

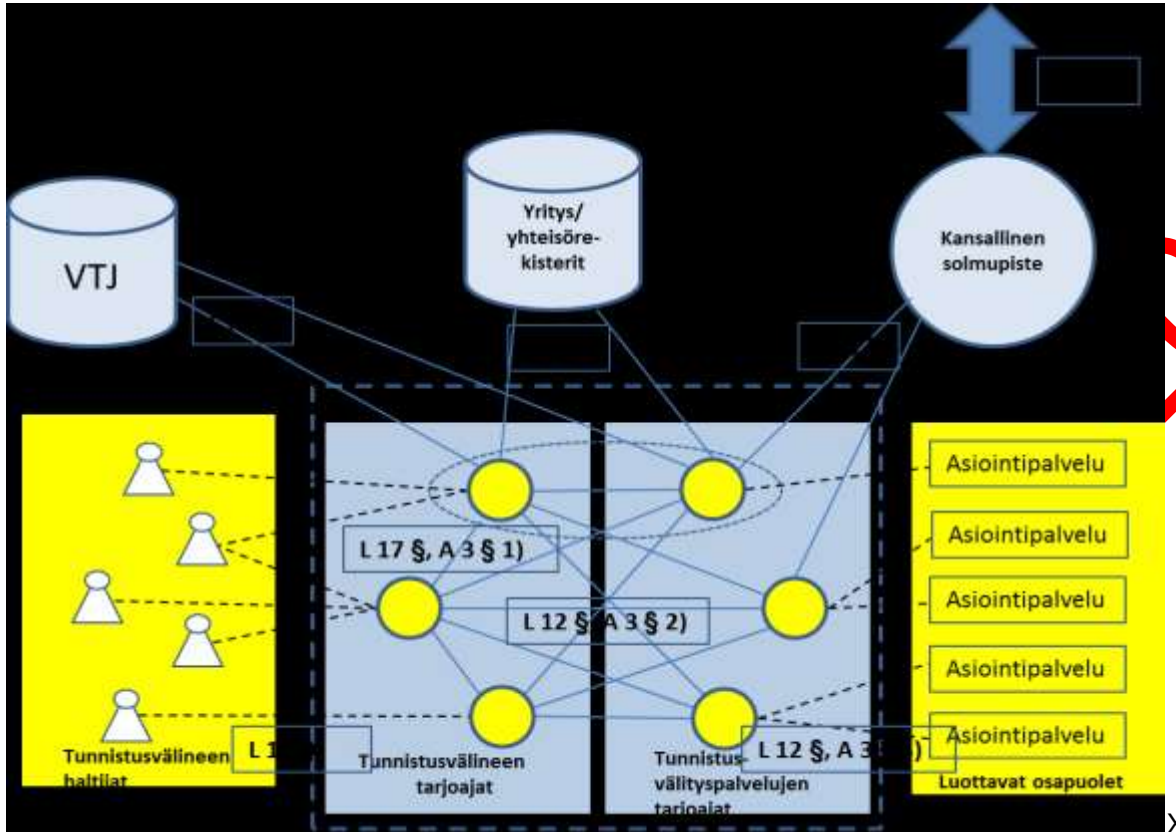
Määräys 72 valmistelumuistio 2020-2021: tunnistusrajapinnat ja attribuutit

Sisällys

1	Kuvat	3
2	Säännös ja perustelut (voimassa olevat)	3
2.1	Säännös 3 § Määritelmät	3
2.1.1	Perustelut	4
2.2	Säännös 12 § Luottamusverkostossa välitettävät vähimmäistiedot	4
2.2.1	Perustelumuistio	5
2.3	Säännös 13 § Rajat ylittävän tunnistamisen edellyttämät tiedot	6
2.3.1	Perustelumuistio	6
2.4	Säännös 14 § Tiedonsiirrossa käytettävä protokolla ja muut vaatimukset	7
2.4.1	Perustelumuistio	8
3	Lähteet 2020-2021 vaikutusarviointiin	8
3.1	Yleiskuvaus lähtötilanteesta	8
3.1.1	Määräyksessä säännelty luottamusverkoston rajapinnat	8
3.1.2	Luottamusverkoston rajapinnat, joista ei määrätä	9
3.1.3	Rajapintaprotokollat, viraston arvio kyselyssä 2020 (OIDC ja SAML)	10
3.1.4	Tunnistamisessa välitettävät attribuutit, kyselyn 2020 arvio (12 §) ..	10
3.1.5	Valinnaiset attribuutit, viraston arvio kyselyssä 2020	11
3.2	Vuonna 2016 ja 2018 vaikutusarvioinneissa linjatut asiat	11
3.2.1	Pakolliset attribuutit 2016 (12 §)	11
3.2.2	Valinnaiset attribuutit 2016 ja 2018 (12 § ja 25 § siirtymäsäännös)	12
3.2.3	Sähköinen ensitunnistus (ensitunnistamisen ketjutus)	15
3.2.4	Protokollat 2016 (14 §)	16
3.3	Lähteet, referenssit	17
3.4	Toimialakysely 2020 muutostarpeista	17
3.4.1	Rajapinnat	17
3.4.2	Kysymykset attribuuteista	19
3.4.3	Kysymykset rajat ylittävästä tunnistamisesta	20
4	Muutosvaihtoehdot ja vaikutusarviointi	21
4.1	Luonnollisen henkilön pakolliset attribuutit (12 §)	21
4.1.1	Arvioitavat vaihtoehdot ja linjaukset	21
4.1.2	Tunnistuspalveluiden kehitys ja toteutettavuus	21
4.1.3	Turvallisuusvaikutukset	21
4.1.4	Taloudelliset vaikutukset	22
4.1.5	Muut ohjauskeinot	22
4.2	Luonnollisen henkilön valinnaiset attribuutit (12 §)	22
4.2.1	Arvioitavat vaihtoehdot ja linjaukset	22
4.2.2	Tunnistuspalveluiden kehitys	23
4.2.3	Taloudelliset vaikutukset	23
4.2.4	Muut ohjauskeinot	23
4.3	Ensitunnistamisen attribuutit	23
4.3.1	Arvioitavat vaihtoehdot ja linjaukset	23

4.3.2	Tunnistuspalveluiden kehitys, toteutettavuus	24
4.3.3	Turvallisuusvaikutukset.....	24
4.3.4	Taloudelliset vaikutukset.....	24
4.3.5	Muut ohjauskeinot.....	25
4.4	Muut attribuutit ("rikastaminen") tai tunnistuksen pseudonymisointi/köyhdyttäminen	25
4.4.1	Tunnistuspalveluiden kehitys ja toteutettavuus	25
4.4.2	Turvallisuus ja yhteentoimivuus	26
4.4.3	Taloudelliset vaikutukset.....	26
4.4.4	Muut ohjauskeinot.....	26
4.5	Rajapintaprotokollat ja tekninen yhteentoimivuus (14 §)	26
4.5.1	Tunnistuspalveluiden kehitys ja toteutettavuus	26
4.5.2	Taloudelliset vaikutukset.....	27
4.5.3	Muut ohjauskeinot.....	27
4.6	Protokollien tai rajapintamäärittysten vaikutus asiointipalveluiden toimintoihin ...	27
4.6.1	Tunnistuspalveluiden kehitys.....	27
4.6.2	Turvallisuus ja yhteentoimivuus	27
4.6.3	Taloudelliset vaikutukset.....	27
4.6.4	Muut ohjauskeinot.....	27
5	Säädäntö	28
5.1	Määräyksen antamisen perusta	28
5.2	Asiaan liittyvät säännökset.....	28
5.3	Muu sääntely.....	31

1 Kuvat



[Kuva MPS72 vuodelta 2016, säännösviittaukset vanhentuneet]

TO DO [Attribuutit]

2 Säännös ja perustelut (voimassa olevat)

Tähän on koottu voimassa olevasta määräyksestä **Viestintävirasto 72/2018 M sähköisistä tunnistus- ja luottamuspalveluista** säännökset, joiden muutostarvetta muistiossa arvioidaan.

Tähän on koottu myös säännösten perustelut ja soveltamisohjeet **perustelumui-
tiosta MPS72**. Perustelumui-
stion 14.5.2018 päivytyssä versiossa ovat mukana
vuoden 2016 perustelut ja 2018 osittaismuutoksen perustelut. Perustelut päivite-
tään muutoksen yhteydessä.

Koko määräys ja perustelumui-
stio Finlexissä <https://www.finlex.fi/fi/viranomaiset/normi/480001/42947>

2.1 Säännös 3 § Määritelmät

3 § määritelmät

Tässä määräyksessä tarkoitetaan:

- 1) rajapinnalla tiedonsiirtoon liittyviä määrittelyjä ja toteutuksia kahden eri järjestelmän tai niiden osien välillä;
- 2) eIDAS-rajapinnalla kansallisen solmupisteen rajapintaa toisen valtion kansalliseen solmupisteeseen.

Muutoin tässä määräyksessä sovelletaan samoja määritelmiä kuin tunnistus- ja luottamuspalvelulaissa ja eIDAS-asetuksessa.

2.1.1 Perustelut

Rajapinnan määritelmä kattaa tiedonsiirtoon käytetyn protokollan mukaisten tekijöiden tarkemman määrittelyn ja valinnaiset tekijät. Se kattaa myös käytännön toteutuksen eli siirrettävien tietosisältöjen valikoiman ja muodon.

Määräyksen kannalta keskeisiä ovat myös useat tunnistuslain 2 §:ssä ja eIDAS-asetuksen 3 artiklassa säädetyt määritelmät. Nämä on kuvattu tarkemmin A osan luvussa 1.4.

2.2 Säännös 12 § Luottamusverkostossa välitettävät vähimmäistiedot

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,
- 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 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) arvonnäkövero- ja verotunniste;
 - c) verorekisterinumero;
 - d) Euroopan parlamentin ja neuvoston direktiivin 2009/101/EY¹ 3 artiklan 1 kohdassa tarkoitettu tunniste;
 - e) komission täytäntöönpanoasetuksessa (EU) N:o 1247/2012² tarkoitettu oikeushenkilötunnus (LEI);

¹ 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).

² Komission täytäntöönpanoasetus (EU) N:o 1247/2012, annettu 19 päivänä joulukuuta 2012, kauppätietorekistereihin OTC- johdannaisista, keskusvastapuolista ja kauppätietorekistereistä 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).

- f) komission täytäntöönpanoasetuksessa (EU) N:o 1352/2013³ tarkoitettu taloudellisen toimijan rekisteröinti- ja tunnistenumero (EORI-numero); sekä
- g) neuvoston asetuksen N:o 389/2012⁴ 2 artiklan 12 kohdassa tarkoitettu valmisteveronumero.

2.2.1 Perustelumuistio

Pykälässä määritellään tiedot eli attribuutit, joita tunnistustapahtumassa täytyy välittää tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun välillä tai joiden välittämiseen täytyy olla valmius. Attribuutit vastaavat EU:n komission yhteentoimivuusasetuksessa (EU) 2015/1501 [23] määriteltyjä pakollisia ja valinnaisia tietoja.

Pykälän tarkoitus on turvata se, että tunnistusvälineen ja tunnistusvälityspalvelun tarjoajat pystyvät sopimaan sujuvasti tunnistustapahtumien välityksestä tarvitsematta määritellä attribuutteja erikseen jokaisessa sopimussuhteessa. Tarkoitus on myös varmistaa se, että kotimaisia tunnistusvälineitä voidaan käyttää rajat ylittävässä asiointinnissa, jos tunnistusvälineitä notifioidaan EU:lle.

Pakolliset tiedot

Pykälän 1 momentissa määrätään ne tunnistetiedot, jotka tunnistusvälineen tarjoajan on välitettävä tunnistustapahtumassa tunnistusvälityspalvelulle.

Luonnollisen henkilön tunnistustapahtumassa tulee välittää henkilön yksilöivä tunniste, joka on joko henkilötunnus (HETU) tai henkilön sähköinen asiointitunnus (SATU) säädösten sen salliessa. Osapuolet sopivat käytettävästä yksilöivästä tunnistuksesta keskenään. Lisäksi tunnistetietoihin sisältyvät henkilön etu- ja sukunimi ja syntymäaika.

Oikeushenkilön tunnistustapahtumassa tulee välittää ainakin oikeushenkilöä edustavan luonnollisen henkilön yksilöivä tunniste, henkilön sukunimi, henkilön etunimi ja organisaation tunniste.

Kansallisessa luottamusverkostossa käytettävän tunnistusvälineen varmuustaso voi olla eIDAS-asetuksen määrittelemä korotettu tai korkea. Tieto välineen varmuustasosta tulee välittää tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa.

Valinnaiset tiedot, perustelut

Määräyksen 25 §:n 4 momentissa määrätään siirtymäaika valmiudelle välittää 2 momentissa tarkoitettuja valinnaisia attribuutteja luottamusverkostossa käytettävässä rajapinnassa. Siirtymäaika olisi sama kuin Tupas-siirtymän määrittelyn määräaika eli 1.10.2018.

Rajat ylittävälle tunnistamiselle olisi tarvetta jo nyt ja kysyntä on lisääntymässä myös yksityisellä sektorilla. Valinnaisten attribuuttien tarkoitus on tukea tunnistusta ja asiointia niissä tilanteissa, joissa pakolliset attribuutit eivät ole riittäviä.

