

3.5.2018

Dnro:  
1497/060/2017

## Lausuntoyhteenveto ja linjaukset määräys 72A/2018

### 1 Lausunnot

Lausunnon 9.4.2018 tehtyyn lausuntopyyntöön antoivat

- Finanssiala ry
- Danske Bank A/S, Suomen sivuliike
- Nets Denmark A/S, Suomen sivuliike
- Nordea Bank Ab (Publ.), Suomen sivuliike
- OP Ryhmä
- Signom Oy
- Ålandsbanken Abp
- Väestörekisterikeskus
- Kilpailu- ja kuluttajavirasto
- Finanssivalvonta

### 2 Yhteenveto lausunnoista ja Viestintäviraston linjaukset

#### 2.1 Tupas-toteutusten muuttamisen siirtymäaika

##### 2.1.1 Muutosehdotus

Määräysmuutoksella Viestintävirasto on harkinnut jatkettavaksi 25 §:ssä määrättyä siirtymäaikaa, jossa nykyiset vahvan tunnistamisen Tupas-toteutukset on korvattava toteutuksilla, jotka täyttävät määräyksen tietoturva-vaatimukset tietoliikenteen salaukselle.

Salauksen lisääminen vaatii toimenpiteitä myös asiointipalveluilta, jotka käyttävät pankkitunnistusta asiakkaidensa tunnistamiseen verkkopalveluisaan.

Viestintävirasto on ehdottanut siirtymäaika jatkettavaksi vaiheittain:

- Tunnistuspalveluiden olisi laadittava tarvittavat määrittelyt 1.10.2018 mennessä.
- Uudet rajapinnat olisi saatettava tarjolle asiointipalveluille viimeistään 1.1.2019.
- Muutokset olisi tehtävä kaikissa asiointipalveluissa 1.10.2019 mennessä.

##### 2.1.2 Lausunnot

Siirtymäajan vaiheistamista ehdotetulla tavalla kannatettiin (OP Ryhmä, Väestörekisterikeskus varauksin).

Toisaalta kritisoitiin, että koko Tupas-toteutuksia koskevan siirtymäajan jatkaminen on epätasapuolista niitä tunnistuspalveluita kohtaan, jotka ovat toteuttaneet vaatimustenmukaiset rajapinnat muita protokollia käyttäen ja että jatkettu siirtymäaika on epätoivottava siksi, että tietoturvallisuuden parantaminen viivästyy lisää (Väestörekisterikeskus).

---

### 1 vaihe

Ensimmäisen vaiheen määräaika 1.10.2018 ei kommentoitu.

### 2 vaihe

Uuden rajapinnan tarjolle saattamisen määräaika 1.1.2019 vastustettiin (Finanssiala, Danske, Nordea) sillä perusteella, että se ajoittuu pankkialan IT-kehityksen vuodenvaihteen rauhoitusjaksolle, jolloin tosiasiallinen määräaika olisi jo joulukuun alussa. Ehdotusta vastustettiin myös sillä perusteella, että rajapintojen määrittelyn takarajasta 1.10.2018 laskettuna tuotantoon viemiseen olisi aikaa vähimmillään kaksi kuukautta. Määräajaksi ehdotettiin 28.2.2019 tai 31.3.2019 (Finanssiala, Danske, Nordea).

Toisaalta määräaikoja kannatettiin (Finanssivalvonta, Väestörekisterikeskus, OP Ryhmä) ja lausuttiin, että valmius vaatimustenmukaisen rajapinnan tarjoamiseen asiointipalveluille on jo nyt (Nets) tai viimeistään ehdotuksessa aikataulussa (OP Ryhmä, Ålandsbanken). Lausunnoissa tuotiin myös esille, että on pankkikohtaisesti vaihtelevaa, milloin muutoksia ei tehdä (Finanssivalvonta).

Määräaika 1.10.2019 kaikkien asiointipalvelurajapintojen saattamiselle vaatimustenmukaiseksi arvioitiin useimmissa lausunnoissa (Finanssiala, Danske, Nordea, OP Ryhmä) tiukaksi, mutta mahdolliseksi. Lausuntojen perusteella Tupas-rajapinnat tullaan korvaamaan tunnistus- ja asiointipalvelun välillä SAML- ja/tai OIDC-rajapinnoilla.

#### 2.1.3 Viestintäviraston päätelmät ja linjaukset

##### **Määrittelyn määräajaksi määrätään 1.10.2018 ja tarjolle saattamisen määräajaksi 1.3.2019.**

OP Ryhmän, Ålandsbankenin ja Netsin lausunnot tukevat sitä Viestintäviraston käsitystä, että vaatimukset täyttävä rajapinta on ollut mahdollista suunnitella tuotantovalmiiksi olemassa olevilla tiedoilla jopa alun perin määrättyssä aikataulussa.

Lausunnoissa tuodaan perustellusti esille, että ehdotettu määräaika uusien rajapintojen tarjolle saattamiselle 1.1.2019 keskellä IT-toimintojen rauhoitusaikaa on ajankohtana hankala.

Väestörekisterikeskuksen lausunnossa muistutetaan, että vain Tupas-toteutuksiin liittyvä siirtymäaika ei ole tasapuolinen toimijoille ja että pitkä siirtymäaika on epätoivottava tietoturvallisuuden kannalta.

Viestintävirasto olettaa, että muutkin toimijat kuin OP Ryhmä ja Ålandsbanken ovat kyenneet valmistelevaan määrittelyä. Virasto katsoo, että myös tuotantoon viemisen suunnittelu olisi mahdollista aloittaa ennen teknisten määrittelyjen valmistumiselle ehdotettua takarajaa 1.10.2018 ja tuotantoon viemiselle käytössä oleva aika olisi siten käytännössä pidempi kuin lausunnoissa todettu 2 kuukautta (1.10.-30.11.2018 määrittelyjen määräajasta rauhoitusajan alkamiseen).

Viestintävirasto joutuu kuitenkin toteamaan, että OP Ryhmä ja Ålandsbanken lukuun ottamatta lausunnoissa ei vastata kysymykseen, kuinka pitkällä uusien SAML- ja/tai OIDC-rajapintojen suunnittelu ja määrittely on tällä hetkellä. Lausuntojen perusteella tuotantoon viemiselle jäisi lyhyt aika

ja se osuisi vuodenvaihteen rauhoitus aikaan. Näillä perusteilla Viestintävirasto katsoo, että osalla pankeista kyky tarjota luotettavasti uudet asiointipalvelurajapinnat 1.1.2019 on siinä määrin epävarma, että tarjolle saattamisen takaraja on turvallisempaa määrätä pidemmälle. Määräajan asettaminen päivämäärään 1.3.2019 mahdollistaa muutosten toteuttamisen vuodenvaihteen rauhoitusjakson jälkeen.

Viestintävirasto suosittelee, että ne pankit, jotka kykenevät toteutukseen aikaisemmin, tuovat rajapinnat tarjolle ennen määräajan päättymistä.

### 3 vaihe

Viestintävirasto katsoo, että tunnistuspalvelun ja asiointipalvelun välisen rajapinnan muuttaminen vaatimustenmukaiseksi voidaan määrätä tehtäväksi viimeistään 1.10.2019.

Lausunnoissa pidetään aikataulua haasteellisena, mutta mahdollisena.

## **2.2 Tunnistamisen valinnaisten attribuuttien valmiusaikataulu**

### **2.2.1 Muutosehdotus**

Valinnaiset attribuutit ovat EU-säätelyn mukainen rajattu valikoima lisätietoja, jotka eivät ole pakollisia jokaisessa tunnistustapahtumassa. Määräyksen 72/2016 M mukaan niiden välittämiseen on oltava valmius ja ne on määritelty Viestintäviraston rajapintasuosituksissa 212/2018 S (SAML) ja 213/2018 S (OIDC).

Valinnaisten attribuuttien tarkoitus on tukea tunnistusta ja asiointia niissä tilanteissa, joissa pakolliset attribuutit eivät ole riittäviä. Tunnistusta pyytävän asiointipalvelun statuksen kertova attribuutti (julkinen vai yksityinen palvelu) on tarpeellinen ainakin rajat ylittävässä tunnistamisessa. Viestintävirasto on pyrkinyt selvittämään lausuntokierroksella valinnaisten attribuuttien tarvetta ja rajat ylittävän tunnistamisen näkymiä kansallisessa solmupisteessä ja tunnistuspalveluissa.

