineen ja tunnistusvälityspalvelun välisen rajapinnan määrittelyyn piirteitä, joilla on vaikutusta asiointipalveluiden rajapintoihin. (Lain 12 a § mukaan luottamusverkoston yhteistyöllä on varmistettava, että tekniset rajapinnat mahdollistavat yleisesti tunnettujen standardien mukaisten rajapintojen tarjoamisen luottaville osapuolille.)

~~2.4 Tarvittaessa jatkotyöpaja 1/1 ja 2/7 ke 3.2.2021~~

2.5 Täydennys 26.3.2021: viraston valmistelulinjaukset, attribuutit ja rajapinnat

- Uudet pakolliset attribuutit, määräys kohta 12. Valmistellaan SPname -attribuutin lisäys määräykseen.
    - Attribuutti on tarpeellinen ja toteutuskelpoinen. Toteutus- ja soveltamiskäytäntöä voidaan tarvittaessa käsitellä määräyksen perusteluissa. Luottamusverkoston yhteistoimintaryhmässä voidaan pohtia parhaita käytäntöjä, jos esimerkiksi nimeämisessä ilmenee ongelmia. Asiakkaiden tunnistama nimi vastannee yrityksen virallista nimeä paremmin attribuutin tavoitetta. Ennalta määritellyt nimet vastaavat dynaamisesti muuttuvia nimiä paremmin attribuutin tavoitetta, joka on ennaltaehkäistä käyttäjien harhaanjohtamista ja muitakin virheitä (typot).

- Uudet valinnaiset attribuutit, määräys kohta 12: Ei valmistella uusia valinnaisia attribuutteja määräykseen.
    - Uusille valinnaisille attribuuteille ei ole nähtävissä sellaista tarvetta, että niiden määrittelyä olisi nyt tarpeen edistää määräyksellä. Mahdollisten eIDAS-asetuksen muutosten vaikutusta seurataan ja huomioidaan tarvittaessa myöhemmin.
- Ensitunnistamisen lisäattribuutit, määräys kohta 12. Ei valmistella muutoksia määräykseen, mutta seurataan tilannetta ja täydennetään tarvittaessa rajapintasuosituksia.
    - Virasto on huomioinut tunnistuspalveluiden palautteen ja arvion siitä, olisivatko luotettuun tunnistusvälineeseen liittyvien lisätietojen tuottamisen kustannukset oikeassa suhteessa saavutettaviin turvallisuushyötyihin. Toimijoiden palautteen perusteella kustannukset ylittäisivät hyödyt ja tiedoista ei olisi välitöntä hyötyä uuden välineen myöntämistilanteessa. On myös seurattava, vaikuttaako valtion tunnistushanke ensitunnistuksen ketjuttamisen tarpeellisuuteen
- Tunnistuksen köyhdyttäminen tai rikastaminen, ei omaa määräyskohtaa. Ei velvoittavia lisäyksiä määräykseen.
- Virasto harkitsee vielä köyhdyttämisen toteutusta selventävää säännöstä (12 tai 14 kohtaan).
    - Köyhdyttäminen on sääntelyn tunnistama toimintamalli. Sitä voi sinänsä tarjota ilman määräyksen muutoksia. Tällaisten palveluiden kehittyminen on toivottavaakin. Luottamusverkoston sisällä olisi tehtävä autentikointi normaalisti ja tallennettava tiedot. Tunnistusvälineen ja tunnistusvälityspalvelun tarjoaja ovat molemmat oletusarvoisesti rekisterinpitäjiä. Yhteentoimivuutta voidaan tarvittaessa edistää luottamusverkoston yhteistoimintaryhmässä.
    - Rikastaminen muilla kuin määräyksen 12 kohdan valinnaisilla tiedoilla, ei määräyskohtaa. Henkilötietojen lisääminen on henkilötietosääntelyn mukaisesti arvioitava lisäpalvelu suhteessa tunnistamiseen. Jos lisätiedot tuottaisi tunnistusvälineen tarjoaja, yhteentoimivuus edellyttäisi kaiketi, että ne on määritelty luottamusverkoston rajapinnoissa. Näistä teknisistä toteutuksista ja ominaisuuksista on mahdollista sopia.
- Rajapintaprotokollat ja muut vaatimukset/tekninen yhteentoimivuus, määräys 14 kohta. Ei uusia vaatimuksia. Valmistellaan määräykseen ainakin selventäviä ja mahdollisesti muita yleisen tason tarkennuksia, viittaus rajapintasuositusten protokolliin.
- Protokollien tai rajapintamääritysten vaikutus asiointipalveluiden toimintoihin. Ei muutoksia määräykseen.
    - Ei havaintoja tai palautetta toiminnoista, joiden mahdollistamista olisi tarpeen tai mahdollista edistää määräyksellä. Sidosryhmätyöpajassa ei saatu tietoa asiointipalveluiden näkökulmasta esimerkiksi tunnistusvälineen käyttörajoitusten tarkastamiseen.