³ 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).

⁴ 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).

Viestintävirasto katsoo, että valmiutta on tarkoituksenmukaista lisätä asteittain ja huomioiden yritysten järjestelmien kehittämisen aikataulut. Ensivaiheessa on riittävä, että attribuutit huomioidaan tunnistusjärjestelmän suunnittelussa. Viestintävirasto arvioi, että suunnittelu nopeuttaa käyttöönottoa tarvittaessa. Tässä voidaan tukeutua Viestintäviraston julkaisemiin SAML- ja OIDC-rajapintasuosituksiin. Attribuutteja ei ole tarpeen viedä järjestelmiin tuotantoon ennen kuin niille syntyy käyttötarve.

Valinnaiset tiedot, soveltaminen

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 tunnistussanomien sisältyvät valinnaiset attribuutit haittaa tunnistustapahtumia silloinkaan, kun niiden käytöstä ei ole sovittu.

Valvontaa varten suunnitelma täytyy käytännössä dokumentoida.

2.3 Säännös 13 § Rajat ylittävän tunnistamisen edellyttämät tiedot

13 § Rajat ylittävän tunnistamisen edellyttämät tiedot

Tunnistauduttaessa suomalaisella tunnistusvälineellä ulkomaiseen asiointipalveluun tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on välitettävä samat tiedot kuin luottamusverkostossa on välitettävä 12 §:n mukaan kansallisessa tunnistautumisessa. Tiedot tulee olla mahdollista välittää edelleen tunnistusvälityspalvelun ja kansallisen solmupisteen välillä. Lisäksi on välitettävä tieto siitä, kohdistuuko tunnistustapahtuma julkisen hallinnon asiointipalveluun vai yksityiseen asiointipalveluun.

Tunnistauduttaessa ulkomaisella tunnistusvälineellä suomalaiseen asiointipalveluun kansallisen solmupisteen ja välityspalvelun tarjoajan välisessä rajapinnassa on välitettävä kansainvälisessä eIDAS-rajapinnassa määritellyt minimitiedot ja rajapinnassa on oltava valmius välittää kansainvälisessä eIDAS-rajapinnassa määritellyt valinnaiset tiedot. Henkilön yksilöivä tunnistetieto välitetään siinä muodossa, missä kansallinen solmupiste vastaanottaa sen kansainvälisestä eIDAS-rajapinnasta. Tiedot tulee olla mahdollista välittää edelleen tunnistusvälityspalvelun ja asiointipalvelun välillä. Lisäksi on välitettävä tieto siitä, kohdistuuko tunnistustapahtuma julkisen hallinnon asiointipalveluun vai yksityiseen asiointipalveluun.

2.3.1 Perustelumuistio

13.1 Tunnistusvälityspalvelun tarjoajan ja kansallisen solmupisteen välinen rajapinta

Suomen notifiomia tunnistusvälineitä on mahdollista käyttää tulevaisuudessa ulkomaisiin julkisen hallinnon asiointipalveluihin tunnistautumises-sa ja toisaalta ulkomaisilla notifioiduilla tunnistusvälineillä on mahdollisuus tulevaisuudessa tunnistautua suomalaisiin julkisen hallinnon asiointipalveluihin. eIDAS-asetuksen mukaan valtioiden täytyy kyetä tähän viimeistään 18.9.2018. Kansallisen solmupisteen käyttämisestä tunnis-tautumisessa yksityisiin asiointipalveluihin ei vielä ole määrittelyjä EU-tasolla eikä Suomessa.

Tunnistamistapahtumat Suomen ja muiden maiden välillä tullaan välittämään Vä-estörekisterikeskuksen hallinnoiman kansallisen solmupisteen (PEPS, Pan European Proxy Server) kautta.

Välityspalvelun tarjoajan ja PEPSin välinen rajapinta on määriteltävä kansallisesti. Rajapintaa koskevat samat yleiset vaatimukset kuin tunnistus-välineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välistä rajapintaa. Muilta osin välityspalvelun tarjoaja ja solmupisteen toteuttaja sopivat rajapinnan ominaisuuksista keskenään. Tarkoituksenmukaista kuitenkin on, että protokollaksi valitaan jokin luottamusverkostossa käytössä oleva protokolla.

Perustelujen täydennys 5/2018

Määräyksen 13 § koskee rajat ylittävää tunnistamista kansallisen solmu-pisteen kautta.

Kansallisessa solmupisteessä keskitytään ensi vaiheessa tunnistamiseen julkishallinnon asiointipalveluihin ja vasta seuraavassa vaiheessa arvioidaan yksityiskohtaisemmin mahdollisuudet toteuttaa tunnistaminen yksityisiin asiointipalveluihin.

Ulkomaiseen julkisen sektorin asiointipalveluun tunnistaminen suomalaisella välineellä tapahtuu tunnistusvälineen tarjoajalta tunnistusvälityspalvelun ja kansallisen solmupisteen kautta. Ulkomaisella tunnistusvälineellä tunnistaminen suomalaiseen julkisen sektorin palveluun tapahtuu kansallisen solmupisteen ja suomi.fi -tunnistuksen kautta.

Koska kansallinen solmupiste ei ole toistaiseksi käytettävissä yksityisiin asiointipalveluihin tunnistamisessa, ulkomaisia tunnistusvälineitä käyttävien asiakkaiden tunnistaminen suomalaisiin asiointipalveluihin voi tapahtua sopimusperusteisesti, samoin kuin suomalaisella tunnistusvälineellä tunnistautuminen ulkomaisessa yksityisen sektorin palvelussa. Ulkomaisen tunnistuspalvelun luotettavuus voisi olla todettavissa notifiointin perusteella, tunnistuspalvelun kotivaltion mahdollisen sääntelyn ja valvonnan perusteella tai sopimusperusteisesti.

Jos jokin luottamusverkostoon kuuluva tunnistuspalvelu haluaa ryhtyä välittämään vahvaa tunnistusta myös ulkomaille, tunnistusvälityspalvelun ja asiointipalvelun rajapintaa ja sopimussuhdetta koskevat samat vaatimukset kuin kotimaisille asiointipalveluille tarjottaessa. Sääntely ja Viestintäviraston valvonta kattavat tällöin tunnistuslain ja Viestintäviraston määräyksen vaatimukset tunnistusvälitykselle. eIDAS-asetuksen rajat ylittävän tunnistamisen yhteentoimivuus- ja turvallisuusvaatimukset komission asetuksessa (EU) 2015/1501 koskevat vain kansallista solmupistettä.

13.2 Asiointipalvelun tyyppi

Rajat ylittävässä tunnistamisessa tunnistautumisen julkisen hallinnon asiointipalveluihin tulee olla ilmaista, mutta yksityisten asiointipalveluiden tunnistamisesta eIDAS-asetus ja täytäntöönpanosäännökset mahdollistavat korvauksen perimisen tunnistusvälineen käytöstä.

Tämän vuoksi tieto siitä, kohdistuuko tunnistustapahtuma julkisen hallinnon asiointipalveluun vai yksityiseen asiointipalveluun, tulee pystyä siirtämään myös tämän rajapinnan yli.

2.4 Säännös 14 § Tiedonsiirrossa käytettävä protokolla ja muut vaatimukset

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 säädettyistä ominaisuuksista ja käytettävästä protokollasta.

2.4.1 Perustelumuistio

14.1 Perustelut ja soveltaminen

Pykälän tarkoitus on selventää sitä, että luottamusverkoston osapuolet sopivat keskenään siitä, mitä protokollaa käyttävät tietojen välittämisessä ja mitä tietoja välittävät tässä määräyksessä määrättyjen vähimmäistietojen lisäksi.

Määräyksen valmistelun yhteydessä on tarkasteltu SAML 2.0- ja Open ID Connect -protokollia. Viestintävirasto laatii ja julkaisee suosituksina 212/2016 S ja 213/2016 S näistä protokollista malliprofiilit vaadittujen tietojen välittämistä varten [11, 12].

Kansallisen TUPAS-protokollan käytettävyyden ja kehitystarpeiden selvittämisestä vastaa protokollan haltija Finanssialan keskusliitto.

Protokollia käsitellään vaikutusarvioinnin (ks. A osa) luvussa 3.4.

14.2 Suositus SAML- tai Open ID Connect -protokollan ja profiilien käytöstä

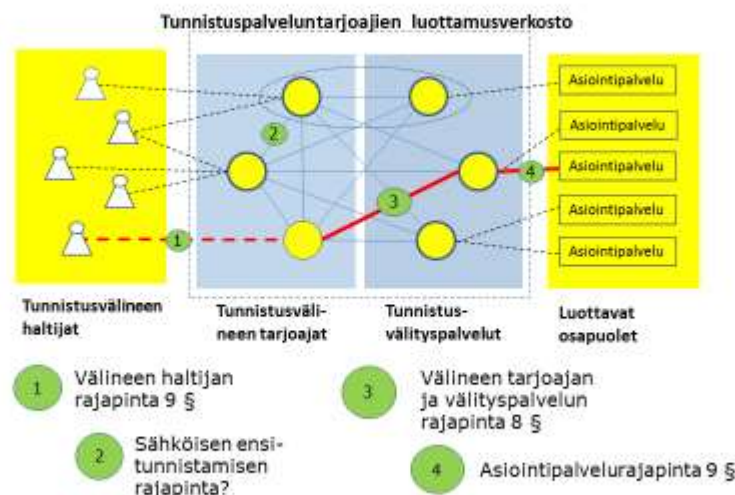
Luottamusverkostossa suositellaan käytettäväksi SAML 2.0 - tai Open ID Connect -protokollaa ja näiden kansallisesti laadittuja profiileja, jotka Viestintävirasto julkaisee erillisinä suosituksina 212/2016 S ja 213/2016 S [11, 12].

3 Lähteet 2020-2021 vaikutusarviointiin

3.1 Yleiskuvaus lähtötilanteesta

3.1.1 Määräyksessä säännelty luottamusverkoston rajapinnat

Määräyksen 72 8 § ja 9 § rajapinnat



[Päivitettävä ja tarkennettava kuva]

3.1.2 Luottamusverkoston rajapinnat, joista ei määrätä

MPS72 2016 12.3.1 Tunnistusvälineiden tarjoajien välinen rajapinta (ensitunnistaminen)

Tunnistusvälineiden tarjoajien välisellä rajapinnalla tarkoitetaan sähköisessä ensitunnistamisessa käytettävää rajapintaa. Muut tunnistusvälineiden tarjoajien väliset rajapinnat voidaan tulkita tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan väliseksi rajapinnaksi ja rajapintaa koskevat siten kyseisen rajapinnan vaatimukset.

Sähköisen ensitunnistamisen rajapinta (SAML/TUPAS) on ollut käytössä jo useita vuosia, koska sähköinen ensitunnistaminen mahdollistettiin tunnistuslaissa (17 §) jo ennen luottamusverkostopykälän (12 a §) lisäämistä. Tästä syystä tässä vaiheessa ei nähdä tarkoituksenmukaiseksi lisätä sähköisen ensitunnistamisen rajapintaa koskevia vaatimuksia määräykseen.

Pidemmän tähtäimen kehityksenä on kuitenkin tuotu esiin toivomus siitä, että rajapinnan kautta voitaisiin välittää tietoa ensitunnistamisesta (esim. mihin henkilökohtainen ensitunnistaminen on perustunut: passi, henkilökortti, sähköinen tunnistus).

MPS72 2016 12.3.2 Tunnistusvälineen haltijan ja tunnistusvälineen tarjoajan välinen rajapinta

[...]

[teksti mukana salausmuistiossa, mihin liittyy enemmän]

MPS72 2016 12.3.3 Väestötietojärjestelmän rajapinta

Tunnistuspalvelun tarjoaja käyttää väestötietojärjestelmän rajapintaa (VTJ-rajapinta) ensitunnistamisen yhteydessä sekä varmistaessaan aika ajoin tunnistamispalvelussa käyttämiensä tietojen ajantasaisuuden.

Väestörekisterikeskuksen tarjoama liitanta on yleisellä tasolla määritelty dokumentissa VTJkysely-palvelu; Sovelluskyselyiden rajapintakuvaus, joka on ladattavissa VRK:n sivuilta [24].

Tunnistuspalvelun tarjoajat ja VRK sopivat keskenään rajapinnan tarkemmasta toteutuksesta, eikä tähän määräykseen sisällytetä mitään tätä rajapintaa koskevia vaatimuksia.

MPS72 2016 12.3.4 Yritys- ja yhteisörekisterien rajapinta

Oikeushenkilön tunnistamisessa tarvittavat tiedot yritysten osalta on haettava tunnistus- ja luottamuspalvelulain 7 a §:n mukaan patentti- ja rekisterihallituksen yritys- ja yhteisörekistereistä. Tunnistuspalvelun tarjoajat ja PRH sopivat rajapinnan toteutuksesta keskenään, eikä tähän määräykseen sisällytetä mitään tätä rajapintaa koskevia vaatimuksia.

3.1.3 Rajapintaprotokollat, viraston arvio kyselyssä 2020 (OIDC ja SAML)

Määräyksessä ei määrätä, mitä protokollaa säännellyissä rajapinnoissa tulisi käyttää. Määräyksen 14 §:ssä on informatiivinen säännös, jonka mukaan tunnistuspalvelut sopivat protokollasta ja muista kuin määräyksen mukaisista ominaisuuksista keskenään.