Määräysmuutoksessa Viestintävirasto on harkinnut ensisijaisesti lyhyttä siirtymäajan jatkamista valinnaisten attribuuttien valmiuden määrittelylle rajapinnoissa. Nykyinen siirtymäaika määräyksessä 72/2016 M on 18.9.2018, jota on harkittu yhdenmukaistettavaksi määräyksessä 72A/2018 M Tupas-toteutusten siirtymäajan 1.10.2018 kanssa.

Lisäksi Viestintävirasto on harkinnut sitä, että määrittelyvaatimus ei koskisi tunnistuspalveluita, jotka tarjoavat ainoastaan tunnistusvälinettä käyttäjille ja ainoastaan omien tunnistusvälineidensä käyttäjien tunnistusta asiointipalveluille.

Toissijaisesti Viestintävirasto on harkinnut valinnaisten attribuuttien määrittelyvaatimuksen poistamista määräyksestä ja muuttamista suositukseksi.

### **2.2.2 Lausunnot**

Ehdotettua määräaika 1.10.2018 ei kommentoitu lausunnoissa suoraan. Osa lausujista totesi, että valinnaisten attribuuttien määrittely rajapintaan Viestintäviraston rajapintasuositusten mukaisesti ei ole ongelma (Nordea, Nets, Ålandsbanken). Osa lausujista piti sitä vaikeana (Danske) tai tarpeettomana (OP Ryhmä).

Lausunnoissa kannatettiin valinnaisten attribuuttien käyttöönoton edistämistä ehdotetulla tavalla vaiheittain (Väestörekisterikeskus, OP Ryhmä toissijaisena vaihtoehtona koko vaatimuksesta luopumiselle). Yhdessä lausunnossa todettiin, että perusteluluonnos selventää sitä, mitä valmius konkreettisesti teknisesti tarkoittaa (OP Ryhmä). Lausunnoissa todettiin, että valinnaisten attribuuttien käyttöönotosta tullaan tarvitsemaan soveltamisohjeita (Danske) tai keskustelua luottamusverkoston työryhmissä (Nets).

Lausunnoissa ei voittopuolisesti kannatettu määrittelyvaatimuksen rajaamista vain osaan toimijoista (Nordea, OP), koska standardinmukainen ratkaisu mahdollistaa niiden käsittelemättä jättämisen (Nordea) ja koska tämä edellyttäisi tunnistevälinekohtaisia lisämäärittelyjä tunnistusvälityspalveluissa (OP Ryhmä). Toisaalta nähtiin, että tunnistusvälityspalveluiden valmius voisi riittää asiointipalveluiden tarpeiden täyttämiseksi (Nets).

Valinnaisten attribuuttien määrittelyn tarpeellisuudesta yleisesti esitettiin vastakkaisia näkemyksiä. Varautuminen eIDAS-asetuksen mukaiseen toimintaan nähtiin perustelluksi ja tarkoituksenmukaiseksi (Väestörekisterikeskus) tai tarpeettomaksi ja kustannuksia aiheuttavaksi (OP Ryhmä). Vaatimukset nähtiin tarpeelliseksi säilyttää määräyksessä, jotta asiaa edistetään tehokkaasti (Kilpailu- ja kuluttajavirasto), kun taas yhdessä lausunnossa kannatettiin vaatimusten muuttamista suositukseksi (OP Ryhmä).

Useimmat asiaan kantaa ottaneet lausijat eivät pitäneet julkisen/yksityinen attribuuttia tarpeellisena kansallisesti tässä vaiheessa (Finanssiala, Danske, Nordea, OP Ryhmä). Kuitenkin yksi lausuja piti attribuuttia tarpeellisena (Ålandsbanken) ja yksi lausuja piti tarpeellisena suoraa kontaktia tunnistusvälineen tarjoajan ja suomi.fi:n välillä häiriöiden ja petosten selvittämisessä, mikä puhuisi erottamisen tarpeellisuuden puolesta (Nordea). Toisaalta kannatettiin valmistautumista rajat ylittävään tunnistamiseen tältäkin osin (Väestörekisterikeskus).

Vaikka valinnaisia attribuutteja ei pidetty tässä vaiheessa tarpeellisena, rajat ylittävän tunnistamisen tarpeita ja kysyntää sekä luonnollisten etteijä- ja oikeushenkilöiden tunnistamiselle pidettiin kuitenkin liiketoiminnassa olennaisina (Danske, Nordea, OP Ryhmä, Nets, Signom). Lausunnoissa tuotiin esille toiveita kansallisen solmupisteen palveluille yksityiselle sektorille (OP Ryhmä, Signom).

Väestörekisterikeskus lausui pyynnöstä kansallisen solmupisteen suunnitelmista. Solmupisteessä keskitytään ensi vaiheessa tunnistamiseen julkishallinnon asiointipalveluihin ja vasta seuraavassa vaiheessa arvioidaan yksityiskohtaisemmin mahdollisuudet toteuttaa tunnistaminen yksityisiin asiointipalveluihin. Väestörekisterikeskus pyytää lausunnossaan selventämään määräyksen perusteluissa, onko määräyksen tarkoitus käsitellä solmupisteitä, joita yksityinen sektori voisi perustaa.

### 2.2.3 Viestintäviraston päätelmät ja linjaukset

#### **Määräyksessä säilytetään vaatimus valmiudesta valinnaisiin attribuutteihin.**

Viestintävirasto arvioi lausuntojen perusteella, että tunnistuspalvelut pystyvät huomioimaan valinnaiset tietokentät ilman kohtuutonta vaivaa. Viestintävirasto arvioi, että koska rajapintojen muuttaminen on yleisesti ottaen

osoittautunut hitaaksi, on perusteltua nostaa luottamusverkoston valmiustasoa valinnaisten attribuuttien käsittelyyn käynnistämällä niiden toteutuksen suunnittelu.

**Suunnittelu on tehtävä viimeistään 1.10.2018 samalla aikataululla kuin uusi rajapinta määritellään. Virasto tarkentaa perusteluja siten, että niistä käy paremmin ilmi, mitä valmiudella teknisesti tarkoitetaan.**

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 tunnistus-sanomiin sisältyvät valinnaiset attribuutit haittaa tunnistustapahtumia silloinkaan, kun niiden käytöstä ei ole sovittu.

Valvontaa varten suunnitelma täytyy käytännössä dokumentoida.

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 siis 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 mahdollisuuksilla malleilla.

Lisäksi Viestintävirasto toteaa, että kansallinen solmupiste välittää tunnistetiedot lähtökohtaisesti sellaisena kuin vastaanottaa ne toisesta valtiosta.

**Lausuntojen perusteella ei ole syytä velvoittaa käsittelemään julkisen/yksityinen-attribuuttia kansallisessa tunnistamisessa eri tavalla kuin muita valinnaisia attribuutteja tai vaatia sitä toteutettavaksi nopeammassa aikataulussa.**

## **2.3 Määräyksen TLS-vaatimuksen noudattamisen valvonnassa määriteltävä korjausaikataulu**

### **2.3.1 Valvottava velvoite**

Viestintävirasto on selvittänyt määräysmuutoksen yhteydessä myös vahvan sähköisen tunnistamisen valvonta-asiassa asetettavaa määräaikaa korjaukselle.

Osa vahvan sähköisen tunnistuksen tarjoajista ei täytä voimassa olevaa vaatimusta siitä, että tunnistuksessa on käytettävä tietoliikenteen salauksessa vähintään TLS-protokollan versiota TLS 1.1. Viestintävirasto harkitsee asettavansa korjaukselle määräajaksi 1.1.2019, jonka jälkeen käy-

tään tarvittaessa velvoitteen tehostamiseksi lain mukaisia hallinnollisia seuraamuksia.

Korjaus vaikuttaa käyttäjiin siten, että tunnistuspalvelut eivät enää toimi sellaisilla selaimilla ja päätelaitteilla, jotka tukevat vain vanhaa TLS 1.0-protokollaa. Monet tunnistuspalvelut ovat sulkeneet TLS 1.0-protokollan vaatimusten mukaisesti ja tiedottaneet asiasta asiakkailleen.

Viestintävirasto on valmistautunut viestimään asiasta.

### 2.3.2 Lausunnot

Lausunnoissa toivottiin, että Viestintävirasto viestii asiasta, koska korjaus vaikuttaa käyttäjiin (Finanssiala, Danske, Nordea, OP Ryhmä). Yhdessä lausunnossa ehdotettiin TLS-vaatimuksen korostamista määräyksessä esimerkiksi omana pykälänä, jotta vaatimus ei sekaannu Tupas-toteutusten siirtymäaikaan sisältyviin vaatimuksiin (Väestörekisterikeskus).

