

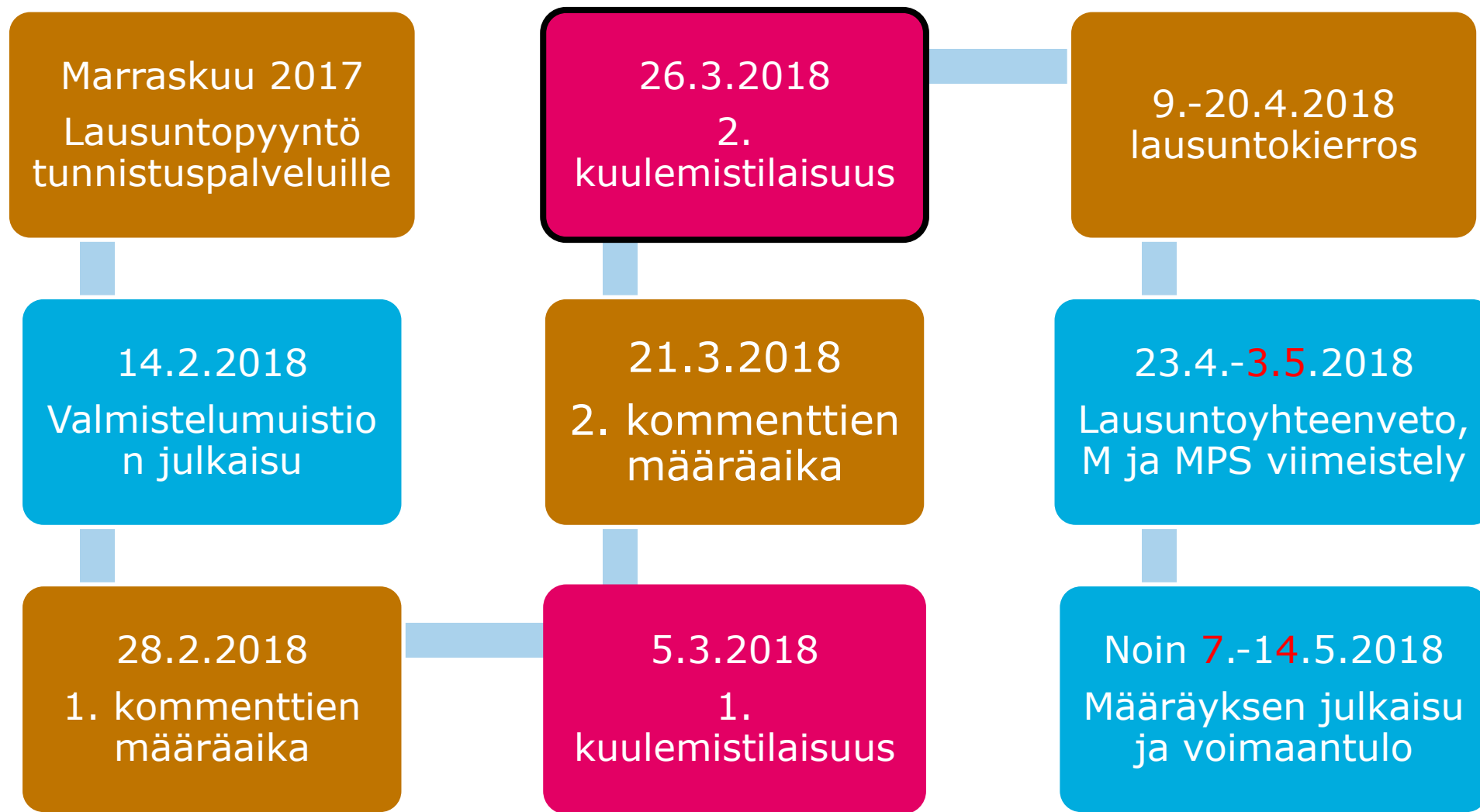


Viestintävirasto

Tunnistismääräyksen 72A Tupas-muutos

2. kuulemistilaisuus 26.3.2018

Määräysvalmistelun aikataulu



Asialista 26.3.18

Klo 13-14.30 työpajat kahdessa eri tilassa

- Työpaja 1: viestintä asiointipalveluille ja käyttäjille
- Työpaja 2: tekninen (työpajan kalvot kalvosetin lopussa)

n. klo 14.45–16 yhteinen osuus

- Määräysmuutos 72A
 - » Optionaaliset attribuutit
 - » Rajapintamuutoksen siirtymäaikataulu
- TLS 1.0 –korjaus aikataulu
- Lausuntokierros 9.-20.4.2018 määräysmuutoksesta

Määräysmuutos 72A

Optionaaliset attribuutit ja tupas-rajapinnat,
siirtymäaikataulu

Optionaaliset attribuutit

Määräys 12 § 2 mom. ja siirtymäsäännös 25 §

Määräys 72 12 § 2 mom.