Sopimusvapauteen vaikuttaa tunnistus- ja luottamuspalvelulain ja valtioneuvoston luottamusverkostoasetuksen sääntely (asetuksen säännösviittaukset ovat tunnistuslakiin ennen muutosta 412/2019, jolloin veloitteet ovat siirtyneet eri kohtiin tunnistuslaissa).

Määräyksen perustelumuistiossa virasto suosittelee käyttämään SAML 2.0 - tai Open ID Connect -protokollaa ja näiden kansallisesti laadittuja profiileja, jotka virasto julkaisee erillisinä suosituksina (212/2018 S ja 213/2018 S).

Rajapintasuosituksen 212 ja 213 päivittäminen on käynnissä ja mahdollisia muutostarpeita voidaan mahdollisesti ratkaista näillä suosituksilla.

Vuoden 2016 jälkeen Tupas-protokolla on poistunut käytöstä ainakin vahvassa tunnistamisessa ja mobiilioperaattorit ovat siirtyneet osassa rajapinnoista käyttämään vanhan ETSI mobiilivarmennerajapinnan sijaan OpenIDConnectia. OpenIDConnect on muutenkin vallitseva protokolla, mutta myös SAML on jossain määrin käytössä.

3.1.4 Tunnistamisessa välitettävät attribuutit, kyselyn 2020 arvio (12 §)

Vähimmäistiedot, jotka vahvan tunnistuspalvelun täytyy määräyksen 12 §:n mukaisesti pystyä tuottamaan, ovat yksilöivä tunniste (hetu tai satu), nimi ja syntymäaika. Lisäksi on säädetty joukko valinnaisia tietoja, joita tunnistuspalvelu voi halutessaan tarjota.

Määräyksen vähimmäistiedot ja valinnaiset tiedot vastaavat rajat ylittävän tunnistamisen eIDAS-vaatimuksia. Tämän tietojoukon merkitys verrattuna kaikkiin muihin mahdollisiin henkilötietoihin on se, että ne on määritelty viraston suositusraja-
pinnoissa (suositukset 212 ja 213/2018) ja ne vastaavat eIDAS-sääntelyä, mikä edistää rajat ylittävää yhteentoimivuutta. Näiden säädettyjen tietojen tuottaminen tunnistuksessa sisältää myös luottamusverkoston hintasääntelyyn tunnistuslain 12 c §:n mukaisesti.

Tavallisin vahvan tunnistuksen tarjontatapa on välittää ja vahvistaa luottavalle osapuolelle käyttäjästä tunnistustapahtumassa henkilötiedot, joiden perusteella henkilöllisyys voidaan yksilöidä. **Vahvan tunnistamisen sääntely on kuitenkin neutraalia siten, että tunnistamisessa voi myös köyhdyttää tietoja ja vaikkapa vahvistaa vain käyttäjän täysi-ikäisyyden.** Tällaiset vahvistukset ovat tunnistuspalvelun lakisääteisten lokitietojen perusteella yhdistettävissä henkilöön, joten vaikka ne ovat asiointipalvelulle anonyymejä, henkilötietojen sääntelyn kannalta ne ovat pseudonyymejä.

Säädettyjen tietojen lisäksi tunnistuspalvelu voi tarjota muita **rikastettuja tietoja** yleistä henkilötietojen suojan sääntelyä tai mahdollista toimialakohtaista sääntelyä noudattaen. Rikastamisen voisi tehdä tunnistusvälineen tarjoaja tai tunnistusvälityspalvelu.

Suomessa vahvassa tunnistamisessa on toistaiseksi nähtävissä vain perustyyppisen nimi ja henkilötunnus -yhdistelmän välittämistä. Traficom ei ole selvittänyt toimijoilta syytä tähän.

3.1.5 Valinnaiset attribuutit, viraston arvio kyselyssä 2020

Konkreettisia velvoitteita valinnaisten attribuuttien toteuttamiseen arvioitiin vuonna 2018 määräyksen osittaisuudistuksen yhteydessä (Tupas-siirtymäajan pidentäminen).

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 tunnistusnominin sisältyvät valinnaiset attribuutit haittaa tunnistustapahtumia silloinkaan, kun niiden käytöstä ei ole sovittu.

Vuonna 2018 arvioitiin, että ei ole tarvetta velvoittaa käsittelemään julkinen/yksityinen-attribuuttia kansallisessa tunnistamisessa eri tavalla kuin muita valinnaisia attribuutteja tai vaatia sitä toteutettavaksi nopeammassa aikataulussa.

3.2 Vuonna 2016 ja 2018 vaikutusarvioinneissa linjatut asiat

3.2.1 Pakolliset attribuutit 2016 (12 §)

MPS72 2016 3.4.4 Rajapinnat: välitettävät attribuutit ja muut tiedot

Arvioitavat kysymykset: Vaaditaanko kansallisesti samat vähimmäistiedot kuin eIDAS-asetus edellyttää rajat ylittävissä siirroissa? Miten huomioidaan eIDAS-asetuksen valinnaiset attribuutit? Otetaanko määräyksessä kantaa siihen, mitä tietoja välineen myöntäjän on välitettävä välityspalvelulle? Käytetäänkö HETUa vai SATUa?

Vaikutusarvioinnin lähtökohdat

Välitettävät vähimmäistiedot voidaan määritellä kansallisten käytäntöjen mukaisesti tai huomioiden eIDAS-asetuksen rajat ylittävää tunnistamista varten laadittu lista vähimmäistiedoista. Luonnollisen henkilön osalta eIDAS-asetuksen mukaisissa vähimmäistiedoissa ei ole olennaista eroa kansalliseen käytäntöön. eIDAS-asetuksen mukaisia valinnaisia tietoja ei juurikaan ole käytössä. Oikeushenkilön vahvat sähköiset tunnistusvälineet eivät tähän asti ole olleet lain mukaan mahdollisia, joten niiden tunnistetiedoista ei ole omaksuttuja käytäntöjä.

Vähimmäistiedot riittävät siihen, että luonnollinen tai oikeushenkilö kyetään yksilöimään luotettavasti. Valinnaiset tiedot voivat olla tarpeen joillekin asiointipalveluille. Luonnollisten henkilöiden eIDAS-asetuksen mukaiset valinnaiset tiedot ovat sinänsä tietoja, jotka tarvittaessa ovat luotettavasti saatavissa väestötietojärjestelmästä. Oikeushenkilön osalta valinnaiset tiedot perustuvat EU-sääntelyyn, joten niiden voidaan olettaa olevan tarvittaessa sektorikohtaisesti saatavissa.

Kun eIDAS-asetuksessa tavoitteena oleva rajat ylittävä tunnistaminen aikanaan tulee käyttöön julkisella ja mahdollisesti myös yksityisellä sektorilla, se on helpompi toteuttaa, kun välitettävät tiedot on jo valmiiksi määritelty eIDAS-asetuksen mukaisesti.

Linjaukset

Kansallisesti vaadittavat vähimmäistiedot määritellään sekä luonnollisen henkilön että oikeushenkilön osalta yhdenmukaisesti eIDAS-vaatimusten kanssa, jotta sama profiili kelpaa sekä kansallisesti että kansainvälisesti.

Edellytetään, että rajapinnoissa on valmius myös eIDAS-asetuksen mukaan valinnaisten tietojen välittämiseen. Valinnaisten tietojen välittäminen on sopimuskysymys, johon ei oteta kantaa määräyksessä. Tekninen valmius helpottaa tarvittaessa sopimusten tekemistä. Koska valinnaiset tiedot eivät ole ennestään toimijoilla käytössä, niille määrätään toimijoiden ehdotuksesta siirtymäaika 18.9.2018 asti.

Henkilötunnisteena voi käyttää HETUa tai SATUa ja malliprofiileissa huomioidaan vaihtoehtona molemmat. Lisäksi varataan kenttä muulle tunnisteelle, joka voi olla esimerkiksi toimialakohtainen, sopimukseen perustuva tai rajat ylittävissä tunnistamisessa välitettävä tunniste.

Valinnaisten tietojen osalta tulee mietittäväksi myös kysymys, kuuluuko tietojen hankkiminen esimerkiksi väestötietojärjestelmästä tunnistusvälineen myöntäjän vai välityspalvelun vastuulle. Laissa ei näyttäisi olevan perusteita ottaa tähän kantaa määräyksessä ja kysymykseen liittyyneen tunnistuslain 12 a §:ssä säädetyn enimmäishinnan tulkintaa. Näin ollen asiaa ei käsitellä tässä määräyksessä.

Määräyksen 12 § ja 13 § on laadittu näiden linjausten mukaisesti.

3.2.2 Valinnaiset attribuutit 2016 ja 2018 (12 § ja 25 § siirtymäsäännös)

MPS72 2016 3.4.4 Rajapinnat: välitettävät attribuutit ja muut tiedot

Arvioitavat kysymykset: ...Miten huomioidaan eIDAS-asetuksen valinnaiset attribuutit? Otaanko määräyksessä kantaa siihen, mitä tietoja välineen myöntäjän on välitettävä välityspalvelulle?...

Vaikutusarvioinnin lähtökohdat

[...] eIDAS-asetuksen mukaisia valinnaisia tietoja ei juurikaan ole käytössä. Oikeushenkilön vahvat sähköiset tunnistusvälineet eivät tähän asti ole olleet lain mukaan mahdollisia, joten niiden tunnistetiedoista ei ole omaksuttuja käytäntöjä.

Vähimmäistiedot riittävät siihen, että luonnollinen tai oikeushenkilö kyetään yksilöimään luotettavasti. Valinnaiset tiedot voivat olla tarpeen joillekin asiointipalveluille. Luonnollisten henkilöiden eIDAS-asetuksen mukaiset valinnaiset tiedot ovat sinänsä tietoja, jotka tarvittaessa ovat luotettavasti saatavissa väestötietojärjestelmästä. Oikeushenkilön osalta valinnaiset tiedot perustuvat EU-sääntelyyn, joten niiden voidaan olettaa olevan tarvittaessa sektorikohtaisesti saatavissa.

Kun eIDAS-asetuksessa tavoitteena oleva rajat ylittävä tunnistaminen aikanaan tulee käyttöön julkisella ja mahdollisesti myös yksityisellä sektorilla, se on helpompaa toteuttaa, kun välitettävät tiedot on jo valmiiksi määriteltä eIDAS-asetuksen mukaisesti.

Linjaukset

...

Edellytetään, että rajapinnoissa on valmius myös eIDAS-asetuksen mukaan valinnaisten tietojen välittämiseen. Valinnaisten tietojen välittäminen on sopimuskysymys, johon ei oteta kantaa määräyksessä. Tekninen valmius helpottaa tarvittaessa sopimusten tekemistä. Koska valinnaiset tiedot eivät ole ennestään toimijoilla käytössä, niille määrätään toimijoiden ehdotuksesta siirtymäaika 18.9.2018 asti.

Henkilötunnisteena voi käyttää HETUa tai SATUa ja malliprofiileissa huomioidaan vaihtoehtona molemmat. Lisäksi varataan kenttä muulle tunnisteelle, joka voi olla esimerkiksi toimialakohtainen, sopimukseen perustuva tai rajat ylittävissä tunnistamisessa välitettävä tunniste.

Valinnaisten tietojen osalta tulee mietittäväksi myös kysymys, kuuluuko tietojen hankkiminen esimerkiksi väestötietojärjestelmästä tunnistusvälineen myöntäjän vai välityspalvelun vastuulle. Laissa ei näyttäisi olevan perusteita ottaa tähän kantaa määräyksessä ja kysymykseen liittyyneen tunnistuslain 12 a §:ssä säädetyn enimmäishinnan tulkintaa. Näin ollen asiaa ei käsitellä tässä määräyksessä.

Määräyksen 12 § ja 13 § on laadittu näiden linjausten mukaisesti.

MPS72 2018 3.4.3 Rajapinnat, 2018 arviointi 12 § 2 mom. valinnaisista attribuuteista

Arvioitavat kysymykset: Miten muutetaan määräyksen 12.2 §:n mukaisten valinnaisten eIDAS-attribuuttien siirtymäaika? Millä aikataululla ja missä tilanteissa attribuuteille on nähtävissä käyttötarvetta kansallisessa ja määräyksen 13 §:n mukaisessa rajat ylittävissä tunnistamisessa? Onko tunnistusvälineen ja tunnistusvälityspalvelun velvoitteet erotettava?

Vaikutusarvioinnin lähtökohdat

Dnro

TRAFICOM/245890/03.04.05.00/2020
7.12.2020

Määräyksessä 72/2016 määrättiin, että toimijoilla oli oltava 18.9.2018 valmius välittää valinnaisia attribuutteja. Valmiudella tarkoitettiin sitä, että tiedot on määritelty rajapintaan.

Annettaessa määräystä vuonna 2016 arvioitiin, että valinnaiset tiedot voivat olla tarpeen joillekin asiointipalveluille ja että attribuuttien määrittely rajapintaan helpottaisi niiden käyttöönottoa tarvittaessa.

Toimijat eivät ole ottaneet valinnaisia attribuutteja käyttöön, eikä vuonna 2016 määrätty siirtymäaika niiden määrittelylle ole toteutumassa.