Lausunnon antoi myös yksi niistä toimijoista, jotka ovat jo toteuttaneet muutoksen vaatimuksen mukaisesti ja tiedottaneet asiasta asiakkailleen (Ålandsbanken).

### 2.3.3 Viestintäviraston päätelmät ja linjaukset

Viestintävirasto valmistelee valvontatoimenpiteenä korjausvelvoitteet niille tunnistuspalveluiden tarjoajille, jotka eivät vielä noudata TLS-vähimmäisvaatimusta. Korjaukset tullaan vaatimaan tehtäväksi viimeistään 1.1.2019.

Viestintävirasto viestii asiasta yleisölle.

## LIITE Lausuntojen kysymyskohtainen tarkastelu

## LIITE: Lausuntojen kysymyskohtainen tarkastelu

### 1 Tupas-toteutusten muuttamisen siirtymäaika (25 § 3 mom.)

#### Lausuntopyynnön kysymys 1

**Valmistelussa saatujen tietojen perusteella pankit korvaavat TUPAS-protokollaan perustuvat tunnistuspalvelut asiointipalveluille SAML- tai OIDC -protokollaan perustuvalla palvelulla. Onko päätelmä oikea? Aikooko joku tunnistuspalvelun tarjoaja säilyttää TUPAS-toteutuksen ja lisätä siihen vaaditun salauksen?**

#### Lausunnot

##### Finanssiala ry

FA päätti jo marraskuussa 2016 olla keskitetysti päivittämättä TUPAS-protokollaa vastaamaan määräyksen M72/2016 tuomia vaatimuksia. FA:n käsitys on, että TUPAS-protokollaan ei tulla jonkun tunnistuspalvelun tarjoajan toimesta lisäämään vaadittua salausta.

**Danske:** Pankki ei tule kehittämään nykyistä TUPAS-toteutusta vastaamaan uusia vaatimuksia. Pankki korvaa nykyisen toteutuksen viestintäviraston suositusten mukaisesti.

**Nordea:** Nordea aikoo ottaa käyttöön OIDC protokollan.

##### OP Ryhmä

OP Ryhmä ei tule säilyttämään TUPAS-toteutusta.

**Nets:** Nets tarjoaa asiointipalveluille SAML ja OIDC rajapintaa. Nets toimii tunnistusvälineen tarjoajien suuntaan kulloinkin voimassa olevien protokollien ja säännösten mukaan.

##### Ålandsbanken

Det är rätt slutsats. Banken kommer att ersätta identifieringstjänster som bygger på TUPAS-protokollet med en tjänst som bygger på OIDC-protokollet enligt Kommunikationsverkets rekommendation 213/2018 S (OIDC) om förtroendenätets gränssnitt:

[https://www.viestintavirasto.fi/attachments/suosituksset/ftn\\_oidc\\_profile\\_v1.0\\_ficora\\_rec\\_213\\_2018\\_s.pdf](https://www.viestintavirasto.fi/attachments/suosituksset/ftn_oidc_profile_v1.0_ficora_rec_213_2018_s.pdf)

Banken kommer inte att bevara och förse TUPAS-protokollet med fordrad kryptering.

#### Viestintäviraston päätelmät

**Vahvan sähköisen tunnistamisen ohjauksessa ja luottamusverkostoyhteistyössä ei ole enää tarvetta selvittää Tupas-protokollan yhteensopivuuskysymyksiä.**

Lausuntojen ja määräysvalmistelun kuulemistilaisuuksien perusteella Viestintävirasto arvioi, että tunnistuspalvelun ja asiointipalvelun välisessä rajapinnassa ollaan korvaamassa Tupas-rajapinta muihin protokolliin perustu-



villa rajapinnoilla ja että tyypillisesti otetaan käyttöön SAML- ja/tai OpenID Connect (OIDC) -protokollaan perustuva rajapinta.

Viestintävirasto ei ole laatinut suositusprofiilia asiointipalvelurajapinnalle. Viestintäviraston suositusten 212/2018 S (SAML) ja 213/2018 S (OIDC) mukaisia määrittelyjä tunnistusvälineen ja tunnistusvälityspalvelun tarjoajien väliselle rajapinnalle voi kuitenkin hyödyntää myös asiointipalvelurajapinnassa.

## **Lausuntopyynnön kysymys 2**

**Miten aikataulu ja sen vaiheistaminen vaikuttaa tunnistusvälineen tarjoajiin? Kuinka pitkällä uusien SAML- ja OIDC-rajapintojen suunnittelu ja määrittely on (ehdotettu määräaika 1.10.2018) ja miten tämä vaikuttaa tarjolle saattamisen aikatauluun (ehdotettu määräaika 1.1.2019)?**

### **Lausunnot**

**Danske:** Alkuperäinen käsityksemme on ollut, että tarjolle saattamisen aikataulu olisi ollut Q1/2019 eli maaliskuun 2019 loppuun mennessä. Pankilla on ns. rauhoitusaika vuoden vaihteessa, jolloin uusia tuotantoon ottoja ei tehdä. Ehdotuksemme on, että tarjolle saattamisen aikataulu olisi maaliskuun 2019 loppuun mennessä.

**Nordea:** Ehdotettu määräaikamuutos luonnokseen nähden, eli Q1/2019 muutettaisiin muotoon 1.1.2019 ei ole Nordean kannalta hyväksyttävä.

Nordea noudattaa tuotekehityksessään ns. Lean toimintamallia, jossa tuotekehitys jaksetaan vuodessa useaan 3-4kk mittaiseen PI (product increment) jaksoon. Q1/2019 aikana meidän ainut PI syklin päätös nykytiedon valossa on 19.3.2019 eli tuohon mennessä esim. viedään ko. PI:n aikana kehitetyt muutokset tuotantoon.

Toiveemme on, että tämän määräajan suhteen noudatettaisiin samaa normaalia globaalia käytäntöä eli että Q1 tarkoittaa käytännössä ko. kvartaalin viimeistä, ei ensimmäistä päivää. Käytännössä siis veisimme muutokset tuotantoon kuitenkin viimeistään 19.3.2019 mennessä.

Joulu-tammikuu on finanssisektorin IT toiminnassa yleisesti rauhoitusaikaa, jolloin tuotantoon ei tehdä muutoksia, muuta kuin äärimmäisissä poikkeustapauksissa.



## Finanssiala ry

Tarjolle saattamisen (rajapinta toteutuksen) määräaika oli toisen kuulemiseen mennessä muuttunut muodosta 'Q1/2019 aikana', muotoon '1.1.2019 mennessä.' Muissa määräajoissa ehdotetaan kvarttereiden viimeistää päivää.

FA toi toisessa kuulemistilaisuudessa esille 1.1. päivämäärän ongelmallisuuden. 1.12.-31.1. (joka vuosi) on yleisesti käytössä oleva IT-tuotannon oton rauhoitusaika. Tänä aikana tehdään tuotantoon vain kriittisiä korjauksia yms. Pankeissa tämä rauhoitusaika perustuu mm. maksuliikenteen 100% varmistamiseen. Halutaan esim. turvata joulumyynnin ja alennusmyynnin saumaton rahaliikenne. Tämä ilmiö ei koske vain Suomea, vaan on käytössä myös muissa maissa sekä myös muilla aloilla.

On myös hyvä muistaa, että SAML- ja OIDC-rajapintojen julkaisu myöhästivät vähintään 8 kk (kun lasketaan päivämäärästä 1.5.2017). Itse toteutukseen voisi siis ehdotuksen mukaan tulla vain noin 2 kk lisäaika alkuperäisestä aikataulusta.

Ja pahimmassa tapauksessa, ottaen taas huomioon rauhoitusajan, itse rajapinta toteutukseen voisi jäädä vain 2 kk aikaa (1.10.-30.11.2018). Todella lyhyt aika.

FA ehdottaa, että tarjolle saattamisen määräaika olisi **vähintään 28.2.2019**. Tämäkin määräaika saattaa aiheuttaa tuotannon oton osalta erikoisjärjestelyjä, eli

31.3.2019 määräaika voisi olla optimaalisin ja turvallisin vaihtoehto. Tämä määräaika oli myös se alun perin oletettu määräaika.

## OP Ryhmä

Kannatamme esityksessä ehdotettua aikataulua.