3 2/7 työpaja: KE 20.1.2021 Tunnistuksen salausvaatimukset ja osapuolten varmentaminen

3.1 Määräyksen nykyiset säännökset

- 5 § *Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet (1 momentin 2 g kohta)*
- 7 § *Tunnistusjärjestelmän ja rajapintojen salausvaatimukset*
- 8 § *Tietoturvavaatimukset tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa*
- 9 § *Tietoturvavaatimukset asiointipalvelurajapinnassa*
- 10 § *Tietoturvavaatimukset kansallisen solmupisteen rajapinnassa*

3.2 Pohjamateriaali, lähteet, referenssit

1) Liikenne- ja viestintäviraston kysely 4.8.2020 tunnistus- ja luottamuspalvelumääräyksen 72 ja muun teknisen ohjauksen muutostarpeista
2) Liikenne- ja viestintäviraston valmistelumuistio 2020-2021 salausvaatimukset (jaetaan 1- 2 viikkoa ennen työpajaa)

3) Liikenne- ja viestintäviraston NCSA-toiminnon hyväksymät salausratkaisut (27.4.2016 dnro 238/651/2013)
   - Uusi linkki 2020: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/NCSA_salausratkaisut.pdf

4) SOGIS-MRA Agreed Cryptographic Mechanisms

   - https://www.sogis.eu/uk/supporting_doc_en.html#:~:text=The%20document%20%C2%AB%20SOG%2DIS%20Crypto,by%20all%20SOG%2DIS%20participants

5) NISTin (National Institute of Standards and Technology) FIPS-standardit (Federal In-formation Processing Standards) www.nist.gov

6) Uusi, TLS-profiileissa mahdollinen guideline
   - https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/finalX

7) Uusi, esimerkki TLS -versioiden yhteensopivuuskooste (selaimiin, clientteihin jne.)
   - https://support.globalsign.com/ssl/general-ssl/tls-protocol-compatibility

8) IANAn (Internet Assigned Numbers Authority) IKEv2-määritykset http://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml ja IANAn ciphersuitet: http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4

9) Kansallisten solmupisteiden välisten rajapintojen vaatimukset määritellään asiakirjassa eIDAS - Cryptographic requirements for the Interoperability Framework, TLS and SAML,
   - Version 1.0, 6 November 2015 - https://joinup.ec.europa.eu/sites/default/files/eidas_-_crypto_requirements_for_the_eidas_interoperability_framework_v1.0.pdf
   - Uusi 2020: Täydennetään

10) ETSI TS 119 312 V1.3.1 (2019-02) "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites" https://ec.europa.eu/cefdigital/wiki/display/EIDTECHSUB/Security+Profile+v+1.3

11) Onko muita lähteitä?

3.3 Arvioitavat kysymykset

3.3.1 Algoritmien ja salausprofiilien ajantasaisuus: oletuslistaus säännöksessä

- Mitkä säännöksessä listatut algoritmit, avainpituudet jne. ovat vanhentuneet ja poistettava?
- Mitä uusia oletusalgoritmeja on syytä lisätä?
- Tarvitaanko siirtymäaikoja?

3.3.2 Miten erotellaan tietoliikenne-, sanomatason- ja säilyttämisen salausvaatimukset?

- Miten TLS 1.2 ja 1.3 ciphersuitet päivitetään perustelumuistioon - mikä lähde (viimeksi IANA)?
- Onko tarpeen selventää perusteluissa sanomatason salausta tai kiintolevysalauksia?

3.3.3 Salausvaatimusten määrittely/tarkkuus ja sääntelytapa

- Säilytetäänkö määräyksessä tarkka listaus algoritmeista jne.?
- Miten uudet hyvät algoritmit jne. sisällytetään joustavasti mukaan sallittuihin, jos määräyksen listausta ei ehditä päivittää? Mikä tai mitkä ovat luotettavia lähteitä, joiden mukaisia algoritmeja jne. voi käyttää määräyksessä määriteltyjen oletusten lisäksi?
- Miten käsitellään haavoittuneista algoritmeista luopuminen?

3.3.4 TLS-vähimmäistaso

- Poistetaanko TLS 1.1?

3.3.5 Tietoliikenteen osapuolten tunnistus ja avaintenvaihdon vaatimukset

- Miten tunnistuspalveluiden välisen tietoliikenneyhteyden varmentamisen vaatimusta tarkennetaan (8.2 §)?
- Miten tunnistusvälityspalvelun ja asiointipalvelun tietoliikenneyhteyden varmentamisen vaatimusta tarkennetaan (9 §)?
- Miten erotetaan uuden luottosuhteen perustamisen vaatimukset ja luottosuhteen aikana tehtävän avainten uusimisen vaatimukset? Eroaako turvallisuusvaatimus luottamusverkoston sisällä ja asiointipalveluiden suuntaan?

3.3.6 Sanomatason salaus

- Onko 8 §:n ja 9 §:n tunnistussanomien sanomatason salausvaatimusta muutettava?
- Miten henkilötietoja sisältävien sanomien luottamuksellisuus voi vaarantua eri toteutuksissa?
- Mitä tunnistusmenetelmän/todentamismekanismin turvallisuuteen liittyviä tekijöitä on huomioitava: tunnistussanomien kopiointi ja mahdollinen väärinkäyttö, …?
- Onko asiaa tarkasteltava erikseen eri protokollien kannalta ja mitä protokollia vaikutusarvioinnissa on huomioitava, OIDC, SAML, ETSI, … WebAuthn/Fido…muita?
- Onko asiaa arvioitava eri tavalla tunnistuspalveluiden välillä ja suhteessa asiointipalveluun?
- Missä henkilötietoja sisältävät tunnistussanomat voivat tallentua?
- Voiko pseudonymisointi olla kokonaisarvioinnissa yksi salausta korvaava turvakeino? Vaikuttaako salaustarpeeseen se, millaista tietoa tunnistussanomassa on, esim. "on alaikäinen", "on kysytyn maksukortin haltija", "on vantaalainen", vrt. "on 121212-999Å, Alma Virtanen"?