Sääntelyn uudelleenarvioinnissa tarkastellaan

- 1) Tunnistusvälineen ja tunnistusvälityspalvelun roolia valinnaisten attribuuttien kannalta
- 2) Kansallisen ja rajat ylittävän tunnistamisen eroa
- 3) Valinnaisten attribuuttien mahdollisia käyttötilanteita, erityisesti tarvetta tiedolle siitä, onko kyseessä yksityinen vai julkinen asiointipalvelu

Kansallisen solmupisteen kannalta määräyksen 13 §:n 1 momentin mukaisesti tiedon siitä, tunnistaanko yksityiseen vai ulkomaiseen asiointipalveluun, on oltava välitettävissä, kun tunnistetaan käyttäjä suomalaisella tunnistusvälineellä ulkomaiseen asiointipalveluun. Säännös koskee rajat ylittävää tunnistamista kansallisen solmupisteen kautta.

Kansallisessa solmupisteessä keskitytään ensi vaiheessa tunnistamiseen julkishallinnon asiointipalveluihin ja vasta seuraavassa vaiheessa arvioidaan yksityiskohtaisemmin mahdollisuudet toteuttaa tunnistaminen yksityisiin asiointipalveluihin.

Koska kansallinen solmupiste ei ole toistaiseksi käytettävissä yksityisiin asiointipalveluihin tunnistamisessa, ulkomaisia tunnistusvälineitä käyttävien asiakkaiden tunnistaminen suomalaisiin asiointipalveluihin voi tapahtua sopimusperusteisesti. Ulkomaisen tunnistuspalvelun luotettavuus voisi olla todettavissa notifiointin perusteella, tunnistuspalvelun kotivaltion mahdollisen sääntelyn ja valvonnan perusteella tai sopimusperusteisesti.

Rajat ylittävän tunnistuksen kehitystä vauhdittaa Pohjoismaiden ja Baltian maiden hallintojen yhteistyö, jossa selvitetään mm. mahdollisuuksia tunnustaa sopimusten perusteella muiden valtioiden sähköinen tunnistus myös silloin, kun tunnistusvälineitä ei ole notifioitu komissiolle.

Julkinen/yksityinen asiointipalvelutieto on tarpeen rajat ylittävässä tunnistamisessa. Valtioiden välillä ei eIDAS-asetuksen mukaisesti suoriteta maksuja tunnistamisesta julkisiin asiointipalveluihin. Suomessa suomalaisen tunnistusvälineen käytöstä ulkomaisessa julkishallinnon asiointipalvelussa syntyvät maksut maksetaan valtion varoista, mutta niistä ei korvata tunnistamista yksityiseen asiointipalveluun.

Kansallisessa tunnistamisessa Viestintävirasto arvioi sitä, voiko tieto yksityisestä tai julkisesta asiointipalvelusta olla tarpeellinen luottamusverkostossa tunnistusvälityksen ehtoihin liittyvistä syistä. Tunnistusta-pahtuman välitys julkisen sektorin asiointipalveluun voi mahdollisesti vaikuttaa esimerkiksi häiriötilanteiden tiedonvaihtoon, tietosuojan tai hinnoitteluun liittyvissä ehdoissa. Valmistelussa saatujen tietojen perusteella tiedolle ei ole selkeää akuuttia tarvetta.

Luonnolliseen henkilöön liittyville valinnaisille attribuuteille voi Viestintäviraston käsityksen mukaan tulla käyttöä lähinnä sellaisissa tilanteissa, joissa suomalainen asiointipalvelu haluaa tunnistaa henkilöitä ulkomaisella tunnistusvälineellä, jossa suomalaisen yksiselitteisen henkilötunnuksen sijaan tulee ulkomailta yksilöinä lisätietoina valinnaisia attribuutteja.

Julkisissa palveluissa toisesta valtiosta tulleet valinnaiset attribuutit välittää julkisen hallinnon palvelulle kansallinen solmupiste, eivätkä sanomat liiku luottamusverkoston kautta.

Oikeushenkilöihin liittyvät valinnaiset attribuutit voivat tulla tarpeellisiksi, jos suomalaiset tunnistusvälineen tarjoajat ryhtyvät tuoteistamaan oikeushenkilön vahvoja tunnistusvälineitä tai jos asiointipalveluille syntyy tarve hyödyntää ulkomaisen yritysten vahvaa sähköistä tunnistusta.

Suomessa ei toistaiseksi ole tarjolla oikeushenkilöiden vahvoja sähköisiä tunnistusvälineitä ja kysynnän ja tarjonnan syntymistä esimerkiksi sähköisen sopimisen tarpeisiin on vaikea ennakoida.

Julkishallinnon rajat ylittävässä toiminnassa kansallinen solmupiste pystyy tarvittaessa välittämään myös ulkomaisen oikeushenkilöiden valinnaiset tiedot kotimaisille viranomaisille. Niin kauan kun tarjolla ei ole vahvoja suomalaisten oikeushenkilöiden tunnistusvälineitä, jää epäselväksi, mikä taho varmentaisi suomalaisten oikeushenkilöiden tiedot niiden toimissa ulkomaisen viranomaisten tai yksityisten tahojen kanssa.

Tunnistusvälityspalvelun valmius välittää valinnaisia attribuutteja asiointipalvelulle voi muodostua tärkeämmäksi kuin tunnistusvälineen tarjoajan valmius. Tunnistuspalveluntarjoajat toimivat kuitenkin usein

Dnro
TRAFICOM/245890/03.04.05.00/2020
7.12.2020

molemmissa rooleissa. Velvoitteen rajaaminen osaan tunnistusvälineen tarjoajista mutkistaisi rajapinnan sääntelyä tarpeettomasti sen sijaan, että toimitaan yhtenäisesti standardien mahdollistamilla malleilla.

Viestintävirasto harkitsi seuraavia sääntelyvaihtoehtoja

- ensisijaisesti määrittelyvaatimusten säilyttämistä pääsääntöisesti ennallaan
- ensisijaisesti määräajan lyhyttä pidentämistä yhdenmukaiseksi Tupas-siirtymän määrittelyn määräjän 1.10.2018 kanssa ja toissijaisesti määräajan pidentämistä 1.1.2019 asti
- velvoitteen rajaamista tunnistusvälityspalveluihin, jotka tarjoavat asiointipalveluille tunnistusta useammalla kuin yhdellä tunnistusvälineellä
- viimesijaisena vaihtoehtona valinnaisten attribuuttien määrittelyn muuttamista vaatimuksesta suositukseksi

Linjaukset

Viestintävirasto linjasi sääntelyn muutokset seuraavasti.

Määräyksessä säilytetään vaatimus valmiudesta valinnaisiin attribuutteihin.

Viestintävirasto arvioi, että valmiutta rajat ylittävään tunnistamiseen on perusteltua parantaa, vaikka akuuttia käyttötarvetta tiedoille ei tällä hetkellä ole tiedossa. Valinnaisten attribuuttien tarkoitus on tukea tunnistusta ja asiointia niissä tilanteissa, joissa pakolliset attribuutit eivät ole riittäviä. Lausuntojen perusteella rajat ylittävälle tunnistamiselle on kasvava tarve.

Viestintävirasto arvioi, että koska rajapintojen muuttaminen on hidasta, on perusteltua nostaa luottamusverkoston valmiustasoa valinnaisten attribuuttien käsittelyyn käynnistämällä suunnittelu.

Viraston arvion mukaan suositus ei edistäisi valinnaisten attribuuttien huomioimista riittävästi, koska 2016 annettu määräyskään ei ole käynnistänyt suunnittelua kaikilla toimijoilla.

Suunnittelu on tehtävä viimeistään 1.10.2018 samalla aikataululla, kun uusi rajapinta muutetaan määritellä. Virasto tarkentaa perusteluja siltä osin, millaista valmiutta vaaditaan.

Viestintävirasto arvioi, että nekin tunnistuspalvelut, jotka eivät ole sitä vielä tehneet, pystyvät huomioimaan valinnaiset tietokentät rajapintojen suunnittelussa ilman kohtuutonta vaivaa.

Viestintävirasto katsoo, että valmiutta on tarkoituksenmukaista lisätä asteittain ja huomioiden yritysten järjestelmien kehittämisen aikataulut. Ensivaiheessa on riittävää, että attribuutit huomioidaan rajapinnan ja tunnistusjärjestelmän suunnittelussa. Tunnistusjärjestelmän suunnittelulla tarkoitetaan sitä, että selvitetään, mitä muita muutoksia valinnaisten attribuuttien käsittely edellyttäisi sen lisäksi, että ne määritellään rajapintaan. Viestintävirasto arvioi, että suunnittelu nopeuttaa käyttöönottoa tarvittaessa. Tässä voidaan tukeutua Viestintäviraston julkaisemiin SAML- ja OIDC-spesifikaatioihin.

Attribuutteja ei ole tarpeen viedä järjestelmiin tuotantoon ennen kuin niille syntyy käyttötarve. Teknisissä konfiguroinneissa tulee huomioida, etteivät valinnaiset attribuutit vaikuta tunnistustapahtumiin silloin, kun niiden käyttöönotto ei ole sovittu.

Lausuntojen perusteella Viestintävirasto arvioi, että valinnaisten attribuuttien varsinainen käyttöönotto voi edellyttää vaatimusten soveltamiseen tai yhteentoimivaan toteutusmalliin liittyvää tulkintaa tai keskustelua luottamusverkoston yhteistoimintaryhmässä.

Valmius valinnaisten attribuuttien välittämiseen koskee jatkossakin kaikkia tunnistuspalveluita.

Velvollisuutta ei rajata tunnistusvälityspalveluihin, jotka tarjoavat asiointipalveluille tunnistusta useammalla kuin yhdellä (omalla) tunnistusvälineellä.

Viestintävirasto arvioi lausuntojen perusteella, että velvoitteen rajaaminen osaan tunnistusvälineen tarjoajista mutkistaisi rajapinnan sääntelyä tarpeettomasti sen sijaan, että toimitaan yhtenäisesti standardien mahdollistamilla malleilla.

Lausuntojen perusteella ei ole syytä velvoittaa käsittelemään julkinen/yksityinen attribuuttia kansallisessa tunnistamisessa eri tavalla kuin muita valinnaisia attribuutteja.

3.2.3 Sähköinen ensitunnistus (ensitunnistamisen ketjutus)

MPS72 2016 3.5 Tunnistuspalvelu: sähköisen ensitunnistamisen rajapinnan sääntelytarve

Arvioitava kysymys: Vaaditaanko tunnistusvälineen myöntäjien välisessä rajapinnassa välittämään tieto ensitunnistamisen tekijästä, tunnistusasiakirjasta ja tunnistamisen ketjuttajista?

Viestintäviraston määräysvaltuus koskee lain vaatimusten teknistä tarkentamista. Ensitunnistamisrajan mahdollista sääntelyä on arvioitava myös siltä kannalta, että tunnistusvälineen tarjoajien välinen toiminta sähköisen ensitunnistamisen mahdollistamiseksi uusia välineitä myönnettäessä on myös kilpailukysymys.

Sähköisen ensitunnistamisen rajapinta (SAML/TUPAS) on ollut toimijoiden välillä käytössä jo useita vuosia. Toiminta on perustunut kahdenvälisiin sopimuksiin. Teknisesti rajapinta vastaa asiointipalveluille tarjottua rajapintaa.

Tunnistus- ja luottamuspalvelulain 17 §:n muutoksella on mahdollistettu se, että tunnistusvälineen tarjoajat voivat rajattomasti ketjuttaa tunnistamista eli luoda uusia sähköisiä tunnistusvälineitä luottamalla muiden tarjoamiin sähköisiin tunnisteisiin. Toisen tunnistusvälineeseen luottava välineen myöntäjä kantaa tunnistus- ja luottamuspalvelulain 17.4 §:n säännöksen perusteella vahinkovastuun ja ketjuttaminen edellyttääkin sitä, että ketjuttamista hyödyntävä välineen myöntäjä arvioi millainen riski luotettuun tunnisteeseen mahdollisesti liittyy. Tähän riskiin vaikuttavia tekijöitä ovat se, kuinka kauan sitten ja minkä henkilöllisyystodistuksen perusteella alkuperäinen henkilökohtainen tunnistaminen on tehty, onko ketjussa useampi tunnistusvälineen myöntäjä, onko jokin ketjussa ollut tunnistusvälineen myöntäjä lopettanut toimintansa ja onko ketjussa oleville tunnistusvälineen myöntäjille tapahtunut tietoturvaloukkauksia, jotka ovat voineet vaikuttaa tiedon eheyteen.

Määräystä valmisteltaessa on todettu, että tieto ensitunnistamisen tekemisestä ja ketjussa olevista toimijoista tukisi riskin arviointia ja hallintaa. Valmistelussa on harkittu vaatimusta siitä, että rajapinnoissa tulisi olla määriteltynä, miten ensitunnistamisen ja ketjutuksen tiedot välitettäisiin.