OPn palvelukuvaukset ja SAML rajapintamäärittelyt ovat jo olemassa, samoin kuin testiympäristö. Toteutus on nykyisten määräysten mukaisesti lähes valmis, lukuun ottamatta tukea vapaaehtoisille attribuuteille.

**Nets:** *Nets voi tarjota tunnistusvälityspalvelua myös tunnistusvälineen tarjoajien avuksi. Netsin palveluvalikoimaan kuuluu myös tunnistusvälineen tarjoajalle annettava välityspalvelun toteuttaminen palveluna.*

## Ålandsbanken

Planering och specificering är ur bankens systemleverantörs perspektiv är nästan klar eftersom den bygger Kommunikationsverkets OICD gränssnittsrekommendation. Tidtabellen är dock snävt satt och det kommer krävas högt tempo för att lyckas.

## Väestörekisterikeskus

Väestörekisterikeskus on aikaisemmin todennut, että yksinomaan Tupas-toteutuksiin kohdistuva siirtymäaika ei ole tasapuolinen kaikkien tunnistusvälineen tarjoajien näkökulmasta eikä pitkä siirtymäaika ole myöskään toivottava tietoturvallisuuden näkökulmasta. Mikäli määräykseen nyt kirjataan esitetyn mukainen Tupakseen liittyvä siirtymäajan jatkokausi, niin VRK:n näkemyksen mukaan jatkettun siirtymäajan pitäisi olla riittävä jo aikaisemmin edellytettyjen toimenpiteiden toteuttamiseksi ja Tupakseen liittyvien vaatimusten täyttämiseksi (esityksessä mainittujen suunnittelun/tarvittavien määrittelyjen laadinnan määräajan 1.10.2018, uuden palvelun tuotantoon viemisen/rajapinnan tarjolle tuomisen määräajan 1.1.2019 ja vanhan palvelun lopettamisen määräajan 1.10.2019 mukaisesti).

## Finanssivalvonta

Finanssivalvonta kannattaa lähtökohtaisesti ehdotettua muutosaikataulua. Toimiala on esittänyt määräystä koskevassa kuulemistilaisuudessa, että määräajan asettaminen vuodenvaihteeseen tarkoittaa käytännössä sitä, että rajapinnat täytyisi saada tuotantoon jo joulukuussa, koska vuodenvaihteessa on IT-muutoksissa tyypillisesti tauko. Toimialan mukaan tauko voi olla jopa 2 kk 1.12.–31.1. Finanssivalvonnan kokemuksen mukaan on pankkikohtaisesti vaihtelevaa, milloin muutoksia ei tehdä.

## Viestintäviraston päätelmät

OP Ryhmän ja Netsin lausunnot tukevat sitä Viestintäviraston käsitystä, että vaatimukset täyttävä rajapinta on ollut mahdollista suunnitella tuotantovalmiiksi olemassa olevilla tiedoilla jopa alun perin määrättyssä aikataulusa.

Lausunnoissa tuodaan perustellusti esille, että ehdotettu määräaika uusien rajapintojen tarjolle saattamiselle 1.1.2019 keskellä IT-toimintojen rauhoitusaikaa on ajankohtana hankala.

Väestörekisterikeskuksen lausunnossa muistutetaan, että vain Tupas-toteutuksiin liittyvä siirtymäaika ei ole tasapuolinen toimijoille ja että pitkä siirtymäaika on epätoivottava tietoturvallisuuden kannalta.

### **Määrittelyn määräajaksi määrätään 1.10.2018 ja tarjolle saattamisen määräajaksi 1.3.2019.**

Viestintävirasto olettaa, että muutkin toimijat kuin OP Ryhmä ja Ålandsbanken ovat kysyneet valmistelevaan määrittelyä. Virasto katsoo, että myös tuotantoon viemisen suunnittelu olisi mahdollista aloittaa ennen teknisten määrittelyjen valmistumiselle ehdotettua takarajaa 1.10.2018 ja tuotantoon viemiselle käytössä oleva aika olisi siten käytännössä pidempi kuin lausunnoissa todettu 2 kuukautta (1.10.–30.11.2018 määrittelyjen määräajasta rauhoitusajan alkamiseen).

Viestintävirasto joutuu kuitenkin toteamaan, että OP Ryhmä ja Ålandsbanken lukuun ottamatta lausunnoissa ei vastata kysymykseen, kuinka pitkällä uusien SAML- ja OIDC-rajapintojen suunnittelu ja määrittely on tällä hetkellä. Lausuntojen perusteella tuotantoon viemiselle jäisi lyhyt aika ja se osuisi vuodenvaihteen maksuliikenteen ruuhka-ajan alkuun.

Näillä perusteilla Viestintävirasto katsoo, että osalla pankeista kyky tarjota luotettavasti uudet asiointipalvelurajapinnat 1.1.2019 on siinä määrin epävarma, että tarjolle saattamisen takaraja on turvallisempaa määrätä pidemmälle. Määräajan asettaminen päivämäärään 1.3.2019 mahdollistaa muutosten toteuttamisen vuodenvaihteen rauhoitusjakson jälkeen.

Viestintävirasto suosittelee, että ne pankit, jotka kykenevät toteutukseen aikaisemmin, tuovat rajapinnat tarjolle ennen viimeistä määräaikaa.

### **Lausuntopyynnön kysymys 3**

**Miten aikataulu ja sen vaiheistaminen vaikuttaa tunnistusvälityspalveluihin? Onko välityspalveluilla jo valmius tarjota tunnistuspalveluita asiointipalveluille vaatimukset täyttävillä SAML- ja OIDC-rajapinnoilla?**

#### **Lausunnot**

**Danske:** Pankin osalta tämä liittyy käsityksemme mukaan rooliimme sekä tunnistusvälineen tarjoajana että tunnistusvälityspalvelun tarjoajana. Aikataulullisesti nämä asiat ovat kytketty toisiinsa, joten viittaamme edellisen kohdan vastaukseemme.

#### **OP Ryhmä**

Kuten edellisessä kohdassa on jo todettu, OP:n ratkaisut ovat näillä aikatauluilla valmiita, joten OP:lla on valmius tarjota tunnistuspalveluita asiointipalveluille vaatimukset täyttävällä SAML-rajapinnalla.

OP pitää aikataulun vaiheistamista lähtökohtaisesti kannatettavana.

**Nets:** Kyllä. Netsillä on ollut tekninen valmius tarjota tunnistusvälityspalveluita 1.5.2017 lähtien.

#### **Ålandsbanken**

Identifiering via OIDC-gränssnitt planeras finnas tillgängligt till senast 1.1.2019.

### **Viestintäviraston päätelmät**

Lausunnoissa ei tullut esille tunnistusvälityspalveluihin vaikuttavia seikkoja, jotka olisi erityisesti huomioitava siirtymäaikataulun vaiheistamisessa.

Edellisen kysymyksen kohdalla todettiin Viestintäviraston käsitys, että vaatimukset täyttävä rajapinta on ollut mahdollista suunnitella tuotantovalmiiksi olemassa olevilla tiedoilla jopa alun perin määrättyssä aikataulussa. Tätä käsitystä tukee se, että ainakin Nets on kyennyt tuomaan tarjolle vaatimukset täyttävän rajapinnan jo 1.5.2017.

### **Lausuntopyynnön kysymys 4**

**Miten näette aikataulun vaikutukset asiointipalveluihin? On hyvä ottaa huomioon, että asiointipalvelut voivat muutostilanteessa myös selvittää mahdollisuutta hankkia tunnistuspalveluita kootusti tunnistusvälityspalveluilta.**

#### **Lausunnot**

## Finanssiala ry

FA:n näkemys on, että ehdotettu 1.10.2019 määräaika (kaikkien muutosten takaraja) sitoo käytännössä myös asiointipalveluita. Ei voi yksinomaan olla tunnistusvälityspalveluiden (kuten pankkien) vastuulla saada muutokset tehtyä. Asiointipalveluilla on myös vastuu tehdä muutoksia omissa tietojärjestelmissään.