3.4 Tarvittaessa jatkotyöpaja ~~1/1 ja~~ 2/7 ke 3.2.2021

- Pidettiin luottamusverkoston sisäisenä työpajana salausasioista.

3.5 Täydennys 26.3.2021: viraston valmistelulinjaukset, tietoliikenteen salaus, osapuolten varmentaminen, sanomien salaus

- **Salausalgoritmien ja -menetelmien ajantasaisuus, määräys 7 kohta.** Listaa täydennetään ja huomioidaan sanomatason salaus.
    - Virasto arvioi valvontakokemuksen perusteella, että vähimmäisvaatimukset on tarpeellista määrätä yksiselitteisesti. Muutokset valmistellaan kyberturvallisuuskeskuksen kryptologien kanssa.
    - Virasto katsoo, että ei ole estettä käyttää jo ennen määräysmuutoksen voimaantuloa määräykseen lisättäviä Poly1305 ja ChaCha20 -menetelmiä. Oikeudelliselta kannalta virasto linjaa, että ei puutu valvonnassa niiden käyttöön tunnistusjärjestelmässä, vaikka niitä ei ole mainittu määräyksen 7 §:ssä. Linjaus yhdistetään kirjallisesti annettavaan vuoden 2021 määräaikaisarviointien neuvontamuistioon.
- **Suositus korkean varmuustason salausvaatimuksista päivitetään ja säilytetään perusteluissa.**
    - Virasto arvioi, että korkean varmuustason suosituksen arvot ovat pääosin ajan tasalla ja ne vastaavat NCSA-toiminnon TL IV -määrittelyjä. Virasto arvioi, että korkean varmuustason suosituksen arvojen muuttaminen pakolliseksi ei aiheuttaisi yhteentoimivuusongelmia. Korkean varmuustason tunnistusvälityksen välittäessä sekä korotetun että korkean varmuustason tason tunnistusta on mahdollista valita algoritmit tapahtumakohtaisesti. Virasto toteaa, että on edellisiä seikkoja vaikeampaa arvioida, miten pakottava vaatimus vaikuttaisi korkean varmuustason tunnistuspalveluita käyttäviin asiointipalveluihin.
- **Salausalgoritmien ja -menetelmien listan joustavoittaminen, määräyksen 7 kohta**. Määräykseen lisätään viittaus NCSA:n ja SOGIS MRA:n hyväksymiin menetelmiin ja niitä voi käyttää määräyksessä listattujen lisäksi.
    - Virasto pitää NCSA:n listaa soveltuvana lähteenä, ja sitä on muutoinkin käytetty perustana ja vertailukohtana määräystä annettaessa. Toisena ajantasaisena ja relevanttina lähteenä virasto pitää SOGIS MRA:n ylläpitämää listaa. Virasto katsoo kuitenkin, että määräystä ei voi korvata viittauksella näihin lähteisiin. NCSA:n ja SOGIS MRA:n listoja ylläpidetään eri tarkoitukseen ja ne voivat joltain osin olla tarpeettoman tiukkoja korotetun varmuustason tunnistamisen vaatimuksiin nähden.
- **TLS 1.2 ehdottomaksi vähimmäistasoksi, määräys 7 kohta.** TLS 1.1 -poikkeus poistetaan määräyksestä.
    - TLS-version päivittäminen on osa tavanomaista teknistä kehittämistä. Tunnistuspalveluiden tarjonnan ja tasapuolisen kilpailun kannalta on edellisestä sääntelymuutoksesta eli TLS 1.0 kieltämisestä saadun kokemuksen perusteella hyvä, että kaikilla on velvollisuus tehdä muutos samaan aikaan. Viraston arvio sidosryhmäpalautteen perusteella on, että siirtymäaikaa vaatimukselle ei tarvita.

- **Osapuolten tunnistaminen ja avaintenvaihto, määräyksen 8 kohta.** Uusi ja osittain tarkennettu vaatimus. Tarkennetaan määräykseen vaihtoehdot tietoliikenteen osapuolen varmentamiselle (8.1) sekä avaintenvaihdon ja päivittämisen perusvaatimukset (8.2).
    - Käytännöt ja vaatimukset ovat olleet epäselvät, joten selvennetään yhtenäiset vaatimukset.
    - Teknisen toteuttamisen ja soveltamismenettelyjen tarkennuksia on selvitetty ja työstetty paljon osana toteutettavuusarviointia ja perustelujen valmistelua. Joitakin yksityiskohtia on edelleen mietittävä ja ratkaistava. Joitakin sidosryhmien esittämiä tai viraston harkitsemia teknisiä toimintamalleja avainten päivittämiselle on hylätty viraston arvioinnissa.
    - Vaatimuksen selkeyttävät toimintaa asiointipalveluiden suuntaan ja tarjoavat mahdollisuuden jossain määrin automaattiseen avainten uusimiseen. Vaatimukset saattavat tiukentaa joidenkin toimijoiden tällä hetkellä käyttämiä menettelyjä.
- **Tunnistussanomien salaus, määräyksen 9 kohta.** Tunnistussanomien kategorinen sanomatason salausvaatimus muutetaan siten, että tunnistussanomien luottamuksellisuuden turvaamiselle määritellään sanomien salauksen rinnalle vaihtoehtoinen menettely tietoliikenneyhteyden luottamuksellisuuden erityisellä varmistamisella.
    - Vaihtoehtoinen menettely on mahdollinen, jos sanomia ei välitetä käyttäjän selaimen tai päätelaitteen kautta. Tämä mahdollistaa esim. nykyisen ETSI MSS-standardia käyttävän mobiilivarmenneratkaisun ja lisää joustavuutta OIDC-toteutuksissa. SAML-toteutuksissa käytetään käyttäjän selainta, joten niissä on toteutettava aina sanomien salaus.
    - Vaatimuksen tarkoitus on, että henkilötiedot eivät paljastu oikeudettomasti käyttäjän päätelaitteen selaimessa tai palvelimilla. Tunnistussanomien salaus suojaa myös tunnistustapahtuman väärentämiseltä ja toisintamiselta (tamper/replay). Salausmenettelyllä turvataan osaltaan sitä, että vahvistus autentikoinnista ja henkilötiedot toimitetaan todentamisessa vain oikealle asiointipalvelulle. Siten ei ole perusteita erotella salausvaatimusta luottamusverkoston sisällä ja luottamusverkosto ja asiointipalveluiden välillä. Henkilötunnusta koskee tietosuojasääntelyssä erityinen suoja, mutta ei ole objektiivista perustetta rajata muitakaan henkilötietoja suojan ulkopuolelle.
    - Salauksen teknisessä toteuttamisessa viitataan 7 kohtaan ja sitä on muutettu siten, että se soveltuu myös sanomatason salaukseen.