Toisaalta toimijat ovat esittäneet valmistelun aikana näkemyksen, että sähköistä ensitunnistamista on käytetty ongelmitta jo tähänkin asti, joskin aikaisemman lain sallimalla tavalla vain nimenomaisella sopimuksella kahden tunnistajan välillä. Tästä ei Viestintäviraston näkemyksen mukaan kuitenkaan voi päätellä, ettei ongelmia syntyisi useamman välineen ketjuttamisessa. Tietoturvaloukkausten selvittämistilanteessa on tärkeää, että tieto ketjuttamisesta on tavalla tai toisella selvitettävissä. Jos tunnistusvälineen tarjoaja myöntää esimerkiksi tunnisteita varastettujen tai väärennettyjen henkilöllisyystodistusten perusteella, on pystyttävä selvittämään, onko näillä väärän henkilön hallussa olevilla sähköisillä tunnistusvälineillä haettu sähköisesti uusia tunnistusvälineitä. Tietoturvallisuuden ja sähköisen tunnistuksen yleisen luotettavuuden kannalta tietojen välittäminen olisi eduksi.

Sisäasianhallinnossa on käynnissä hanke palvelusta, josta tunnistusvälineen tarjoajat voivat 1.5.2017 lähtien tarkistaa, onko henkilöllisyystodistus voimassa, kadonnut tai varastettu. Tämä on huomioitu myös tunnistus- ja luottamuspalvelulain 7 b §:ssä (Tieto passin tai henkilökortin voimassaolosta). Palvelu vähentää riskiä ainakin henkilökohtaisen ensitunnistamisen osalta.

Myös tunnistus- ja luottamuspalvelulain 6 §:ssä edellytetty VTJ-tarkistus välinettä myönnettäessä ja riittävän usein myös sen jälkeen vähentävät riskiä, että sähköisiä tunnistusvälineitä myönnettäisiin sellaisen henkilötunnuksen perusteella, jota ei löydy väestötietojärjestelmästä.

Tunnistus- ja luottamuspalvelulain muutosehdotuksen lausunnoissa monet lausunnonantajat katsoivat, että tunnistuksen rajoittamatonta ketjuttamista ei pitäisi sallia. Edelleen useissa lausunnoissa katsottiin, että sähköinen ensitunnistaminen ei ole helpottunut lain aikaisemman muutoksen myötä, koska ensitunnistaminen hinnoitellaan kalliiksi. Liikenne- ja viestintäministeriö on käynnistänyt kesällä 2016 lain-säädännön muutoshankkeen ensitunnistamisen hintasääntelystä.

Näiden asioiden tarkentaminen ei kuulu Viestintäviraston määräykseen tai määräysvaltuuteen, mutta vaikutusarvioinnissa on otettava huomioon, millaisia vaikutuksia eri sääntelyvaihtoehdoilla on kilpailuun.

Linjaus

Ensitunnistamis- ja ketjuttamistietojen välittäminen tunnistusvälineen tarjoajien välisessä rajapinnassa vaikuttaisi edistävän uusien tunnistusvälineiden myöntämistä ja siten myös kilpailua, koska se helpotaisi riskin arvioimista ja hallintaa.

Toimijat ovat kuitenkin työryhmätyössä pitäneet rajapintamäärittelyjä tarpeettomina. **Tästä syystä tässä vaiheessa ei nähdä tarkoituksenmukaiseksi lisätä ensitunnistamisen rajapintaa koskevia vaatimuksia määräykseen.**

Pidemmän tähtäimen kehityksenä on kuitenkin tuotu esiin toivomus siitä, että rajapinnan kautta voitaisiin välittää tietoa ensitunnistamisesta (esim. mihin henkilökohtainen ensitunnistaminen on perustunut: passi, henkilökortti, sähköinen tunnistaminen).

Tässä vaiheessa ei ole arvioitu tarkemmin sitä, onko työläämpää tehdä määrittely näille tiedoille nyt tulevaisuuden varalle vai myöhemmin, kun tarve syntyy tai miten rajapinnoissa huomioidaan se, että joku on jo nyt valmis tarjoamaan tiedot.

Myöskään määräykselle vaihtoehtoisia ohjauskeinoja ei ole tarkasteltu tarkemmin. Teknisiä määrittelyjä ensitunnistamisrajapinnassa välitettävälle tiedoille olisi toki mahdollista työstää yhteissääntelynä tai suosituksena. Viestintäviraston tunnistus- ja luottamuspalvelutyöryhmässä on valtiovarainministeriön aloitteesta keskusteltu mahdollisuudesta pilotoida lohkoketjuteknologian soveltuvuudesta ensitunnistamisen ketjuttamistiedon hallinnassa. On mahdollista, että tätä kautta syntyy **yhteis- tai itsesääntelyratkaisu.**

On hyvä huomata, että luottamusverkoston **yhteissääntelyryhmässä** ei missään tapauksessa tulla käsittelemään hinnoittelukysymyksiä tai keskustelemaan hinnoittelusta.

3.2.4 Protokollat 2016 (14 §)

MPS72 2016 3.4.2 Rajapinnat: protokollien sääntely

Arvioitava kysymys: Millä tarkkuudella rajapintavaatimukset laaditaan määräykseen suhteessa yksittäisiin protokolliin, kuten SAML ja Open ID Connect? Mahdollistetaanko toisin sanoen myös muiden protokollien käyttö? Miten huomioidaan puhtaasti kansallinen TUPAS-protokolla, joka ei kaikilta osin täytä vaatimuksia ja jonka kehityssuunnitelmista tai mahdollisuuksista ei ole ollut määräyksen valmistelussa varmaa tietoa?

Arvioinnin lähtökohdat

Valmistelussa on tarkasteltu kolmea protokollaa: SAML, Open ID Connect ja TUPAS.

SAML on yleinen kansainvälisesti ja myös määritelty eIDAS-asetusta tarkentavassa EU-sääntelyssä ja -ohjeistuksessa kansainvälisen välittämisen rajapinnan protokollaksi.

Open ID Connect on yleistymässä ja käytössä erityisesti mobiilivarmentamisessa.

Koska pankkien tarjoamat tunnistukset perustuvat puhtaasti kansallisesti määriteltyyn vanhaan TUPAS-protokollaan, on määräystä valmisteltaessa pitänyt harkita poikkeusta siitä yleisesti noudatetusta periaatteesta, että noudatetaan ensisijaisesti kansainvälisesti yleisiä standardeja.

TUPAS-protokollan mukaan ottamisen vaikutukset toiminnan jatkuvuuteen ovat myönteisiä, koska nykyinen tarjonta asiointipalveluille voi jatkua ilman katkosta. Asiointipalveluiden kannalta tämä ei edellytä välittömiä muutoksia.

Vaikutukset kilpailuun ja tekniseen kehitykseen voivat olla negatiivisia, koska TUPAS-protokollaan ei ole ollut tiedossa kehityssuunnitelmia ja se edellyttää uusilta välitystoimijoilta sopeutumista puhtaasti kansalliseen protokollaan, mikä voi heikentää markkinoille tulon kiinnostavuutta. TUPAS-protokollan oikeudet omistava Finanssialan keskusliitto on kuitenkin käynnistänyt sidosryhmiensä kanssa arvioinnin protokollan kehitysmahdollisuuksista.

Protokollan tehtävä on määritellä yhteentoimivasti tiedot ja niiden siirtotapa, jotta tiedot voidaan siirtää toimijoiden välillä. Mitä vähemmän eri protokollia toimijoilla on käytössä, sitä helpompaa on tältä osin sopimusten aikaansaaminen luottamusverkoston toimijoiden välillä.

Linjaukset

Ei määrätä, mitä protokollia on käytettävä, vaan tämä jää toimijoiden sovittavaksi. Sen sijaan määrätään lopputuloksesta, joka protokollalla on saatava aikaan eli vähimmäistiedoista, jotka protokollan avulla on kyettävä siirtämään (ks. seuraava kohta) ja rajapinnan tietoturva-vaatimuksista.

Malliprofiilit laaditaan Viestintäviraston suosituksena 212/2016 S [11] ja 213/2016 S [12] SAML 2.0 ja Open ID Connect -protokollille ja suositellaan näiden käyttöä.

TUPAS-protokollan [13] kehitystyötä seurataan aktiivisesti.

Määräyksen 14 § on laadittu näiden linjausten mukaisesti.

3.3 Lähteet, referenssit

- Liikenne- ja viestintäviraston suositus 212/2021 S Finnish Trust Network SAML 2.0 Protocol Profile
- Liikenne- ja viestintäviraston suositus 213/2021 S OpenID Connect Protocol Profile for the Finnish Trust Network
- ~~TUPAS, Pankkien Tupas-tunnistuspäätöksen tunnistusperiaatteet v2.0b 28.3.2011~~
- ~~<http://www.finanssiala.fi/maksujenvalitys/dokumentit/Tupas-tunnistuspäätöset-v20b.pdf>~~
- Mahdollisesti ETSI MSS -standardi(t) https://www.etsi.org/deliver/etsi_ts/102200_102299/102204/01.01.04_60/ts_102204v010104p.pdf
- komission yhteentoimivuuspäätös EU 2015/1501

3.4 Toimialakysely 2020 muutostarpeista

Seuraavaan on koottu viraston elokuussa 2020 tekemästä muutostarvekyselystä aiheeseen liittyviä kysymyksiä ja vastauksia.

Vastauksia ei tässä ole anonymisoitu, koska lausunnoissa ei tältä osin ollut lausuntojen antajien esittämän perusteella tai viraston arvion perusteella liikesalaisuuksia tai muita salassa pidettäviä tietoja. **Tämä arvioidaan jokaisessa valmistelu-muistiossa erikseen.**

3.4.1 Rajapinnat

44) **Määräysvaatimukset rajapinnoista.** Onko rajapintasuosituksissa asioita, joita tulisi mielestänne yhentää tai tehostaa nostamalla ne määräykseen? Mitkä asiat ja miksi?

Aktia

- suosituksen uudistaminen on hyvä tehdä erillisenä kokonaisuutenaan
- rajapintasuosituksissa ei ole erityisiä määräyksen tasolle tuotavia kohteita
- Monista yksityiskohdista toteutukseen ja yhteen liittämiseen liittyen jouduttiin osapuolien kanssa neuvottelemaan erikseen, kun osapuolet eivät kokeneet 213/2018 suositusta juurikaan velvoittavana, vaan toteuttivat yhteen liittämistä valitsemansa tuotteen rajoitteiden ja mahdollisuuksien pohjalta.
- On etunsa, että implementaatio-ohje on määräyksen sijaan suositus. Tämä mahdollistaa sen, että osapuolet voisivat tarvittaessa sopia keskenään tavanomaisesta poikkeavasta yhteyskäytännöstä. Ohjeessa ja niihin viittaavissa muissa asiakirjoissa ja säätelyssä olisi hyvä tähdentää, että implementaatio-ohjeiden noudattaminen on suotavaa, jos asiakkaan tavoitteena on sovittaa palvelunsa markkinoiden muiden toimijoiden kanssa.
- teknisen toteutuksen suosituksessa 213/2018 S on puutteita ja määrittelyksiä, jotka ovat ristiriidassa OIIC:n keskeisten määrittelyjen kanssa (OIDCCore). Näiden löytämiseen ja korjaamiseen on kuitenkin konteksti erikseen, kun verkoston teknisessä työryhmässä on käynnissä erillinen linja ko. suosituksen uudistamiseksi.

DVV

- Velvoittaa rajapintojen tarjoaminen IPv6 yli siirtymäajalla/tiettyyn päivämäärään mennessä. Palvelut, jotka ovat saavutettavissa IPv6, käyttäytyvät eri tavalla tilanteessa jossa yksittäinen tunnistuksen välityspalvelun tarjoaja tai tunnistuspalvelun tarjoaja ei pysty tarjoamaan rajapintoja IPv6 verkon yli.

45) Asiointipalvelurajapinta. Olisiko asiointipalvelurajapinnasta tarpeen laatia teknistä ohjausta (suositus)?

Aktia

- Oletus on, että asiointipalvelujen rajapintasuosituksissa olisi hyvä pysyttäytyä mahdollisimman pitkälti yhtenevänä verkoston muiden rajapintojen kanssa.

Findy -konsortio⁵

- Siirtyessämme uusiin hajautettuihin teknologioihin on tärkeää, että tuetaan sekä vallitsevia että tulevia teknologisia standardeja. Niiden kautta voidaan rakentaa digitaalisen identiteetin yhteensopivuus juuri-identiteetistä liiketoimintaprosesseihin asti.

DVV: Ei ole.

46) Käyttäjäraajapinta. Olisiko käyttäjäraajapinnasta tarpeen laatia teknistä ohjausta (määräys, ohje, suositus)?

DVV

- Verkkopalveluiden saavutettavuusdirektiivin ja digipalvelulakiin olisi hyvä viitata. Nämä tulisi huomioida tunnistusvälineen tarjoajien käyttöliittymissä ja tunnistautumismenetelmissä.
- Sen tunnistusta pyytävän asiointipalvelun nimi, johon käyttäjä on kirjautumassa, tulisi olla tunnistuspalvelun tarjoajan etusivulla näkyvässä ennen kuin mitään tietoja syötetään. Tällä varmistettaisiin, että kansalainen pystyisi toteamaan näytetäänkö hänelle oikean tahon tunnistamisen näkymä. Välttävä ratkaisu olisi näyttää edes välityspalveluntarjoajan tunnistetiedot. Tietosuojaseloste pitäisi olla helposti löydettävissä niin välityspalveluntarjoajien kuin tunnistuspalveluntarjoajien näytöiltä, jotta GDPR:n mukainen informointivelvoite täyttyy.

47) Sopiminen protokollasta. Onko määräyksen 14 § mielestänne tarpeellinen?