**Danske:** *Käsityksemme mukaan asiointipalveluiden on tehtävä tarvittavia muutoksia omiin järjestelmiinsä huolimatta siitä, että tunnistuspalvelut hankitaan tunnistusvälityspalveluilta. Mikäli asiointipalveluiden toimintaympäristö on monimutkainen saattaa aikataulu olla heille haasteellinen. On myös syytä huomioida, että muutos ei ole pelkästään tekninen vaan siihen liittyy myös uuden palveluntarjoajan hankintaprosessi sopimusneuvotteluineen.*

**Nordea:** *Nordea julkistaa uuden protokollan kuvaukset sekä integraatiota helpottavan testiportaalin q3/2018 aikana sekä tiedotamme tuolloin asiakkaita tulevista muutoksista. Yksi vuosi tulisi olla asiointipalveluille riittävän pitkä aika sisäistää ja aikatauluttaa tarvittavat muutokset emmekä näe, että uuden protokollan vieminen tuotantoon alkuperäisen ehdotuksen eli 31.3.2019 mukaisesti vaikuttaa tähän.*

## OP Ryhmä

OPn käsityksen mukaan aikataulu on mahdollinen, joskin erittäin haastava asiointipalveluille. Asiointipalveluilla voi olla hyvinkin erilaisia haasteita omien palveluidensa järjestämisessä, joka vaatii aikaa (kilpailutuksen järjestäminen, vanhojen järjestelmien uusiminen, osaamattomuus, taloudelliset haasteet ym.). Ehdotettu aikataulu antaa jonkin verran sopeutumisaikaa asiointipalveluille. OP toivoo, että Viestintävirasto selvittäisi asiointipalveluiden tilannetta uusien tunnistusrajapintojen käyttöönotossa ennen määräajan päättymistä ja arvioisi mahdolliset lisätoimiensa tarpeet vielä tässä vaiheessa.

**Nets:** *Kts. kohta 1 ja 3. Nets ei ole kohdannut asiointipalveluita, jotka olisivat halunneet palvelun TUPAS rajapinnalla. OIDC mahdollistaa asiointipalveluille helpon ja joustavan tunnistamisen vahvoilla ja heikoilla tunnistteilla.*



## Väestörekisterikeskus

VRK:n tulee tunnistusvälityspalvelua luottamusverkostosta kilpailuttaessaan (kevät-kesä 2018) Suomi.fi-tunnistusta varten huomioida em. Tupaksen siirtymäajat, niiden vaikutukset käytännön toteutuksissa ja mahdolliset viivästykset hankintasopimuksessa omina erityisinä ehtoinaan.

Käytännössä nykyisin toimialueella haasteena on esimerkiksi omien varmenteiden käyttö allekirjoituksissa, SHA-1 käyttö ym. vanhentuneet ratkaisut, eikä pitkä siirtymäaika anna palveluiden tilaajille luotamusta ja varmuutta tietoturvan parantamiseen.

Tunnistamisen välityspalveluita hankkivan organisaation näkökulmasta määräyksessä (tai sitä täydentävässä materiaalissa) voitaisiin selkeämmin ilmaista, kenellä on oikeus ja velvollisuus arvioida tunnistamisen palveluita myyvien tahojen, palveluiden ja teknisten ratkaisujen tietoturvaa, sekä toisaalta mille tahoille tunnistajat ja välityspalvelut ovat niistä velvollisia raportoimaan ja missä laajuudessa. Käytännössä nykyisin tilaava taho ei voi olla varma, onko heillä aihetta ja oikeutta pyytää toimittajalta selvityksiä tietoturvan toteuttamisesta, auditoinneista ja käytetyistä kehyksistä, vai missä laajuudessa asia on jo hyväksytyllä tasolla ja asianmukaisesti toteutettuna Viestintävirastolle tehtyjen selvitysten ja hyväksynnän myötä.

## Viestintäviraston päätelmät

**Viestintävirasto katsoo, että tunnistuspalvelun ja asiointipalvelun välisen rajapinnan muuttaminen vaatimustenmukaiseksi voidaan määrätä tehtäväksi viimeistään 1.10.2019.**

Lausunnoissa pidetään aikataulua haasteellisena, mutta mahdollisena. Muutos pidentää vaatimusten alun perin määrättyä siirtymäaikaa (18.9.2018) vuodella.

Viestintävirasto katsoo, että asiointipalveluiden tietoisuuden lisääminen muutostarpeesta on ensisijaisesti tunnistuspalveluntarjoajien tehtävä, mutta Viestintävirasto tiedottaa asiasta käytettävissään olevilla keinoilla.

Väestörekisterikeskus on lausunnossaan tuonut esille siirtymäajan heijastusvaikutukset suomi.fi -kilpailutukseen. Viestintävirasto yhtyy näkemykseen, että siirtymäajat hankaloittavat hankintaa. Viestintävirasto katsoo kuitenkin siirtymäajan jatkamisen välttämättömäksi, jotta yksityisen sektorin asiointipalvelut ehtivät tehdä muutokset.

Väestörekisterikeskus tuo esille, että tunnistuspalveluita hankkiva organisaatio tarvitsee tietoa tunnistuspalvelun tietoturvallisuuden arvioinnista, luotettavuudesta ja valvonnasta. Viestintävirasto arvioi, ettei rekisteröinnin ja valvonnan kuvaus sovellu määräykseen, mutta virasto harkitsee sopivan tavan parantaa tietoisuutta rekisteröidyn tunnistusvälityspalveluiden luotettavuuden arvioinnista ja valvonnasta.

## Lausuntopyynnön kysymys 5

**Mitä muuta haluatte tuoda esille siirtymäajan vaikutuksista?**

**Lausunnot**

**Danske:** Merkittävin huolestus kohdistuu siihen, miten asiointipalvelut pystyvät annetussa aikatauluissa implementoimaan tarvittavat muutokset, valitsemaan uuden/t palveluntarjoajat, tekemään tarvittavat uudet sopimukset sekä ohjeistamaan asiakkansa.

**Nordea:** Toimijoiden tasapuolisen kohtelun nimissä ~8kk viivästys uusien protokollakuvausten julkaisun suhteen ei saa johtaa siihen, että niiden implementointiin saataisiin käytännössä vain 2-3 kuukautta lisäaikaa.

**Nets:** Siirtymäajalla ja sen pituudella ei ole vaikutusta Netsin tarjoamiin palveluihin.

## Viestintäviraston päätelmät

Asiointipalveluiden muutosaikataulua käsitellään edellä kysymyksen 4 kohdalla. Asiointipalveluiden asema on ollut valmistelussa tärkeä harkintaperuste.

Viestintävirasto ei tunnista, mistä asiasta asiointipalvelun pitää ohjeistaa omia käyttäjiään, kun asiointipalvelun ja tunnistuspalvelun väliseen rajapintaan lisätään sanomatason salaus. TLS 1.0-tuen poistamisen viestintää käsitellään kysymyksen 12 kohdalla.

Tasapuolisen kohtelun osalta Viestintävirasto viittaa edellisiin kohtiin: osa toimijoista on kyennyt tuottamaan rajapinnat samoilla tiedoilla ja koko Tupas-toteutuksia koskevan siirtymäajan jatkaminen on epätasapuolista niitä toimijoita kohtaan, jotka eivät käytä Tupasta, vaan ovat toteuttaneet tietoturvallisuusvaatimukset muuhun protokollaan perustuvilla toteutuksilla.

## 2 Tunnistamisen valinnaisten attribuuttien valmiusaikataulu (12 § 2 mom. ja 25 §:n 4 mom.)

### Lausuntopyynnön kysymys 6

**Näettekö tunnistusvälityksen ehtoihin (kuten häiriötiedon vaihtoon, tietosuojaan tai hinnoitteluun) liittyvää tarvetta kansallisessa tunnistamisessa tiedolle siitä, onko tunnistusta pyytänyt yksityinen vai julkinen asiointipalvelu?**

### Lausunnot

#### **Finanssiala:**

FA:n näkemys on, että markkinalla ei ole tapahtunut sellaisia konkreettisia muutoksia marraskuusta 2016, että tätä kyseistä valinnaista attribuuttia pitäisi nyt ottaa käyttöön. Mikä olisi se tämän päiväinen konkreettinen tarve tälle valinnaiselle attribuutille?

**Danske:** Emme näe tarvetta edellä mainitun tiedolle.

**Nordea:** Parametrin käyttöönotto ei Nordean mielestä ole oikea tapa korjata ongelmaa, joka johtuu siitä, että Suomi.fi palvelu on lain voimalla keinoitekoisesti määrätty asiointipalveluksi, vaikka todellisuudessa on välityspalvelu.