4 3/7 työpaja: KE 10.2.2021 Tunnistusjärjestelmän tekniset vaatimukset ja arviointi

4.1 Määräyksen nykyiset säännökset

Tekniset vaatimukset
- *Luku 2 Tunnistuspalvelun tietoturvavaatimukset*
- *4 § Tunnistuspalvelun tarjoajan tietoturvallisuuden hallinnan vaatimukset*
- *5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet*
- *11 § Tunnistuspalveluntarjoajan häiriöilmoitukset Viestintävirastolle*

Vaatimustenmukaisuuden arviointi

- *Luku 4 Tunnistuspalvelun arviointikriteerit*
- *15 § Arviointikriteerit*
- *16 § Selvitys muiden vaatimusten täyttämisestä*
- *17 § Kansallisen solmupisteen arviointiperusteet*
- *Luku 5 Tunnistuspalvelun arviointielimen pätevyys*
- *18 § Tunnistuspalvelun ulkoisen arviointielimen vaatimukset*
- *19 § Tunnistuspalvelun sisäisen tarkastuslaitoksen vaatimukset*

4.2 Pohjamateriaali, lähteet, referenssit

1) Liikenne- ja viestintäviraston kysely 4.8.2020 tunnistus- ja luottamuspalvelumääräyksen 72 ja muun teknisen ohjauksen muutostarpeista
2) Liikenne- ja viestintäviraston valmistelumuistio 2020-2021 tunnistusjärjestelmän tekniset vaatimukset (jaetaan 1 - 2 viikkoa ennen työpajaa)
3) Liikenne- ja viestintäviraston valmistelumuistio 2020-2021 tunnistusjärjestelmän vaatimustenmukaisuuden arviointi (jaetaan 1 - 2 viikkoa ennen työpajaa)

Tekniset vaatimukset

4) ISO/IEC 27001:2013 Information security management tai uudempi
5) Häiriönhallinnan ISO/IEC xx
6) LoA Guidance EU:n varmuustasoasetuksen epävirallinen soveltamisohje
   - https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Guidance+documents
   - Suomenkielinen käännös https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LOA_Guidance_Final_suomeksi.pdf
7) ETSI EN 319 401 V2.1.1 Electronic Signatures and Infra-structures (ESI); General Policy Requirements for Trust Service Providers
8) Enisa [täydennetään tarvittaessa]
9) NISTin (National Institute of Standards and Technology) FIPS-standardit (Federal Information Processing Standards) www.nist.gov
10) SANS (The SANS Institute) www.sans.org
11) Liikenne- ja viestintäviraston kyberturvallisuuskeskuksen NCSA (National Communications Security Authority, NCSA-FI)
   - [TBD poimintoja turvallisuusohjeista]
12) KATAKRI, Tietoturvallisuuden auditointityökalu viranomaisille
   - https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/ncsa
13) PiTuKri, Pilvipalveluiden turvallisuuden arviointikriteeristö
   - https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/ncsa

Arviointivaatimukset

14) BIS, Bank for International Settlements:
   - External audits of banks http://www.bis.org/publ/bcbs280.htm,
   - The internal audit function in banks http://www.bis.org/publ/bcbs223.htm
15) Finanssivalvonnan määräys- ja ohjekokoelma
   - https://www.finanssivalvonta.fi/saantely/maarays-ja-ohjekokoelma/
16) IIA, ISACA, muut 18 ja 19 §:n lähteet
   - www.theiia.fi
   - [Täydennetään]

4.3 Arvioitavat kysymykset

4.3.1 Tietoturvallisuuden hallinnan vaatimusten selkeyttäminen (4 §)

- Kattaako 4 § selvästi tarpeelliset tunnistusjärjestelmän hallinnan osa-alueet? Vaatiiko määräyksen tai perustelujen selventämistä?
- Onko vaatimusta tietoturvallisuuden hallinnan standardien noudattamisesta/käyttämisestä tarkasteltava/tarkennettava/tiukennettava?
- Mitkä standardit ovat relevantteja tietoturvallisuuden hallinnan kannalta ISO 27001 lisäksi? (PCIDSS, …?)