Aktia

- rajapintasuosituksien tulee olla sopimuksenvaraisia
- rajapintasuosituksien ohjaavuutta tulisi korostaa, jotta yhteen toimivuus markkinatoimijoiden välillä olisi sujuvampaa.

DVV

⁵ Tämä vastaus edustaa Findy-konsortion jäsenten näkemystä ja vastaukset on annettu hajautettujen identiteettiverkkojen kehityksen näkökulmasta. Findy-konsortion tavoitteena on perustaa vuoden 2020 aikana voittoa tavoittelematon osuuskunta hallinnoimaan ja operoimaan vahvistetun datan SSI-verkkoa. Findy-konsortioon kuuluvat ja oheisen vastauksen laatimiseen ovat osallistuneet seuraavat organisaatiot: • Accenture • Suomen Asiakastieto • Posti • Kela • Nixu • Nordea Bank • OP Financial Group • TietoEVRY • Vastuu Group • Verohallinto

- Sopimismahdollisuus on hyvä säilyttää toiminnan osapuolilla. Eli jossain asia on hyvä mainita, pykälän voi säilyttää.

3.4.2 Kysymykset attribuuteista

49) **Suosituksen ja määräyksen suhde.** Attribuuttien määrittelystä SAML ja OpenIDConnect - rajapinnoissa on suositukset, joilla pyritään yhdenmukaistamaan vähimmäisattribuuttien ja valinnaisten attribuuttien käsittely. Onko määräyksen ja suosituksen suhteessa jotain asioita, joita olisi arvioitava määräysvalmistelussa?

50) **Vähimmäisattribuutit.** Onko EU-säätelyn kanssa yhdenmukaisten attribuuttien lisäksi joitain muita tietoja, joita olisi arvioitava määräysvalmistelun yhteydessä?

51) **Valinnaiset attribuutit.** Onko EU-säätelyn kanssa yhdenmukaisten attribuuttien lisäksi joitain muita tietoja, joita olisi arvioitava määräysvalmistelun yhteydessä?

DVV

- Kansalaisuustiedon tarve on noussut esiin FinnAuth-palvelun puitteissa ja voi olla asiointipalvelun kannalta hyvin relevantti. Tunnistustapahtumassa eIDAS-solmupisteelle tulee vain tieto tunnistusvälineen lähtömaasta.
- eIDAS-tunnisteen käsittely asiointipalveluissa on todettu haasteelliseksi. Enintään 256 merkkiä pitkät eIDAS-tunnisteet ovat liian pitkiä monille asiointipalveluille. Näiden mahdolliseen harmonisointiin olisi hyvä sopia kansallinen yhteinen käytäntö. Esimerkkinä vastaavasta käytännöstä on Ruotsissa käytössä oleva prid (https://docs.swedenconnect.se/technical-framework/latest/11_-_eIDAS_Constructed_Attributes_Specification_for_the_Swedish_eID_Framework.html).

Handelsbanken

- Tunnistusvälineen tarjoajalta edellytettävien vähimmäis- ja valinnaisattribuuttien lisäämisessä on syytä olla pidättyväinen.
- Tunnistusvälineen tarjoajilta edellytettäviin muutoksiin liittyvät järjestelmäkustannukset (määrittely, kehittäminen, testaus) ovat yleensä merkittäviä eivätkä hintasäätelyn ollessa voimassa ole missään suhteessa tunnistustapahtumista saataviin korvauksiin.

S-Pankki:

- onko rajapinnassa tarpeen olla valmius välittää tunnistettavan henkilön sukupuoli? Perustelemme tämän sillä, että suunnitteilla olevassa henkilötunnuksen uudistushankkeessa henkilötunnuksesta ei jatkossa ilmenisi sukupuoli. Mielestämme sukupuolitiedon välittäminen on turhaa henkilötiedon välittämistä, kun suurimmassa osassa käyttötapauksista halutaan vain asiakkaan identiteetti (nimi ja hetu).

Aktia

ei näe tarvetta määritellä kattavampaa joukkoa valinnaisia attribuutteja. Tunnistamisessa tapahtuvan henkilötiedon rikastamisen olisi hyvä tapahtua välikerroksissa, ei niinkään suoraan tunnistusvälineeseen liittyen. Tunnistamisen rikastamisen tulisi olla varsinaisesta tunnistustapahtumasta erillinen prosessi.

52) **Julkinen/yksityinen luottava osapuoli.** Näettekö kansallisessa tunnistamisessa tarvetta tiedolle siitä, onko tunnistusta pyytänyt yksityinen vai julkinen asiointipalvelu - esimerkiksi häiriötiedon vaihdon, tietosuojan tai hinnoittelun takia?

Aktia

- ei näe tarvetta tiedolle, onko tunnistukseen luottava osapuoli julkinen vai yksityinen
- Tunnistusvälineen tarjoajan näkökulmasta prosessi on sama tunnistukseen luottavasta osapuolesta riippumatta.

DVV

- Emme näe tällä hetkellä tarvetta tällaiselle tiedolle.

53) Oikeushenkilöt. Onko oikeushenkilöiden vahvan tunnistuksen sääntelyssä asioista, joita olisi tarkasteltava määräysvalmistelussa?

Aktia

- Oikeushenkilön tunnistamisen osalta haastavaa voi olla ulkomaisten organisaatioiden yksilöinti. Kansallisesti Suomessa on rekisterit yritysten ja yhteisöjen yksilöintiin julkiseen rekisteriin rekisteröidyllä tunnisteella. Kansainvälisesti ei ole yhtä yhtenäistä rekisteriä, johon tukeutua.

DVV

- Ei ole arvioitu tarkemmin, koska leimapalveluja ei ole tuotannossa. Nämä vaatimukset on kuitenkin hyvä sovittaa yhteen QWAC-varmenteiden myöntöön ja organisaatioiden tunnistamiseen liittyvien vaatimusten kanssa (OVCP).

54) Ulkomaiset tunnistettavat. Onko yksityisellä sektorilla tarvetta ulkomaisten luonnollisten ja oikeushenkilöiden vahvaan tunnistamiseen sähköisessä asiainnissa? Mitkä attribuutit tällöin olisivat hyödyllisiä?

55) Yleistä attribuuteista. Mitä muuta haluatte tuoda esille attribuuteista?

Findy-konsortio

- Tunnistuspalveluiden rajapintojen avaaminen:
- Määräysten tulisi myös mahdollistaa tunnistuspalveluiden parempi rajapintojen käyttö, velvoittamalla identiteettidatapalveluntarjoajien rajapintojen avaaminen. Rajapintojen avaamista ja kehittämistä tarvitaan monipuolisempien tunnistustapahtumien ja tunnistuksen ketjuttamisen mahdollistamisessa. Esimerkiksi, jos henkilö on tunnistaunut vahvan tunnistamisen välineellä, tulee tunnistamisen yhteydessä pystyä määrittämään kuinka tunnistusta voidaan käyttää tai pyytää esimerkiksi vahvistusta tunnistamisesta. Vaatimus voi tapahtua tunnistustapahtuman yhteydessä, tunnistustietoja esittäessä tai niitä vahvistaessa, tai jossain näiden kombinaatiossa. Identiteetti ja sen vahvistaminen tapahtuu tulevaisuudessa monimutkaisissa ketjutetuissa transaktioissa, mikä tarvitsee monipuolisemman tunnistautumismekanismin.

3.4.3 Kysymykset rajat ylittävästä tunnistamisesta

56) Rajat ylittävä tunnistus julkiselle sektorille. Onko [kyselyssä] edellä esitetty vuoden 2016 ja 2018 määräysvalmisteluun perustuva arvio oikea?

DVV

- Tällä hetkellä arvio on oikea.
- Tulevaisuudessa on mahdollisesti muutostarpeita.

57) **Rajat ylittävä tunnistus julkiselle sektorille.** Onko määräyksen 13 §:ssä muutostarpeita?

DVV: Ei ole.

58) **Rajat ylittävä yksityinen tunnistus.** Onko [kyselyssä] edellä esitetty arvio oikea?

DVV: on.

59) **Rajat ylittävä yksityinen tunnistus.** Onko rajat ylittävässä tunnistusvälityksestä asioita, joita olisi tarkasteltava määräysvalmistelun yhteydessä?

DVV: Ei tällä hetkellä.

4 Muutosvaihtoehdot ja vaikutusarviointi

4.1 Luonnollisen henkilön pakolliset attribuutit (12 §)

Arvioitava kysymys:

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

4.1.1 Arvioitavat vaihtoehdot ja linjaukset

- 1) Lisätään SPname eli tieto luottavasta osapuolesta pakolliseksi attribuutiksi
- 2) Muita turvallisuuden tai yhteentoimivuuden kannalta pakollisia relevantteja attribuutteja ei ole tunnistettu. Muita attribuutteja arvioidaan valinnaisten attribuuttien kohdalla.
- 3) eIDAS-asetuksen mahdollisten muutosten vaikutukset arvioidaan, kun sääntelyn sisältö on selvillä.

4.1.2 Tunnistuspalveluiden kehitys ja toteutettavuus

SPname tuotetaan tunnistusvälityspalvelun ja luottavan osapuolen välillä. Attribuutin tarkoitus on mahdollistaa käyttäjän informointi luottavasta osapuolesta, jolle vahvistus ja henkilötiedot ollaan toimittamassa.

Tunnistustapahtumien toteutus ja käyttäjää informoiva taho tunnistusketjussa vaihtelee, joten ei ole tarkoituksenmukaista määritellä sitovasti, näyttääkö tiedon käyttäjälle tunnistusvälityspalvelu vai tunnistusvälineen tarjoaja.

Aloite attribuutin pakollisuuteen on tullut tunnistusvälineen tarjoajien puolelta.

4.1.3 Turvallisuusvaikutukset

SPname attribuutti mahdollistaa sen, 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. Luotettavuuden takia vastuun attribuutista on oltava tunnistusvälityspalvelulla, koska asiointipalvelun antaman tiedon käyttäminen vesittää tarkoituksen.

4.1.4 Taloudelliset vaikutukset

Tunnistusvälineen tarjoaja. Pakolliset attribuutit sisältyvät tunnustuslain 12 b §:n perusteella tunnustustapahtuman enimmäishintasääntelyn piiriin. Uusien attribuuttien tuottaminen vaikuttaa siis tunnistusvälineen tarjoajan kustannuksiin.

SPname-attribuutin tuottaa *tunnistusvälityspalvelu*.

Attribuutti on ollut määriteltynä rajapintasuosituksiin, joten valmius voi olla osalla tunnistusvälineen tarjoajista jo määriteltynä rajapinnoissa. Tunnistusvälineen tarjoajalta se edellyttää kentän lisäämistä käytössä oleviin rajapintamäärittelyihin ja käyttäjälle annettavan informaation lisäämistä tunnistuspyynnössä.

Tunnustuslain 12 a §:n 5 momentissa säädetään luottamusverkostossa saadun tiedon käyttörajoituksista ja vahingonkorvausvastuusta. Tällä perusteella liikenne- ja viestintävirasto arvioi, että tunnistusvälineen tarjoaja ei voi käyttää saamaansa tietoa tunnistusvälityspalvelun asiointipalveluasiakkaista esimerkiksi oman kilpailevan tunnistusvälityksensä markkinoinnissa.

Tunnistusvälityspalvelu. Tunnistusvälityspalvelu tuottaa SPname-attribuutin (luottava osapuoli, jolle tunnustus ollaan välittämässä). Asiointipalveluiden kanssa on joka tapauksessa tehtävä sopimukset, joten palvelunimen määrittely sopimussuhteessa ei aiheuttane olennaisia lisäkustannuksia. Sisällöllisen määrittelyn lisäksi muutos edellyttää kentän lisäämistä käytössä oleviin rajapintamäärittelyihin. Attribuutti on ollut määriteltynä rajapintasuosituksiin, joten valmius voi olla osalla tunnistusvälineen tarjoajista jo määriteltynä rajapinnoissa.

Asiointipalvelu/luottava osapuoli. Asiointipalvelun on yhdessä tunnistusvälityspalvelun kanssa määriteltävä käyttäjälle informoitava palvelunsa nimi. Tällä ei ole olennaista taloudellista vaikutusta.

4.1.5 Muut ohjauskeinot

Ohje. Valvonnan havaintojen ja kyselyssä saadun palautteen perusteella virasto arvioi, että attribuutin käyttöönotto kaikissa tunnistuspalveluissa ei välttämättä toteutuisi pelkällä ohjeella, vaan edellyttää sitovaa määräystä.

Suositus. Attribuutti on jo viraston rajapintasuosituksissa. Se status muutetaan suositusten päivityksessä pakolliseksi.

Yhteissääntely. Luottamusverkostossa voidaan tarvittaessa vaihtaa tietoa asiointipalvelun nimen määrittelyyn liittyvistä havainnoista ja tiedon esittämisestä käyttäjälle.

Informaatiolla ohjaaminen. Ei huomioita.

4.2 Luonnollisen henkilön valinnaiset attribuutit (12 §)

Arvioitava kysymys:

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

4.2.1 Arvioitavat vaihtoehdot ja linjaukset

- a) Olisiko tarvetta lisätä luonnollisen valinnaisiin attribuutteihin kansalaisuus, syntymämaa, syntymäkaupunki, asuinmaa, puhelinnumero, sähköposti.
- b) Oikhlö: puhelinnumero, sähköposti

- c) eIDAS-asetuksen mahdollisten muutosten vaikutukset arvioidaan, kun sääntelyn sisältö on selvillä.