*Luottamusverkosto toimisi paremmin, mikäli Suomi.fi tuotaisiin samalle tasolle muiden välityspalveluiden kanssa. Tämä vaihtoehto olisi parempi ratkaisu koska:*

- 1) se mahdollistaisi paremmat suorat neuvottelusuhteet kaikkien tunnistusvälineen tarjoajien ja VRK kesken*
- 2) olisi kaikin puolin kustannustehokkaampi ratkaisu, koska välikädet puuttuisivat*
- 3) estäisi sen, ettei suomi.fi sopimuksen voittava välityspalvelu saa ei toivottua kilpailuetua muihin välityspalveluihin nähden. Suomi.fi sopimus kattaa >2/3 koko Suomen tunnistusvolummeista eikä käytännössä voi mitenkään olla vaikuttamatta välityspalveluiden väliseen kilpailuasetelmaan.*
- 4) Selkeyttäisi markkinan rakennetta ja rooleja.*
- 5) Loppukäyttäjät näkisivät yhdenmukaisesti tiedon, että ovat kirjautumassa juuri Suomi.fi palveluun.*
- 6) Häiriö & petosselvittely voidaan tehdä suoraan ilman välikäsiä.*

### **OP Ryhmä**

OPn näkemyksen mukaan tällä hetkellä Tunnistusvälineen tarjoajalla ei ole tarvetta tiedolle siitä, onko tunnistusta pyytänyt yksityinen vai julkinen taho. Tieto säilyy välityspalvelulla, jolta Tunnistusvälineen tarjoaja saa tiedon yksittäisen tapahtuman osalta tarvittaessa. Myöskään kilpailulainsäädäntö ei tue hinnoittelumallia, jossa hinta vaihtelisi sen mukaan, onko kyseessä yksityinen vai julkinen asiointipalvelu. Tiedon lisääminen vaatisi merkittävää muutosta tekniseen toteutukseen. Asian tarpeellisuutta ja toteuttamiskelpoisuutta voidaan tarvittaessa tarkastella uudelleen siinä vaiheessa, kun perusraja-annat on saatu valmiiksi ja todellinen käyttötapaus konkretisoituu.

**Nets:** *Markkinarakenteet eivät saisi vääristää kilpailua.*

### **Ålandsbanken**

*Ja.*

### **Väestörekisterikeskus**

Varautuminen eIDAS-asetuksen mukaiseen toimintaan on peruste tuoda esiin kyvykkyys välittää optionaalaisia henkilöön liittyviä attribuutteja tarvittaessa, kuten myös tieto siitä, pyytääkö tunnistamista yksityisen vai julkisen sektorin taho. Tämä private / public -tieto on välttämätön solmupisteiden välisissä sanomissa ja siten tarkoituksenmukainen myös kansallisesti.

### **Viestintäviraston päätelmät**

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



Lausunnoissa katsotaan yhtä lausujaa lukuun ottamatta, ettei kansallisessa tunnistamisessa ole tarvetta erotella sitä, tunnistetaanko käyttäjä julkiseen palveluun (suomi.fi:hin) vai yksityisen sektorin asiointipalveluun. Toisaalta Nordean lausunnossa tuodaan esille häiriö- ja petosselvittely, missä siis ilmeisesti asiointipalvelun statuksella voisi olla merkitystä.

#### Määräyksen ulkopuoliset asiat

Nordean lausunnosta suomi.fi -tunnistuksen asemasta luottamusverkoston ulkopuolella Viestintävirasto toteaa, että määräysmuutoksessa ei käsitellä lainsäädännön tasolla tehtyjä ratkaisuja tai suomi.fi:n kilpailutuksen markkinavaikutuksia.

### **Lausuntopyynnön kysymys 7**

**Viestintäviraston suosituksissa rajapintamäärittelyistä 212/2018 S (SAML) ja 213/2018 S (OIDC) on huomioitu valinnaiset attribuutit. Voidaanko valinnaiset attribuutit (tietokentät) lisätä rajapintamäärittelyihin suositusten mukaisesti? Onko valinnaisten attribuuttien tietokenttien käsittelyssä jotain teknisiä ongelmia sellaisissa tunnistustapahtumissa, joissa niitä ei tarvita?**

#### **Lausunnot**

**Danske:** *Valinnaisten attribuuttien käsittely aiheuttaa tietojärjestelmille lisämäärittelyjen tekemistä. Soveltamisohjeiden pitää olla yksikäsitteiset, jotta välttyään erilaisilta tulkinnoilta eri toimijoiden välillä.*

**Nordea:** *Meidän tapauksessa ymmärsimme, että tässä tarkoitetaan Id Tokenin optionaalisia kenttiä (OIDC 4.1.1.2 Optional attributes) emmekä näe näissä ongelmaa meidän teknisen toteutuksen kannalta.*

**Nets:** *Netsin näkemyksen mukaan valinnaiset attribuutit voidaan lisätä rajapintamäärittelyihin suositusten mukaisesti. Netsillä ei ole teknisiä ongelmia tämän suhteen. Asia vaatineee keskustelua luottamusverkoston työryhmissä, muun muassa miltä osin valinnaiset attribuutit ovat tunnistuslain ulkopuolella.*

#### **Ålandsbanken**

*Ikke-obligatoriska attribut kan fogas till gränssnittsspecifikationerna enligt rekommendationerna, vi ser inte några tekniska problem vid behandling av dem.*

## OP Ryhmä

OPn näkemyksen mukaan valinnaisia attribuutteja ei tulisi lisätä rajapintamäärittelyihin, vaan ne tulisi poistaa määräyksestä. Ylimääräisten attribuuttien lisääminen varmuuden vuoksi lisää kustannuksia. Rajapintaa tulisikin kehittää todellisten käytötapausten perusteella.

Viestintäviraston esitys valinnaisten attribuuttien kirjaamisesta suosituksiksi on OPn mielestä mahdollinen vaihtoehto. Tämä suositusmalli voisi pitää sisällään mahdollisuuden nostaa attribuutteja erikseen määriteltävällä siirtymäajalla rajapintamäärittelyihin silloin, kun suosituksissa oleville attribuuteille ilmenee todellinen käyttötarkoitus. Suosituksiin olisi myös mahdollista tuoda uusia attribuutteja, mikä lisäisi luottamusverkostossa läpinäkyvyyttä mahdollisiin tuleviin muutoksiin.

Mikäli valinnaiset attribuutit kuitenkin jäävät rajapintamäärittelyihin, perustelutekstin selvennös siitä, että valinnaisten attribuuttien osalta riittää määrittely, mutta niitä ei tarvitse viedä tuotantoon, selventää määräyksen vaatimusta varautumisesta. Tämä kuitenkin tarkoittaa, että valinnaiset attribuutit tulisi käytännössä toteuttaa ja vain tuotantoon vieminen jäisi tekemättä. Viestintäviraston perustelutekstissä todetaan, että Teknisissä konfiguroinneissa tulisi huomioida, etteivät valinnaiset attribuutit vaikuta tunnistustapahtumiin silloin, kun niiden käyttöönotosta ei ole sovittu. Tämän kirjauksen OP ymmärtää siten, että on riittävää, jos rajapintaa hyödyntävillä toimijoilla valinnaisen attribuutin välittyminen ei aiheuta virhetilannetta, mutta tietoa ei tarvitse muuten käsitellä. Tämä taso valinnaisten attribuuttien osalta, mikäli ne tulee määritellä ennen varmaa käytötapausta, on OPn mielestä kannatettava.

## Väestörekisterikeskus

VRK pitää esityksen mukaisesti perusteltuna valmistella ja siirtyä valinnaisten attribuuttien käyttöön asteittain, ja siinä vaiheessa, kun on olemassa tosiasiallinen valinnaisten attribuuttien käyttötarve.

Varautuminen eIDAS-asetuksen mukaiseen toimintaan on peruste tuoda esiin kyvykkyys välittää optionaalisia henkilöön liittyviä attribuutteja tarvittaessa, kuten myös tieto siitä, pyytääkö tunnistamista yksityisen vai julkisen sektorin taho. Tämä private / public -tieto on välttämätön solmupisteiden välisissä sanomissa ja siten tarkoituksenmukainen myös kansallisesti.

## Kilpailu- ja kuluttajavirasto

KKV:n näkemyksen mukaan valinnaisten attribuuttien määrittelyä ei pitäisi muuttaa vaatimuksesta suositukseksi, koska Viestintäviraston arvion mukaan suositus ei tehokkaasti edistä valinnaisten attribuuttien huomioimista. Perustelumuistion mukaan toimijat eivät ole ottaneet valinnaisia attribuutteja käyttöön, eikä vuonna 2016 määrätty siirtymäaika niiden määrittelylle ole toteutumassa.