4.3.2 Tunnistusjärjestelmän tekniset vaatimukset (5 §)

- Varmuustasojen vaatimusten eriyttäminen? Kautta linjan tai yksittäisten vaatimusten kannalta - minkä vaatimusten?
- Perustelumuistion täydentäminen ja esimerkkien lisääminen (esim. tunnistusjärjestelmän arviointiohjeen, Katakrin ja/tai Pitukrin avulla)?
- Vaatimusten tarkentaminen?
  - Prosessivaatimusten, kuten haavoittuvuusskannausten lisääminen säädettyihin vaatimuksiin?
  - Pääsyoikeuksien hallinnan ja minimoinnin tarkennustarpeet, pääkäyttäjäteemat yms.?

4.3.3 Häiriöilmoituskynnys - toimivuushäiriöiden merkittävyys (11 §)

- Onko tarpeellista tiukentaa toimivuushäiriöiden ilmoitusvaatimusta viranomaiselle, jotta valvova viranomainen saa kokonaiskuvan toimivuushäiriöistä?
- Mikä olisi ilmoituskynnys (tunnit, käyttäjämäärät, …)?

4.3.4 Arviointi (15 §, 17 §, 18 §, 19 §)

- Ovatko 18 § ja 19 §:n viittaukset soveltuvia ja ajan tasalla
- Onko perustelumuistion esimerkkistandardilista arvioinnille soveltuva, ajan tasalla ja hyödyllinen
- Solmupisteen tietoturvallisuuden arvioinnin perusteet (17 §)
  - DVV toivonut arviointia ja komission eIDAS-työryhmässä ollaan selvittämässä asiaa.

~~4.4 Tarvittaessa jatkotyöpaja 3/7 ke 17.2.2021~~

4.5 Täydennys 26.3.2021: viraston valmistelulinjaukset, tunnistusjärjestelmän tekniset vaatimukset ja arviointi, häiriöilmoitukset

- **Tietoturvallisuuden hallinta, määräyksen 4 kohta.** Säännöksen sanamuotoa muutetaan siten, että valittua tai valittuja tietoturvallisuuden hallinnan standardeja on noudatettava, ei ainoastaan käytettävä.
  - Muutos tiukentaa vaatimusta hienoisesti. Tarkoitus on korostaa tunnistuspalvelun tarjoajan johdon sitoutumisen merkitystä ja tietoturvallisuuden hallintajärjestelmän ja prosessien ylläpidon merkitystä.
  - Määräysmuutostarvekyselyssä annetussa palautteessa ehdotettiin, että säännöksen sanamuotoa tiukennettaisiin tai tarkennettaisiin siten, että edellytetään standardin noudattamista tai sertifiointia. Liikenne- ja viestintävirasto arvioi, että ehdoton sertifiointivaatimus olisi taloudellisesti raskas ja

soveltuisi huonosti siihen tilanteeseen, että tietoturvallisuuden hallinnasta huolehditaan usean standardin yhdistelmällä.

- Korkeallakaan tasolla ei määrätä pakolliseksi sertifiointia, mutta tietoturvallisuuden hallinnan toteutusta ja tehokkuutta arvioidaan kautta linjan tiukasti. Tietoturvallisuuden hallinnan on oltava poikkeuksetta kattavaa, johdonmukaista ja aktiivista.

- **Tunnistusjärjestelmän turvallisuus ja luotettavuus/tekniset tietoturvavaatimukset, määräyksen 5 kohta.** Lisätään säännös, jolla tarkennetaan tunnistusjärjestelmän turvatoimenpiteiden ja teknisten määrittelyjen kokonaisuuden vaatimustaso viittauksella hyökkäyksensietokykyyn. Muutoin tietoliikenne-, tietojärjestelmä- ja käyttöturvallisuuden vaatimuksia tarkennetaan ja perusteluja lisätään valvonta ja -soveltamiskäytännön mukaisesti. Etähallinnan tarkennettuja eriyttämisvaatimuksia ei muuteta.

  - Tulkinnallisesti hyökkäyksensiedon vaatimustaso olisi johdettavissa myös laista, mutta asiaa halutaan selkeyttää määräyksessä. Korotetun ja korkean varmuustason yksittäisiä vaatimuksia ei pääsääntöisesti ole määritelty määräyksessä erikseen. Virasto katsoo, että varmuustasojen vaatimusten tarkentaminen määräyksessä ei ole mahdollista, koska tunnistusjärjestelmään sisältyy lukuisia osatekijöitä. Yksityiskohtainen määrääminen ei olisi tarkoituksenmukaista, koska tekniset toteutukset ja uhkat muuttuvat jatkuvasti.

- **Suositus tunnistusjärjestelmän kellonajan luotettavuudesta siirretään muutettuna osaksi määräyksen 5 kohdan perusteluja.**

  - Tärkeä osatekijä lokituksessa ja niiden aikaleimoissa ja muutoinkin keskeinen perusvaatimus.

- **Häiriöilmoitukset, määräyksen kohta 11**. Tarkennetaan sanamuotoa, mutta ilmoituskynnystä ei muuteta.

  - Virasto ei pidä tarkoituksenmukaisena tai tarpeellisena laatia määräykseen toimivuushäiriöille uusia ilmoituskynnyksiä. Arviota ei muuteta vuonna 2016 tehdystä arviosta. On myös huomattava, että tunnistuslaissa ei ole nimenomaisia vaatimuksia tunnistuspalveluiden toimintavarmuudesta, varmistamisesta tai varautumisesta eikä siten toimivaltuutta määrätä niistä.