12 § Luottamusverkostossa välitettävät vähimmäistiedot

[...]

Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on oltava valmius välittää:

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

Määräys 72

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.*

Valmisteluvaiheen linjaukset optionaalisista attribuuteista 1/2

- M72 *"oltava valmius välittää"* tarkoittaa määräyksen perustelujen MPS72:n mukaan sitä, että *"Pykälän 2 momentissa lueteltuja tietoja varten täytyy määritellä tietokentät käytettävään prokollaan, jotta tietojen välittäminen voidaan ottaa helposti käyttöön, jos niin sovitaan."*
- Ehdotus: Pidetään kiinni määrittelyvelvoitteesta, koska spesifikaatiot ovat valmiina ja määrittely parantaa valmiutta ottaa tiedot käyttöön
- Ehdotus: Muutetaan siirtymäaikaa (nyt voimassa oleva 18.9.2018)
- Ehdotus: "Valmius välittää" pidetään samanlaisena. Muutokset tehdään siirtymäsäännökseen. Lisätään MPS72A:een selventäviä perusteluja, mitä valmius tarkoittaa.
- Ehdotus: Määrittelyt näille attribuuteille täytyisi tehdä **1.10.2018 mennessä** samalla kun muutenkin tehdään uudet rajapintamäärittelyt. Attribuutit on määritelty kansallisessa SAML- ja OIDC-spesifikaatiossa.

Valmisteluvaiheen linjaukset optionaalisista attribuuteista 2/2

- Selvennys: Määräyksessä ei vaadita, että tunnistuspalveluiden *kaikkiin taustajärjestelmiin* määritellään valmius käsitellä näitä attribuutteja. Ei siis tarvitse viedä tuotantoon, ennen kuin tiedolla on kysyntää ja asiasta sovitaan.
- Viestintävirasto suosittelee, että kun järjestelmiin tehdään muutoksia, huomioidaan ja arvioidaan näiden attribuuttien määrittely myös taustajärjestelmissä. Toimijat voisivat harkintansa mukaan valmistautua attribuuttien käyttöön muiden järjestelmämuutostensa yhteydessä.
- Ehdotus: poikkeuksena muihin valinnaisiin attribuutti julkinen/yksityinen asiointipalvelu täytyisi viedä tuotantoon asti samassa tahdissa kuin rajapinnat uusitaan muutenkin. Tälle tiedolle arvioidaan olevan tarvetta muita valinnaisia attribuutteja nopeammin sekä kansallisissa että rajat ylittävissä veloituksissa.
- Kysymys: julkinen vai yksityinen asiointipalvelu -attribuutti kulkenee välityspalvelun suunnasta informaationa välineen tarjoajalle. Suomessa julkinen asiointipalvelu lienee aina suomi.fi (sen takana oleva asiointipalvelu). Olisiko tarvetta porrastaa välineen ja välityksen tarjoajan siirtymäaikaa luottamusverkoston sisällä esim. 1.1.19 ja 14.9.19?

Määräys 72/2016 nykyinen siirtymäsäännös

25 § 4 mom.

25 § Voimaantulo ja siirtymäsäännökset

Tämä määräys tulee voimaan 2.11.2016 ja on voimassa toistaiseksi.

[...]

[...]

Määräyksen 3 lukua sovelletaan 1.5.2017 alkaen lukuun ottamatta 12 §:n 2 momenttia, jonka mukaiset vaatimukset tulee täyttää viimeistään 18.9.2018.

Määräys 72A/2018 25 § 4 mom. muutosehdotus

25 § Voimaantulo ja siirtymäsäännökset

Tämä määräys tulee voimaan 14.5.2018 ja on voimassa toistaiseksi.

[...]

[...]

Määräyksen ~~3 luku~~ sovelletaan ~~1.5.2017~~ alkaen lukuun ottamatta 12 §:n 2 momentintia, jonka tietojen määrittelyvaatimukset rajapinnassa käytettävässä protokollassa on tehtävä tulee täyttää viimeistään 1.10.2018. Edelleen 12 §:n 2 momentin 1 alakohdan tarkoittaman tiedon on oltava välitettävissä määräyksen 8 §:n, 9 §:n ja 13 §:n tarkoittamissa rajapinnoissa 1.1.2019.