## Viestintäviraston päätelmät

**Määräyksessä säilytetään vaatimus valmiudesta välittää valinnaisia attribuutteja.**

Viestintävirasto arvioi lausuntojen perusteella, että tunnistuspalvelut pystyvät huomioimaan valinnaiset tietokentät ilman kohtuutonta vaivaa. Viestintävirasto arvioi, että koska rajapintojen muuttaminen on yleisesti ottaen osoittautunut hitaaksi, on perusteltua nostaa luottamusverkoston valmiustasoa valinnaisten attribuuttien käsittelyyn käynnistämällä niiden toteutuksen suunnittelu.

**Suunnittelu on tehtävä viimeistään 1.10.2018 samalla aikataululla kuin uusi rajapinta määritellään. Virasto tarkentaa perusteluja siten, että niistä käy paremmin ilmi, mitä valmiudella teknisesti tarkoitetaan.**

Valmius välittää valinnaisia attribuutteja tarkoittaa, että valinnaisten attribuuttien käsittely täytyy suunnitella rajapinnassa ja tunnistusjärjestelmässä siten, että tunnistuspalvelun tarjoajalla on käsitys käyttöönnotossa tarvittavista teknisistä toimenpiteistä.

Teknistä toteutusta järjestelmiin ei vaadita valinnaisille attribuuteille. Teknisissä konfiguroinneissa tulee kuitenkin huomioida, etteivät tunnistus-sanomiin sisältyvät valinnaiset attribuutit haittaa tunnistustapahtumia silloinkaan, kun niiden käytöstä ei ole sovittu.

Valvontaa varten suunnitelma täytyy käytännössä dokumentoida.

OP Ryhmä katsoo lausunnossaan, että suosituksiin olisi mahdollista tuoda uusia attribuutteja, mikä lisäisi läpinäkyvyyttä luottamusverkostossa. Viestintävirasto toteaa, että luottamusverkoston yhteistyöryhmässä on mahdollista käsitellä uusia attribuuttitarpeita ja Viestintäviraston SAML- ja OIDC-rajapintasuosituksiin on mahdollista lisätä attribuutteja, jos niille havaitaan luottamusverkostossa objektiivisesti perusteltu tarve. Nyt suosituksissa on pitäydytty eIDAS-sääntelyn mukaisissa tietosisällöissä ilman kansallisia lisätietoja.

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

### **Lausuntopyynnön kysymys 8**

**Olisiko riittävää, että valmius valinnaisten attribuuttien välittämiseen koskisi vain tunnistusvälityspalveluita, jotka tarjoavat asiointipalveluille tunnistusta useammalla kuin yhdellä tunnistusvälineellä?**

### **Lausunnot**

**Danske:** *Viittaamme tässä vastauksemme edellisessä kohdassa.*

**Nordea:** *Emme tiedä miksi tällainen spesiaalivaatimus tarvittaisiin, kun speksissä on jo määriteltynä scope request parametri, jonka mukaisesti valinnaiset attribuutit joko lisätään tai jätetään pois.*

## OP Ryhmä

Tämä ei ole OP:n käsityksen mukaan suositeltava ratkaisu. Mielestämme solmupisteen velvollisuus olisi muuntaa ulkomaalaiset tunnisteet soveltuvaksi kansalliseen luottamusverkkoon.

Mikäli valinnaisten attribuuttien käsittely tapahtuisi vain välityspalvelussa, välityspalvelun pitäisi pystyä päättämään, mitä eri attribuutteja eri tunnistuspalvelut tukevat ja rakentamaan tunnistusvälinekohtainen käsittely. Tämä lisää välityspalveluiden kompleksisuutta merkittävästi eikä ole siten suositeltava ratkaisu ongelmaan.

**Nets:** *Netsin näkemyksen mukaan tämä voisi olla riittävää asiointipalveluiden tarpeiden täyttämiseksi.*

## Viestintäviraston päätelmät

**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 mahdollisilla malleilla.

Lisäksi Viestintävirasto toteaa, että kansallinen solmupiste välittää tunnistetiedot lähtökohtaisesti sellaisena kuin vastaanottaa ne toisesta valtiosta. Valinnaiset attribuutit tukevat henkilön yksilöintiä mm. niissä tilanteissa, joissa käyttäjän tunnistustiedot tulevat valtiosta, jossa ei ole käytössä yhtä henkilötunnuksen kaltaista yksilöivää tunnusta.

## Lausuntopyynnön kysymys 9

**Vastaavatko määräyksen 13 § perusteluihin MPS72A:ssa lisätyt arviot rajat ylittävästä tunnistamisesta VRK:n kansallisen solmupisteen suunnitelmia? Onko muita seikkoja, jotka vaikutusarvioinnissa olisi hyvä tuoda esille?**

## Lausunto, Väestörekisterikeskus

Esityksessä todetaan, että Suomen solmupisteessä pyritään teknisesti huomioimaan myös tunnistaminen yksityisiin asiointipalveluihin. VRK tuo esille, että solmupistetoteutuksessa keskitytään ensi vaiheessa tunnistamiseen julkishallinnon asiointipalveluihin ja sitä seuraavassa vaiheessa arvioidaan yksityiskohtaisemmin mahdollisuudet toteuttaa tunnistaminen yksityisiin asiointipalveluihin.

Esityksessä myös todetaan lähtökohtana olevan, että tunnistustapahtumat välitetään ulkomaille luottamusverkoston tunnistusvälityspalvelun kautta. VRK toteaa, että tunnistustapahtumat välitetään ulkomaille *julkisen sektorin asiointipalveluun* kansallisen solmupisteen kautta, sitä ennen tapahtumat välittyvät kansallisesti tunnistusvälityspalvelun kautta kansalliseen solmupisteeseen.

Mikäli määräyksessä halutaan ennakoiden ottaa kantaa skenaarioon, jossa on toteutettu erikseen yksityisen sektorin tarpeisiin erillinen eIDAS-solmupiste (lähinnä ns. connector ulkomaalaisten tunnistamista varten), skenaarion voisi tuoda esiin selkeämmin. Muuten asian tarkoituksenmukaisuus voi herättää hämmennystä, kun VRK toteuttaa kansallisen solmupisteen ja tunnistamisen julkisen sektorin tarpeisiin. Siitä huolimatta toteutuuko skenaario yksityisen sektorin solmupisteestä, vai lisätäänkö kansallisen solmupisteen piiriin mahdollisesti myöhemmin yksityisen sektorin palveluita, M72A voi osaltaan toimia ohjeena myös VRK:lle kansallisen solmupisteen ja sen rajapintojen ja integroinnin toteutukselle. VRK lisäksi tiedustele, että onko määräysluonnoksen solmupistettä koskevien kappaleiden tarkoitus ennakoiden ohjata mahdollisia yksityisen sektorin toimijoita rajat ylittävässä välitystoiminnassa, vai onko tarkoitus ohjata nimenomaan kansallisen solmupisteen ja Suomi.fi-tunnistuksen integraatiota. Jälkimmäinenkin vaihtoehto on VRK:n näkökulmasta mahdollinen. VRK esittää, että asiaa selkeytettäisiin määräyksessä palveluntarjoajille.

## Viestintäviraston päätelmät

**Viestintävirasto selkeyttää perusteluja siten, että määräyksessä on pitäydytty eIDAS-asetuksessa ja kansallisessa tunnistuslaissa säädetyn kansallisen solmupisteen kautta välitettävän tunnistuksen yhteentoimivuudessa.**

Väestörekisterikeskus esittää hyviä näkökohtia, joiden avulla perusteluja voi selventää.

Viestintävirasto toteaa, että määräyksen tarkoitus on edistää sekä kansallisen ja että rajat ylittävän tunnistuksen yhteentoimivuutta ja turvallisuutta. Rajat ylittävän tunnistuksen sääntelyssä määräyksessä pitäydytään eIDAS-asetuksessa ja kansallisessa tunnistuslaissa säädetyn kansallisen solmupisteen kautta välitettävässä tunnistuksessa.

Määräyksellä tai sen perusteluilla ei siis ole tarkoitus ohjata yksityisen sektorin toimintaa. Lausuntopyynnön yhteydessä laaditun perustelutekstin tarkoitus on neutraalisti kuvata ja selventää skenaarioita ennen kaikkea siltä kannalta, mitä attribuuttivaatimuksia olisi tarpeen määrätä yhteentoimivuuden takaamiseksi luottamusverkoston ja kansallisen solmupisteen välillä.