  - Viraston kyselyyn määräyksen muutostarpeista annetuissa vastauksissa esitettiin huoli, että kaikki eivät ilmoita häiriöistä virastolle riittävän alhaisella kynnyksellä ja että kaikki tunnistuspalvelut eivät informoi toisiaan häiriötilanteista. Virasto arvioi, että näihin havaintoihin on vaikutettava ensisijaisesti valvonnalla ja tehostamalla edelleen luottamusverkoston keskinäistä informointia. Luottamusverkoston toimijoiden keskinäinen häiriöinformointi ei kuulu määräystoimivallan piiriin, vaan on valvonta-asia.

- **Arviointikriteerit ja arviointielimet, määräykset 15, 18 ja 19 kohdat.** Säännösten sanamuotoja selkeytetään ja perusteluissa täydennetään ja päivitetään informatiivisia arviointireferenssejä.

5 4/7 työpaja: KE 10.3.2021 Tunnistusmenetelmä vrt. PSD2, Blockchain ja SSI

5.1 Määräyksen nykyiset säännökset

- *6 § Tunnistusmenetelmän tietoturvavaatimukset*

5.2 Pohjamateriaali, lähteet, referenssit

1) Liikenne- ja viestintäviraston kysely 4.8.2020 tunnistus- ja luottamuspalvelumääräyksen 72 ja muun teknisen ohjauksen muutostarpeista
   - https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Traficomin%20kysely%2004082020%20tunnistus-%20ja%20luottamuspalvelumuutostarpeista.pdf
2) Liikenne- ja viestintäviraston valmistelumuistio 2020-2021 todentamistekijät vrt. PSD2 (jaetaan 1 - 2 viikkoa ennen työpajaa)
3) Biometristen viitteet [täydennetään tarvittaessa]
4) Tunnuslukulaitteet [täydennetään tarvittaessa]
5) (EU) 2015/1502 komission varmuustasoasetus (eIDAS-varmuustasoasetus)
6) eIDAS LOA Guidance 2016, eIDAS yhteistyöverkoston soveltamisohje
   - EN: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Guidance+documents
   - Suomenkielinen käännös https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LOA_Guidance_Final_suomeksi.pdf
7) (EU) 2018/389 komission delegoitu asetus direktiivin (EU) 2015/2366 (PSD2) täydentämisestä asiakkaan vahvaa tunnistamista sekä yhteisiä ja turvallisia avoimia viestintästandardeja koskevilla teknisillä sääntelystandardeilla (RTS SCA & CSC).
   - (EU) 2018/389 https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32018R0389&from=EN
8) Euroopan pankkiviranomaisen (EBA) kannanotot ja tulkinnat Opinion RTS SCA & CSC:n tulkinnasta
   - EBA-Op-2018-04 RTS SCA & CSC:n tulkinnasta https://eba.europa.eu/sites/default/documents/files/documents/10180/2137845/0f525dc7-0f97-4be7-9ad7-800723365b8e/Opinion%20on%20the%20implementation%20of%20the%20RTS%20on%20SCA%20and%20CSC%20%28EBA-2018-Op-04%29.pdf
   - EBA-Op-2019-06 Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 https://eba.europa.eu/sites/default/documents/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf
   - EBA PSD2 Q&A prosessin mukaisia vastauksia, jotka koskevat RTS SCA & CSC sääntelyä. Työkalussa oli 25.5.2020 nähtävissä 79 tulkintavastausta. https://eba.europa.eu/single-rule-book-qa/search?field_legal_act%5B%5D=517&field_legal_act_topic%5B%5D=676&field_qa_com%5B%5D=927&items_per_page=20

5.3 Arvioitava kysymykset

5.3.1 Todentamistekijöiden turvallisuusvaatimusten tarkentaminen (6 §)

- Mitä sellaisia turvallisuusnäkökohtia todentamistekijöihin liittyy, joille olisi asetettava vaatimuksia määräyksessä
  - Tunnuslukulista: Pidetäänkö paperista tunnuslukulistaa riittävän turvallisena?

- Mobiilisovellus: Voidaanko turvattomaksi todettuja mobiililaitteita (laitteistotason haavoittuvuuksien takia) ja käyttöjärjestelmiä käytännössä rajata tunnistusmenetelmän ulkopuolelle ja miten se tehdään?
- tunnuslukulaitteet, SMS, biometrinen todentamistekijä, salasanakäytännöt yms.
- Mitä PSD2-sääntelyn rinnakkaisia vaatimuksia voi hyödyntää

- Miten tunnistusmenetelmän ominaispiirteitä vrt. todentamistekijöiden riippumattomuusvaatimusta voidaan tarkentaa?
  - Mitä PSD2-sääntelyn rinnakkaisia vaatimuksia voi hyödyntää

5.3.2 Blockchain, SSI -keskustelu ja EU-lähteet

1) SSI eIDAS Legal Report (How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market), Dr. Ignacio Alamillo Domingo April – 2020
   - https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf
2) European Blockchain Partnership (EBP) and cooperate in the establishment of a European Blockchain Services Infrastructure (EBSI)
   - https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership

~~**5.4 Tarvittaessa jatkotyöpaja 4/7 ke 17.3.2021**~~

5.5 Täydennys 26.3.2021: viraston valmistelulinjaukset, tunnistusmenetelmä

- **Tunnistusmenetelmän turvallisuus, määräyksen 6 kohta.** Tunnistusmenetelmän todentamistekijöiden ja kokonaisuuden turvallisuusvaatimuksia tarkennetaan lisäämällä määräykseen vaatimukset erityisen uhka- ja riskiarviosta ja siinä huomioitavista seikoista. Lisätään myös vaatimus turvatoimenpiteistä todentamistekijöiden riippumattomuuden varmistamiseksi.