4.2.2 Tunnistuspalveluiden kehitys

Rajat ylittävän tunnistamisen kehitys. Mainitut attribuutit ovat keskustelussa rajat ylittävän tunnistamisen teknisessä eIDAS -ryhmässä. Attribuutit edistäisivät rajat ylittävän tunnistamisen yhteentoimivuutta ja mahdollisuutta yhdistää henkilö tunnistuksen vastaanottomaassa asiointipalvelussa häntä koskeviin mahdollisiin aikaisempiin henkilötietoihin.

Attribuuttien lähteet ja mahdollisuus niiden luotettavaan varmentamiseen vaihtelee. Attribuuteilla voisi olla eri luotettavuustasoja.

4.2.3 Taloudelliset vaikutukset

Attribuutit, jotka eivät sisälly komission päätökseen, eivät kuulu TunnL 12 b hintasääntelyn piiriin.

Lisätiedot voi hankkia/varmentaa ja tarjota tunnistusvälineen tarjoaja tai tunnistusvälityspalvelu.

Henkilötiedot eivät sisälly säänneltyihin välttämättömiin tunnistuksessa käsiteltäviin henkilötietoihin. Henkilötietojen käsittelyperusteet ja suojaan liittyvät velvoitteet olisi arvioitava ja huolehdittava yleisen tietosuoja-asetuksen perusteella.

4.2.4 Muut ohjauskeinot

Ohje. Ei huomioita.

Suositus. Yhteentoimivuuden mahdollistamiseksi valinnaiset attribuutit ja niiden esitystavat voidaan listata rajapintasuosituksissa.

Yhteissääntely. Luottamusverkostossa voidaan tarvittaessa vaihtaa tietoa asiointipalveluiden attribuuttitarpeista.

Informaatiolla ohjaaminen. Yhteentoimivuus edellyttää yhtenäisiä rajapintamäärittelyjä. Pelkkä informaatio eri tunnistuspalveluilla käytössä olevista attribuuteista ei ole toimiva keino yhteentoimivan attribuuttilistan ja esitystavan määrittelemiseksi monitoimijaympäristössä.

4.3 Ensitunnistamisen attribuutit

Arvioitava kysymys:

- a) Määritelläänkö ensitunnistuksen ketjuttamisessa tarvittavia attribuuttiteja pakolliseksi?
- b) Mitkä attribuutit ovat saatavilla tai tarpeellisia? Esim. tunnistuspyynnön tyyppi (ensitunnistus), ensitunnistuksen pyytäjä ja tarjoaja, tarjotun ensitunnistuksen oma perusta (kuten tieto henkilöllisyydestä tai ketjutuksesta)?
- c) Millainen siirtymäaikataulu toteutukselle tarvittaisiin?

4.3.1 Arvioitavat vaihtoehdot ja linjaukset

- a) Lisätään pakolliset attribuuttivaatimukset *tunnistusvälineen tarjoajien väliseen* rajapintaan
- b) Lisätään pakolliset attribuuttivaatimukset yleisesti tunnistusvälineen tarjoajien väliseen ja tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun väliseen rajapintaan
- c) Harkittavia attribuutteja vastausviestissä:
1. tunnistusvälineen myöntämisaika
 2. aikaisempi tunnistusketju

3. tunnistusvälineen myöntämisperuste tunnistusasiakirja
4. tunnistusvälineen myöntämisperuste ketjutus
5. ketjun ensimmäinen tunnistusväline

4.3.2 Tunnistuspalveluiden kehitys, toteutettavuus

Vuonna 2016 tuotiin pidemmän tähtäimen kehityksenä esiin toivomus siitä, että rajapinnan kautta voitaisiin välittää tietoa ensitunnistamisesta (esim. mihin henkilökohtainen ensitunnistaminen on perustunut: passi, henkilökortti, sähköinen tunnistaminen).

Rajapintasuosituksissa on jo määritelty ensitunnistustapahtuma: *FTN chain level*. Tämä esitetään tunnistusvälineen tarjoajan toiselle tunnistusvälineen tarjoajalle tekemässä tunnistuspyynnössä. Pyyntö- ja tunnistus voidaan välittää myös tunnistuspalvelun kautta.

Tekniseltä kannalta tiedot ovat valmiina, joten toteuttaminen vaatisi vain rajapintamäärittelyjen laatimista suositukseen ja sen mukaisia muutoksia tunnistusvälineen tarjoajien rajapintoihin ja tietokantoihin. Luottamusverkoston sisällä on oletettavasti käytössä yksi rajapintamäärittely muille luottamusverkoston jäsenille, joten erillisen määrittelyn toteuttaminen tunnistusvälityspalveluille ei leine tarkoituksenmukaista.

Tieto tunnistuksen (autentikoinnin) tekijästä välittyy jokaisessa tunnistustapahtumassa, ei ole tarpeen arvioida tässä erikseen.

Tiedot luotetun tunnistusvälineen myöntämisperusteista eli

- onko se myönnetty henkilöllisyystodistuksen tarkistamisen perusteella vai ketjuttamalla
- tiedot ketjusta
- tiedot ketjun ensimmäisen tunnistusvälineen myöntäjästä ja myöntämisperusteesta.

4.3.3 Turvallisuusvaikutukset

Tietoturvallisuuden ja sähköisen tunnistuksen yleisen luotettavuuden kannalta tietojen välittäminen olisi eduksi. Hintasäätelyn takia ensitunnistuksen ketjutuksen käytön voi olettaa lisääntyvän.

Tunnistus- ja luottamuspalvelulain 17 §:n muutoksella on mahdollistettu se, että tunnistusvälineen tarjoajat voivat rajattomasti ketjuttaa tunnistamista eli luoda uusia sähköisiä tunnistusvälineitä luottamalla muiden tarjoamien sähköisiin tunnisteisiin.

Tietoturvaloukkausten selvittämistilanteessa on tärkeää, että tieto ketjuttamisesta on tavalla tai toisella selvitettävissä nopeasti ja tehokkaasti. Jos tunnistusvälineen tarjoaja myöntää esimerkiksi tunnisteita varastettujen tai väärennettyjen henkilöllisyystodistusten perusteella, on pysyttävä selvittämään, onko näillä väärän henkilön hallussa olevilla sähköisillä tunnistusvälineillä haettu sähköisesti uusia tunnistusvälineitä.

4.3.4 Taloudelliset vaikutukset

Tunnistusvälineen tarjoaja.

Pakolliset attributit sisältyvät tunnistuslain 12 b §:n perusteella tunnistustapahtuman enimmäishintasäätelyn piiriin. Tekniseltä kannalta tiedot ovat valmiina, joten toteuttaminen vaatisi vain rajapintamäärittelyjen laatimista suositukseen ja sen mukaisia muutoksia tunnistusvälineen tarjoajien rajapintoihin ja tietokantoihin.

Tieto ensitunnistamisen tekemisestä ja ketjussa olevista toimijoista tukisi riskin arviointia ja hallintaa. Toisen tunnistusvälineeseen luottava välineen myöntäjä kantaa tunnistus- ja luottamuspalvelulain 17.4 §:n säännöksen perusteella vahinkovastuun. Ketjuttaminen edellyttääkin

sitä, että ketjuttamista hyödyntävä välineen myöntäjä arvioi, millainen riski luotettuun tunnistukseen mahdollisesti liittyy. Tähän riskiin vaikuttavia tekijöitä ovat se [seuraavassa lainaus vuoden 2016 arviosta], kuinka kauan sitten ja minkä henkilöllisyystodistuksen perusteella alkuperäinen henkilökohtainen tunnistaminen on tehty, onko ketjussa useampi tunnistusvälineen myöntäjä, onko jokin ketjussa ollut tunnistusvälineen myöntäjä lopettanut toimintansa ja onko ketjussa oleville tunnistusvälineen myöntäjille tapahtunut tietoturvaloukkauksia, jotka ovat voineet vaikuttaa tiedon eheyteen.

Tunnistusvälityspalvelu. Ensitunnistuksen ketjutuksen välittäminen voi olla myös tunnistusvälityspalvelun tehtävä. Luottamusverkoston sisällä on oletettavasti käytössä yksi rajapintamäärittely muille luottamusverkoston jäsenille, joten erillisen määrittelyn toteuttaminen tunnistusvälityspalveluille ei liene tarkoituksenmukaista.

Asiointipalvelu/luottava osapuoli. Ei vaikutusta.

4.3.5 Muut ohjauskeinot

Ohje.
Suositus.
Yhteissääntely.
Informaatiolla ohjaaminen.

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

Arvioitava kysymys:

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

4.4.1 Tunnistuspalveluiden kehitys ja toteutettavuus

Rikastaminen, vrt. kohta 4.2 valinnaiset attribuutit.

Köyhdyttäminen/pseudonymisointi

Vahvan sähköisen tunnistuksen sääntely ei edellytä, että pakolliset tai valinnaiset attribuutit toimitetaan tai vahvistetaan luottavalle osapuolelle.

Vahva sähköinen tunnistuspalvelu voidaan tuotteistaa myös siten, että luottavalle osapuolelle toimitetaan vain kertaluonteinen pseudonyymi ("salanimi"), pysyvä pseudonyymi ("salanimi"), tai vaikkapa vahvistus tunnistaution täysi-ikäisyydestä.

Esim.

"on alaikäinen", "on kysytyn maksukortin haltija", "on vantaalainen"
vrt. on "121212-999Ä, Alma Virtanen"

Pseudonyymiin perustuva vahva autentikointi lisäisi vahvan sähköisen tunnistuksen käyttökel-
poisuutta ja potentiaalisia käyttötilanteita.

Mitä toteuttaminen edellyttäisi?

Kuka informoi käyttäjää siitä, että asiointipalveluun X ollaan välittämässä vahvistus vain tietystä tiedosta tai vain siitä, että on tunnistettu.

4.4.2 Turvallisuus ja yhteentoimivuus

Tunnistuksen jäljitettävyyden kannalta myös pseudonymisoidut tunnistustapahtumat olisi välitettävä ja käsiteltävä **luottamusverkoston sisällä** normaalisti eli välitettävä ja tallennettava henkilötiedot. Muutos tapahtuisi tunnistusvälityspalvelun ja asiointipalvelun välillä.

Pseudonyymiin perustuva vahva autentikointi lisäisi turvallisuutta ja tietosuojaa asioinnissa myös sellaisissa tilanteissa, joissa henkilöä ei ole tarpeellista identifioida asiointipalvelussa.

4.4.3 Taloudelliset vaikutukset

Pseudonyymiin perustuva vahva autentikointi lisäisi vahvan sähköisen tunnistuksen käyttökel-
poisuutta ja potentiaalisia käyttötilanteita.

4.4.4 Muut ohjauskeinot

Ohje.

Suositus.

Yhteissääntely.

Informaatiolla ohjaaminen.

4.5 Rajapintaprotokollat ja tekninen yhteentoimivuus (14 §)

Arvioitava kysymys:

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

4.5.1 Tunnistuspalveluiden kehitys ja toteutettavuus

Virasto harkitsee säännöksen tarkentamista esimerkiksi viittauksella suositeltuihin protokoliin. Myös rajapinnan yleisen tason ominaisuuksien tarkentamista arvioidaan rajapintasuosituksen soveltamisessa saatujen kokemusten perusteella.

Kyselyyn saadut vastaukset tukivat viraston ennakoarviota siitä, että 14 § informatiivinen säännös on hyvä säilyttää. Rajapintojen tarkempi ohjaaminen on tarkoituksenmukaista edelleen tehdä suosituksella. Suositusten tehokkuudesta tai pikemminkin tehottomuudesta yhteentoimivuuden edistämiseksi tuli kuitenkin kriittisiä kommentteja.

Kyselyyn saatujen vastausten perusteella rajapintaprotokollien tekniseen ohjaukseen ei liity suuria muutostarpeita. Luottamusverkoston sisällä OpenIDConnect ja SAML vaikuttavat riittävästi mahdollistamaan tunnistuspalveluiden kehityksen. ETSI on jossain määrin käytössä mobiilivälikomponenttien välisissä rajapinnoissa.

Kyselyn perusteella vaikuttaa siltä, että teknisessä ohjauksessa ei ole tarpeen käsitellä tarkemmin uusia protokollia.

Kyselyssä tuli esille tarve edistää IPv6-tukea rajapinnoissa. Asia ei ole aikaisemmin tullut esille ohjauksessa tai valvonnassa. Valmistelussa voidaan tarkastella, millainen kyvykyys toimijoilla tällä hetkellä on ja miten asiaa voisi tarkoituksenmukaisesti edistää.

4.5.2 Taloudelliset vaikutukset

Rajapintojen yhteentoimivuuden tilanne on kyselyn perusteella saatu muutosvaiheen jälkeen melko vakiintuneelle tasolle. Yhteentoimivuutta voidaan kehittää rajapintasuosituksen päivityksillä ja luottamusverkoston yhteistyöllä. Mahdollisimman vakiintunut määrittely ja sujuva yhteistyö vähentävät toimijoiden työtä ja siten kustannuksia. Nähtävissä ei ole tarvetta uusille muutoksille, jotka lisäisivät toimijoiden kustannuksia.