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 tunnis-



tamisen yhteentoimivuus- ja turvallisuusvaatimukset komission asetuksessa (EU) 2015/1501 koskevat vain kansallista solmupistettä.

Väestörekisterikeskuksen lausunto vahvistaa sen käsityksen, että tunnistustapahtumat välitetään myös rajat ylittävässä tunnistamisessa luottamusverkostosta solmupisteelle tunnistusvälityspalvelun kautta (eikä suoraan tunnistusvälineen tarjoajilta), joten tunnistettaessa suomalaisella tunnistusvälineellä ulkomaisessa asiointipalvelussa tunnistustiedot välitetään myös luottamusverkostossa tunnistusvälineen ja tunnistusvälityksen välillä.

Väestörekisterikeskuksen lausunnossa ei esitetä suoranaisia aikataulutaivoitteita valinnaisten attribuuttien välityskyvylle kansallisessa luottamusverkostossa.

### **Lausuntopyynnön kysymys 10**

**Onko yksityisellä sektorilla tarvetta ulkomaisten luonnollisten ja oikeushenkilöiden vahvaan tunnistamiseen sähköisessä asiointinnissa?**

#### **Lausunnot**

**Danske:** *On oletettavaa, että tarvetta ulkomaisten luonnollisten ja oikeushenkilöiden vahvaan tunnistamiseen sähköisessä asiointinnissa tulee olemaan.*

**Nordea:** *Nordealla on erityisesti yrityspankkipuolella noussut joitain kysymyksiä tähän liittyen esim. hoidettaessa joidenkin monikansallisten yritysten asioita. Olisi hyvä, että tämän käyttöönnotolle luotaisiin tekninen valmius mahdollisimman pian.*

#### **OP Ryhmä**

OP kannattaa rajat ylittävän tunnistamisen kehittämistä. Tarvetta on tunnistaa asiakkaita etenkin Pohjoismaiden ja Baltian kesken. Lisäksi tarvetta on erityisesti ulkomaalaisten asiakkaiden tuntemista koskevan KYC-prosessin hoitamiseen. Oleellista on ratkaista se, miten tämä voidaan käytännössä toteuttaa ja mitkä ovat ne tekniset menetelmät, joiden varaan se rakennetaan.

**Nets:** *Netsin kokemuksen mukaan kansainvälisillä asiointipalveluilla on tarve rajat ylittävään vahvaan tunnistamiseen sähköisessä asiointinnissa.*

**Signom:** *Kyllä on. Saamme jatkuvasti asiakkailta kyselyjä ulkomailla olevien luonnollisten henkilöiden ja oikeushenkilöiden tunnistamismahdollisuuksista. Mikäli Väestörekisterin solmupisteen kautta tapahtuvaa tunnistusta voisi hyödyntää myös yksityisen sektorin toimijat, näkisimme sen erinomaisena kehityksenä ja edistysaskeleena digitaalisten sisämarkkinoiden luomisessa.*

#### **Finanssivalvonta**

Finanssivalvonnan näkemyksen mukaan tällainen tarve voi olla esimerkiksi muodostettaessa asiakkuuksia finanssialan palveluissa, jolloin edellytetään asiakkaan tuntemista.

### **Viestintäviraston päätelmät**



Lausunnot tukevat sitä, että valmiutta valinnaisten attribuuttien käyttöön-ottoon on hyödyllistä nostaa. Valinnaiset attribuutit tukevat ulkomaisen henkilön yksilöimistä silloin, kun ulkomailta saadut pakolliset attribuutit eivät riitä siihen.

Kansallisen solmupisteen kehittämisestä Viestintävirasto viittaa Väestörekisterikeskuksen lausumaan edellä kysymyksen 9 kohdalla.

### **Lausuntopyynnön kysymys 11**

#### **Mitä muuta haluatte tuoda esille valinnaisista attribuuteista?**

##### **Lausunnot**

###### **OP Ryhmä**

Käsityksemme mukaan valinnaisia attribuutteja ei pitäisi edellyttää tässä vaiheessa edes määrittelyn ja suunnittelun tasolla, koska niille ole olemassa todellista tarvetta ja rajapintamäärittelyjen laajentaminen valinnaisiin attribuutteihin aiheuttaisi lisäpainetta jo ennestään haastavalle aikataululle.

Kuten aiemmin olemme jo todenneet, emme ymmärrä valinnaisten attribuuttien tarkoitusta kansallisessa järjestelmässä. Valinnaiset attribuutit tulisikin poistaa ja solmupisteen tulisi sen sijaan muuttaa kansainväliset tunnistuspyynnöt kansalliseen formaattiin. Rajapintalajennukset voidaan tulevaisuudessa toteuttaa rajapintojen versioinnilla ilman valinnaisia attribuutteja.

##### **Viestintäviraston päätelmät**

Ks. päätelmät kysymysten 7 ja 9 kohdalla.

Rinnakkaisten versioiden käyttäminen tuotannossa on asia, joka voidaan ottaa pohdittavaksi luottamusverkoston yhteistoimintaryhmässä. Nykyisten SAML- ja OIDC-rajapintasuosittelujen lähtökohta on ollut, että käytössä on yksi versio, jossa voidaan välittää eri poimintoja määritellyistä attribuuteista.

### **3 Määräyksen TLS-vaatimuksen noudattamisen valvonnassa määriteltävä korjausaikataulu**

#### **Lausuntopyynnön kysymys 12**

##### **Mitä haluatte tuoda esille korjausaikataulusta ja viestinnästä käyttäjille?**

##### **Lausunnot**

###### **Finanssiala ry**

Se, että tunnistuksessa on käytettävä tietoliikenteen salauksessa vähintään TLS-protokollan versiota TLS 1.1., on ollut jo jonkin aikaa voimassa oleva vaatimus. Kuten jo todettua, tällä korjauksella on suuria vaikutuksia tunnistamisen palveluiden käyttäjäkunnassa. FA:n mielestä on ensiarvoisen tärkeää, että Viestintävirasto on valmistautunut viestimään asiasta. FA tukee, omien resurssien puitteissa, tätä viestintää.

**Danske:** *On tärkeää, että Viestintävirasto on varautunut viestimään TLS-asiasta käyttäjille. Viestinnässä pitää kiinnittää huomiota asian kansantajuistamiseen.*

**Nordea:** *TLS protokollan käytöstä luopuminen ei ole suoraan liityksissä TUPAS protokollasta luopumiselle vaan voidaan toteuttaa oman erikseen sovittavan aikataulun mukaan. Olennaisinta muutoksen läpiviennissä on yhtenäinen ja selkeä viestintä muutoksesta viranomaisten toimesta, johon toimijat voivat viitata omassa viestinnässään muutosta tehtäessä.*

## OP Ryhmä

Viestintäviraston tulisi toimia tulevissa muutoksissa aktiivisena viestijänä käyttäjien ja asiointipalveluiden suuntaan. Erityistä viestintätarvetta on havaittu esimerkiksi vanhentuneiden laitteiden osalta.

## Ålandsbanken

*OIDC-lösningen kommer att stöda TLS 1.2, banken har redan slutat stöda TLS 1.0-protokollet i enlighet med kraven och informerat kunder om det.*

*Ingen av de ärendehanteringstjänster banken har avtal med verkar använda TLS 1.0-protokollet längre.*

## Väestörekisterikeskus

*Selkeyden vuoksi, mikäli siirtymäaikaa jatketaan rajapintojen osalta, määräyksessä voisi omana kohtanaan (pykälänä) tuoda esiin ainakin yhteyden suojaukseen liittyvään vaatimukseen (TLS 1.2). Nykyisen luonnoksen viittaus 7 §:n momentteihin 1-4 saattaa hämmentää ja siten hankaloittaa varhaisemmista TLS-versioista luopumista, vaikka ne ovat riski eikä niistä luopuminen vaadi varsinaista rajapintamuutosta.*

## Viestintäviraston päätelmät

Viestintävirasto valmistelee valvontatoimenpiteenä korjausvelvoitteet niille tunnistuspalveluille, jotka eivät vielä noudata TLS-vähimmäisvaatimusta.

**Korjaukset tullaan vaatimaan tehtäväksi viimeistään 1.1.2019.**

Viestintävirasto viestii asiasta yleisölle.

Tässä määräysmuutoksessa muutetaan vain siirtymäaikoja koskevaa 25 §:ää. Muita määräyksen muutos- ja päivitystarpeita voidaan selvittää seuraavassa määräysmuutoksessa.