- Valitussa sääntelymallissa tarkennetaan riskiarvion tekemisen vaatimusta ja osatekijöitä, jotka siinä on otettava huomioon. Todentamistekijöiden ja todentamismekanismin riskit on arvioitava erikseen ja tunnistusmenetelmän suojautumiskyvyn on perustuttava varmuustason mukaiseen uhka- ja riskiarvioon. Virasto arvioi, että tällainen malli on tarpeeksi joustava eri tunnistusmenetelmien ja todentamistekijöiden suhteen ja huomioi tunnistusmenetelmän turvakontrollit kokonaisuutena. Viraston mahdolliset valvontaratkaisut tulisivat perustumaan tunnistuspalvelun tarkkaan riskiarvioon, jossa huomioidaan myös turvakontrollien vaikutus. Sidosryhmäpalautteen perusteella riskilähtöinen lähestymistapa on toimiva, mutta on hyvä ohjeistaa, mitä arvioidaan ja millä metodilla, jotta jäännösriskin hyväksyttävyys on mahdollisimman ennakoitava. Virasto arvioi sidosryhmäpalautteen perusteella, että vaatimukselle ei tarvita siirtymäaikaa.

- Virasto on arvioinut **vaihtoehtoina** sääntelymalleja, joissa määräyksessä tarkennettaisiin todentamistekijäkohtaiset vaatimukset tai tarkennettaisiin tunnistusmenetelmän suojautumiskyvyn vaatimukset. Todentamistekijäkohtaiseen sääntelytapaan liittyisi todentamistekijöiden moninaisuuden ja kehittymisen takia paljon yksityiskohtia, joita ei ole viraston arvion mukaan mahdollista eikä tarkoituksenmukaista pyrkiä kattamaan säännöstasolla. Myöskään uhkat tunnistusmenetelmän turvallisuudelle ja turvakeinot uhkilta suojaamiselle eivät ole puhtaasti todentamistekijätyyppikohtaisia. Suojautumiskyvyn mittareita tai muunlaisia tarkennuksia määräyksessä voisi ajatella

määriteltäväksi viittauksella johonkin yleisesti käytettyyn riskiarviostandardiin. Virasto katsoo, ettei standardien soveltuvuudesta kaikkiin tunnistusmenetelmiin ole riittävästi tietoa, jotta niihin olisi perusteltua viitata määräyksessä velvoittavana. Sen sijaan virasto katsoo, että suojautumiskyvyn vaatimusta voidaan tarkentaa määräyksessä listaamalla osatekijöitä, joita arvioinnissa on huomioitava.

- **Tunnistusmenetelmän turvallisuus, salaus ja käyttäjälle näytettävät tiedot määräyksen 6 kohta.** Arvioidaan vielä tarve täydentää säännöksessä salausvaatimukset käyttäjän ja tunnistusvälineen tarjoajan välillä todentamisessa täydentämään 7 ja 9 kohtien salauskokonaisuutta. Säännökseen lisätään velvoitteet tunnistuspyynnön yksilöintitiedosta ja asiointipalvelun nimestä.
    - Salausvaatimusten tarkastelun tarkoitus on, että vähintään nykyisen määräyksen 7 §, 8 § ja 9 § kokonaisuus katetaan.
    - Tunnistuspyynnön yksilöintitiedon (session binding) tarkoitus on sitoa/yhdistää selain/sovellusistunto tunnistustapahtumaan ja mahdollistaa tunnistusvälineen käyttäjälle väärien/petollisten tunnistuspyyntöjen vahvistamatta jättäminen. Vaatimus koskee vain tunnistusmenetelmää, jossa on oma näyttö. Toteutustapaa ei määrätä. Mahdolliseen siirtymäajan tarpeeseen ei ole saatu vielä kattavasti palautetta.
    - Tieto kohdepalvelusta (SP/RP –name) tulossa määräyksen 12 kohdassa pakolliseksi attribuutiksi. Määräyksen 6 kohdan vaatimuksen tarkoitus on, että käyttäjälle näytetään sen asiointipalvelun nimi, johon vahvistus tunnistuksesta on pyydetty ja menossa. Tämä vähentää osaltaan riskiä siitä, että käyttäjää johdetaan harhaan siitä, mihin asiointipalveluun hän on tunnistautumassa. Tunnistusvälityspalvelu tuottaa SPname-attribuutin (luottava osapuoli, jolle tunnistus ollaan välittämässä). Attribuutti on ollut määriteltynä rajapintasuosituksiin, joten valmius voi olla osalla tunnistusvälineen tarjoajista jo määriteltynä rajapinnoissa. Tunnistustapahtumien toteutus ja käyttäjää informoiva taho tunnistusketjussa vaihtelee, joten ei ole tarkoituksenmukaista määritellä sitovasti, näyttääkö tiedon käyttäjälle tunnistusvälityspalvelu vai tunnistusvälineen tarjoaja.