Rajapintamäärittelyjen vakiintunut ja dokumentoitu käytäntö helpottaa uusien tunnistuspalveluiden liittymistä teknisesti luottamusverkostoon ja siten markkinoille tuloa.

4.5.3 Muut ohjauskeinot

Ohje.

Suositus.

Yhteissääntely. Virasto on antanut kysyttäessä neuvontaa uusien protokollien tuomisesta luottamusverkoston sisäisiin rajapintoihin. Prosessista ei ole määräysvaltuutta, joten luottamusverkoston yhteistoimintaryhmän tai viraston ohjauksen käytäntöä voisi kirjata perustelumuihistoon tai johonkin ohjeeseen tai suositukseen.

Informaatiolla ohjaaminen.

4.6 Protokollien tai rajapintamäärittelyjen vaikutus asiointipalveluiden toimintoihin

Arvioitava kysymys: Lain 12 a § mukaan luottamusverkoston yhteistyöllä on varmistettava, että tekniset rajapinnat mahdollistavat yleisesti tunnettujen standardien mukaisten rajapintojen tarjoamisen luottaville osapuolille.

a) Liittyykö tunnistusvälineen ja tunnistusvälityspalvelun välisen rajapinnan määrittelyyn piirteitä, joilla on vaikutusta asiointipalveluiden rajapintoihin.

4.6.1 Tunnistuspalveluiden kehitys

Kyselyssä ei tullut esille erityisiä asiointipalvelurajapintojen mahdollistamiseen liittyviä tarpeita.

Virasto nostaa aiheen esille nyt valmistelun yhteydessä, jotta mahdolliset havainnot saadaan keskusteluun.

Voidaanko esimerkiksi tunnistuslain 18 §:ssä asiointipalvelulle asetetun tarkistusvelvollisuuden toteuttamista edistää rajapintojen ominaisuuksilla yhteentoimivasti luottamusverkostossa, jos tunnistusvälineen tarjoaja on asettanut tunnistusvälineelle käyttörajoituksia.

4.6.2 Turvallisuus ja yhteentoimivuus

4.6.3 Taloudelliset vaikutukset

4.6.4 Muut ohjauskeinot

Ohje.

Suositus.

Yhteissääntely.

Informaatiolla ohjaaminen.

5 Säädäntö

5.1 Määräyksen antamisen perusta

TunnL 12 a § ja 42 § 2 mom.

Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä:

- 1) tunnistusjärjestelmän 8 §:n 1 momentin 4 ja 5 kohdan mukaisista turvallisuutta ja luotettavuutta koskevista vaatimuksista;**
- 2) 10 §:ssä tarkoitettujen ilmoitettavien tietojen sisällöstä ja niiden toimittamisesta Liikenne- ja viestintävirastolle;
- 3) 12 a §:n 3 momentissa tarkoitetuista luottamusverkon rajapintojen ominaisuuksista;**
- 4) siitä, milloin 16 §:ssä tarkoitettu häiriö on merkittävä sekä 16 §:n 1 momentissa tarkoitettun ilmoituksen sisällöstä, muodosta ja toimittamisesta;
- 5) 29, 30 ja 32 §:ssä tarkoitetuista arvioitavan tunnistus- tai luottamuspalvelun sekä kansallisen solmupisteen vaatimustenmukaisuuden arviointiperusteista;
- 6) 33 §:ssä säädettyistä vaatimustenmukaisuuden arviointielimen pätevyysvaatimuksista ottaen huomioon, mitä sähköisestä tunnistamisesta ja luottamuspalveluista annetussa EU:n asetuksessa säädetään;
- 7) 35 §:ssä tarkoitettuun hakemukseen sisällytettävistä tiedoista ja niiden toimittamisesta Liikenne- ja viestintävirastolle;
- 8) 36 §:ssä tarkoitettua sertifiointilaitosta koskevista vaatimuksista, sertifiointissa noudatettavasta menettelystä sekä sähköisen allekirjoituksen ja leiman luontivälinettä koskevista vaatimuksista ottaen huomioon, mitä sähköisestä tunnistamisesta ja luottamuspalveluista annetussa EU:n asetuksessa säädetään.

5.2 Asiaan liittyvät säännökset

Valtioneuvoston asetus vahvan sähköisen tunnistuspalvelun tarjoajien luottamusverkostosta 2016/169

1 § Luottamusverkon 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;
- 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 tarkoitettun tunnistetiedon veloituksen välittämiseen tarvittavasta tai muusta luottamusverkon 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.

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

TunnL 12 a § Tunnistuspalvelun tarjoajien luottamusverkosto

1 mom. Tunnistuspalvelun tarjoaja liittyy osaksi luottamusverkostoa tehdessään 10 §:n mukaisen ilmoituksen Liikenne- ja viestintävirastolle.

2 mom. Tunnistusvälineen tarjoajan on tarjottava tunnistuspalvelunsa käyttöoikeutta tunnistusvälityspalvelun tarjoajille siten, että ne voivat välittää tunnistustapahtumia sähköiseen tunnistukseen luottavalle osapuolelle. [...]

3 mom. 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.

5 mom. Tunnistuspalvelun tarjoaja saa käyttää käyttöoikeuden luovutuksen tai 16 §:n nojalla saatua toista tunnistuspalvelun tarjoajaa koskevia tietoja vain siihen tarkoitukseen, jota varten ne on tunnistuspalvelun tarjoajalle annettu. Tietoja saavat tunnistuspalvelun tarjoajan palveluksessa tai sen lukuun käsitellä ainoastaan ne, jotka tarvitsevat tietoja välttämättä työssään. Tietoja on muutoinkin käsiteltävä siten, ettei toisen tunnistuspalvelun tarjoajan liikesalaisuuksia vaaranneta. Tunnistuspalvelun tarjoaja, joka aiheuttaa tämän momentin vastaisella menettelyllä vahinkoa toiselle tunnistuspalvelun tarjoajalle, on velvollinen korvaamaan menettelystään aiheutuvan vahingon.

6 mom. Luottamusverkoston hallinnollisista käytännöistä, teknisistä rajapinnoista ja hallinnollisista vastuista annetaan tarkempia säännöksiä valtioneuvoston asetuksella.

TunnL 12 b § Tunnistuspalvelun käyttöoikeuden toimitusehdot ja tunnistusvälineen tarjoajan tiedonantovelvollisuus

Tunnistusvälineen tarjoajan on julkaistava tunnistuspalvelunsa käyttöoikeuden toimitusehdot sekä muut käyttöoikeuden luovuttamisen ja tunnistuspalveluiden yhteentoimivuuden kannalta merkitykselliset tiedot verkkosivuillaan. Tunnistusvälineen tarjoajan on julkaistava vähintään seuraavat tiedot:

- 1) kuvaus tunnistusvälineestä mukaan lukien tieto saatavilla olevista yhteentoimivuuksjärjestelmän vahvistamisesta sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 12 artiklan 8 kohdan mukaisesti annetun komission täytäntöönpanoasetuksen (EU) 2015/1501 liitteen mukaisista henkilön tunnistetiedoista;
- 2) tunnistusvälineeseen liittyvät mahdolliset 18 §:ssä tarkoitetut estot ja rajoitukset sekä tieto siitä, miten ne ovat luottavien osapuolten tiedossa tai havaittavissa, taikka tiedot käytörajoituksen teknisestä toteuttamisesta;
- 3) kuvaus tunnistustapahtumien välityksen teknisistä rajapinnoista ja testausjärjestelystä siltä osin kuin ne eivät sisällä liikesalaisuuksia tai tietoturva vaarantavia tietoja; [...]

TunnL 17 § Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen

4 mom. Tunnistusvälineen tarjoajan on mahdollistettava se, että toinen tunnistusvälineen tarjoaja voi käyttää sen myöntämää vahvaa sähköistä tunnistusvälinettä ensitunnistamiseen haettaessa vastaavan tai alemman varmuustason vahvaa sähköistä tunnistusvälinettä. Mitä 12 a ja 12 b §:ssä säädetään tunnistuspalvelun käyttöoikeuden luovutuksesta ja toimitusehtojen julkaisemisesta, sovelletaan myös tässä momentissa tarkoitettuun tunnistusvälineen käyttämiseen ensitunnistamisessa. ([29.3.2019/412](#))

5 mom. Aiempaan ensitunnistamiseen luottava tunnistusvälineen tarjoaja vastaa mahdollisesta aiemman ensitunnistamisen virheellisyydestä aiheutuvasta vahingosta suhteessa vahinkoa kärsineeseen. ([29.3.2019/412](#))

TunnL 18 § Oikeustoimen tekemiseen kohdistuvat estot ja rajoitukset

Tunnistuspalvelun tarjoajan, tunnistuspalvelua käyttävän palveluntarjoajan sekä tunnistusvälineen haltijan välisillä sopimuksilla voidaan tunnistusvälineen käyttäminen oikeustoimien tekemiseen estää. Lisäksi oikeustoimien tekemiselle voidaan asettaa sekä käyttötarkoitukseen että tapahtumien rahamääräiseen arvoon liittyviä rajoituksia. Estot tai rajoitukset eivät saa kohdistua yksittäisiin palveluntarjoajiin, eivätkä ne saa riippua siitä, mikä tunnistusvälytyspalvelun tarjoaja välittää tunnistustapahtuman.

Tunnistuspalvelun tarjoajan on huolehdittava siitä, että estot tai rajoitukset ovat kaikkien osapuolten tiedossa tai havaittavissa helpolla sekä selvällä ja ymmärrettävällä tavalla. Tunnistusvälineen tarjoaja voi myös toteuttaa estot tai rajoitukset teknisin keinoin. Tunnistuspalvelun tarjoaja ei vastaa niistä toimesta, jotka on tehty estojen tai rajoitusten vastaisesti siitä huolimatta, että tunnistuspalvelun tarjoaja on toiminut huolellisesti.

Tunnistusvälineen tarjoajan on järjestettävä tunnistuspalvelua käyttävälle palveluntarjoajalle mahdollisuus tarkastaa tunnistusvälineeseen liittyvät estot tai rajoitukset ympäri vuorokauden. Velvollisuutta ei kuitenkaan ole, jos tunnistusvälineen estojen tai rajoitusten vastainen käyttö on teknisin keinoin estetty.

Tunnistuspalvelua käyttävän palveluntarjoajan on tarkastettava tunnistuspalvelun tarjoajan ylläpitämistä järjestelmistä ja rekistereistä mahdolliset estot tai rajoitukset tunnistusvälineen käytön yhteydessä. Tarkastaminen ei kuitenkaan ole tarpeen, jos tunnistusvälineen estojen tai rajoitusten vastainen käyttö on teknisin keinoin estetty.

(EU) 2015/1501 Komission täytäntöönpanoasetus ... yhteentoimivuusjärjestelmän vahvistamisesta

11 artikla Henkilön tunnistetiedot

1. Luonnollista tai oikeushenkilöä yksilöivästi edustavien henkilön tunnistetietojen on vähimmillään täytettävä liitteessä esitetyt vaatimukset, kun näitä tietoja käytetään rajat ylittävissä tapauksissa.
2. Oikeushenkilöä edustavaa luonnollista henkilöä koskevien tietojen on vähimmillään sisällettävä liitteessä luonnollisten ja oikeushenkilöiden osalta mainittujen määreiden yhdistelmä, kun näitä tietoja käytetään rajat ylittävissä tapauksissa.
3. Tiedot on toimitettava käyttäen alkuperäistä merkistöä ja lisäksi tarvittaessa transliteroitava latinalaisin kirjaimin.

LIITE

Luonnollista tai oikeushenkilöä yksilöivästi edustavien henkilön tunnistetietojen vähimmäisvaatimukset (11 artikla)

1. Luonnollisen henkilön tunnistetietoja koskevat vähimmäisvaatimukset

Luonnollisen henkilön vähimmäistietojen on sisällettävä kaikki seuraavat pakolliset määreet:

- a) nykyinen sukunimi (-nimet);
- b) nykyinen etunimi (-nimet);
- c) syntymäaika;
- d) yksilöllinen tunniste, jonka lähettävä jäsenvaltio on luonut noudattaen teknisistä eritelmiä rajat ylittävää tunnistamista varten ja joka on mahdollisimman pitkäkestoinen.

Luonnollisen henkilön vähimmäistiedot voivat sisältää yhden tai useamman seuraavista lisämääreistä:

- a) etunimi (-nimet) ja sukunimi (-nimet) syntymähetkellä;
- b) syntymäpaikka;
- c) nykyinen osoite;
- d) sukupuoli.

2. Oikeushenkilön tunnistetietoja koskevat vähimmäisvaatimukset

Oikeushenkilön vähimmäistietojen on sisällettävä kaikki seuraavat pakolliset määreet:

- a) *nykyinen virallinen nimi;*
- b) *yksilöllinen tunniste, jonka lähettävä jäsenvaltio on luonut noudattaen teknisiä eritelmiä rajat ylittävää tunnistamista varten ja joka on mahdollisimman pitkäkestoinen.*

Oikeushenkilön vähimmäistiedot voivat sisältää yhden tai useamman seuraavista lisämääreistä:

- 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);*
- g) *neuvoston asetuksen N:o 389/2012 2 artiklan 12 kohdassa tarkoitettu valmisteveronumero.*

5.3 Muu sääntely

Yleinen tietosuojasäätely.