6 5/7 työpaja: TO 15.4.2021 Luottamuspalvelut ja akkreditoidut arviointilaitokset

6.1 Määräyksen nykyiset säännökset

Luku 6 Hyväksytyt luottamuspalvelut (QTSP, QTS)
- *20 § Hyväksytyn luottamuspalvelun tarjoajan arviointikriteerit*
- *21 § Hyväksytyn luottamuspalvelun arviointikriteerit*

Luku 7 Luottamuspalvelujen vaatimustenmukaisuuden arviointilaitokset (CAB)
- *22 § Arviointilaitosten pätevyyden arviointi*

Luku 8 Hyväksytyn sähköisen allekirjoituksen ja sähköisen leiman luontivälineen sertifiointi (QSCD)
- *23 § Sähköisen allekirjoituksen tai leiman luontivälineen vaatimukset*
- *24 § Sertifiointilaitosta koskevat vaatimukset*

6.2 Pohjamateriaali, lähteet, referenssit

1) Liikenne- ja viestintäviraston kysely 4.8.2020 tunnistus- ja luottamuspalvelumääräyksen 72 ja muun teknisen ohjauksen muutostarpeista
2) Liikenne- ja viestintäviraston valmistelumuistio 2020-2021 luottamuspalvelut ja akkreditoidut arviointilaitokset (jaetaan 1 - 2 viikkoa ennen työpajaa)
3) ETSIn standardit
   - https://www.etsi.org/standards-search#page=1&search=&title=1&etsiNumber=1&content=1&version=1&onApproval=1&published=1&historical=1&startDate=1988-01-15&endDate=2020-06-06&harmonized=0&keyword=&TB=607&stdType=&frequency=&mandate=&collection=&sort=3
4) Enisan guidelinet
   - https://www.enisa.europa.eu/publications#c5=2010&c5=2020&c5=false&c2=publicationDate&reversed=on&b_start=0
5) Onko muita?

6.3 Arvioitavat kysymykset

6.3.1 ETSI-standardiviittausten päivittäminen ja täydentäminen (20 §, 21 §)

- Määräyksen vaatimukset hyväksytyille luottamuspalveluille perustetaan niihin ETSI:n standardeihin, joita on saatu valmiiksi kullekin luottamuspalvelutyypille komission standardointimandaatin nojalla.
- Määräykseen lisätään voimassa olevat standardiviittaukset

6.3.2 Arviointilaitoksen ja arviointikertomuksen standardiviittaukset (22 §)

- Arvioidaan, onko syytä lisätä määräykseen ETSI-standardin (ml. uusi osa arviointikertomuksesta) vaatimukset luottamuspalveluiden akkreditoitujen vaatimustenmukaisuuden arviointilaitokselle ja arvioinnille

6.3.3 Kehittyneen allekirjoitus- tai leimapalvelun kysymykset eivät sisälly määräykseen

- Kehittyneen sähköisen allekirjoituksen vaatimukset eivät kuulu sääntelytoimivaltaan
- Niitä koskevat informatiiviset osat vuoden 2016 perustelumuistiosta poistetaan ja käsitellään tarvittaessa muussa yhteydessä.

6.4 Tarvittaessa jatkotyöpaja 5/7 ke 21.4.2021

7 Täydennys 26.3.2021: 6/7 työpaja: KE 12.5.2021 tunnistuspalvelun ja arvioinnin vaatimuksiin tehtävät muutokset

7.1 Määräyksen nykyiset säännökset

numerot viittaavat määräyksen säännöksiin (§-merkkiä ei enää käytetä)

- 1. soveltamisala
- 3. määritelmät
- 4. tietoturvallisuuden hallinta
- 5. tekniset tietoturvavaatimukset (kokonaisuus) ja varmuustasot
- 6. tunnistusmenetelmä, todentamistekijät
- 7. salausvaatimusten sääntelymalli ja tekninen ajantasaisuus
- 8. osapuolten varmentaminen, avaintenvaihto
- 9. sanomatason salaus
- 11. häiriötilanteiden hallinta

- 12. tunnistuspalveluiden attribuutit
- 14. tunnistuspalveluiden rajapinnat
- 15., 18., 19. vaatimustenmukaisuuden arviointi

7.2 Pohjamateriaali, lähteet, referenssit

- Määräysluonnos ja perustelumuistioluonnos julkaistaan verkkosivulla arviolta 3.5.
- Linjaukset 26.3.2021 ilmenevät edellä työpajojen kohdalla
- Työpajojen valmistelumuistioissa ja työpajoista julkaistuilla kalvoilla näkyy tarkempia tietoja. Valmistelumuistioita ei päivitetä, vaan valmistelu jatkuu määräys- ja perustelumuistioluonnoksessa.

7.3 Arvioitavat kysymykset

- Käsitellään kokonaisuus ja tarvittaessa tarkemmin viraston tai toimijoiden nostot määräysmuutoksista

7.4 Tarvittaessa jatkotyöpaja 6/7 to 20.5.2021

- Jatketaan tarvittaessa kokonaisuuden tai yksittäisten säännösten käsittelyä, jos siihen jää 12.5. työpajan jälkeen tarvetta.

8 7/7 työpaja: TO 10.6.2021, koko muutetun määräyksen läpikäynti

8.1 Pohjamateriaali ja lähteet

- Määräysluonnos (lausuntokierrokselle valmis versio)
- Perustelumuistioluonnos (lausuntokierrokselle valmis versio)

9 Palautetilaisuus: lokakuu 2021, lausuntokierroksen yhteenvedon ja viraston linjausten käsittely

9.1 Pohjamateriaali ja lähteet

- Lausuntoyhteenveto ja viraston linjaukset
- Määräysluonnos (lausuntojen perusteella tehdyt muutokset)
- Perustelumuistioluonnos (lausuntojen perusteella tehdyt muutokset)

9.2 Määräysmuutosten täytäntöönpano ja tiedottaminen

- ✓ Viraston toimenpiteet
- ✓ Tunnistuspalveluiden ja muiden sidosryhmien toimenpiteet?
- ✓ Yhteiset toimenpiteet?
- ✓ Tiedotuskanavat
- ✓ Mahdolliset valvontasuunnitelmat