Kuulemistilaisuudessa 26.3.18 esitetyt kommentit

- Julkinen/yksityinen asiointipalvelu -attribuutin tarve
 - » Kommentoitiin, että tietokentän lisääminen rajapintaan ehdotetussa aikataulussa olisi vaikea muutos, koska rajapintoja on nyt jo määritelty Viestintäviraston suosituksen mukaan (ilman valinnaisia attribuutteja)
 - » Keskusteltiin siitä, onko tieto kansallisessa tunnistamisessa tarpeellinen ja syntyykö tarvetta tiedolle suomi.fi:lle tarjoamisessa. Kommentoitiin, että ei ole tarvetta.
 - » Keskusteltiin siitä, mitä toimijoita rajat ylittävä tunnistaminen koskee. Kommentoitiin, että attribuutteja ei pitäisi vaatia muilta kuin niiltä, joilla on tarvetta tai jotka notifioivat välineensä EU:lle.
 - » Viestintävirasto totesi, että MPS72:ssa oletus on VRK:n kanssa 2016 tehdyn valmistelun perusteella, että rajat ylittävä tunnistaminen välittyy molemmissa suunnissa tunnistusvälityspalvelun kautta (virasto varmistaa suunnitelmien nykytilaa vielä VRK:lta)
- Valinnaisten attribuuttien valmiuden tekninen toteutettavuus rajapinnassa
 - » Kommentoitiin, että jos valinnaisten attribuuttien tietokentät määritellään valmiiksi rajapintaan, ne täytyy tarvittaessa määritellä käsittelyssä ohitettavaksi.
 - » Joissakin protokollissa pystytään dynaamisesti ohittamaan tarpeettomat kentät.
- Viestintävirasto miettii palautteen perusteella sääntelyn vaihtoehtoja:
 - » Siirtymäajan jatkaminen määräyksessä, suositukseksi muuttaminen tai joku muu?
 - » Toimijat eivät esittäneet muita vaihtoehtoja kuin poistaminen määräyksestä suositukseksi.
 - » Lausuntokierros vielä tärkeä

TUPAS-rajapinnat

Määräys 7-9 §§ ja siirtymäsäännös 25 §

Valmisteluvaiheen linjaukset siirtymäajasta ja valvonnasta

1/2

- Ehdotus: Siirtymäaikataulu porrastetaan
 - » Perustelu: Noudattaa normaalia tuotannon vaiheistusta
 - » Perustelu: Mahdollistaa etenemisen valvonnan
- Ehdotus: Rajapinnan suunnittelu ja määrittely viimeistään olisi tehtävä viimeistään **1.10.2018**
 - » Perustelu: Salausvaatimukset ovat olleet selvillä määräyksessä vuonna 2016.
 - » Perustelu: Uudet rajapintaspesifikaatiot on julkaistu 1/2018 (luonnokset lausunnoilla 10/2017)
 - » Suunnitelma: Viestintävirasto tekee valvontakyselyn syys-lokakuussa 2018. Tarvittaessa harkitaan normaalit tunnistuslain hallintoseuraamukset (korjausvelvoite, huomautus, uhkasakko)
- Määräyksessä ei oteta kantaa tunnistusperiaatteiden tai niissä viitattujen palveluehtojen ehtojen määrittelyyn. Määräyksen perusteluihin MPS:ssä lisätään maininta, että rajapinnan tarjolle saattaminen edellyttää luonnollisesti myös ehtojen saatavuutta.

Valmisteluvaiheen linjaukset siirtymäajasta ja valvonnasta 2/2

- Ehdotus: Uudet rajapinnat olisi tuotava tarjolle viimeistään **1.1.2019**
 - » Perustelu: Salausvaatimukset ovat olleet selvillä määräyksessä jo vuoden 2016 lopusta.
 - » Perustelu: Uudet rajapintaspesifikaatiot on julkaistu 1/2018 (luonnokset lausunnoilla 10/2017)
 - » Perustelu: Mahdollistaa uuden toteutuksen käyttöönoton asiointipalveluille, jotka ovat valmiita siirtymään tai hankkivat palveluita uutena asiakkaana
 - » Suunnitelma: Viestintävirasto tekee valvontakyselyn joului-tammikuussa. Tarvittaessa harkitaan normaalit tunnistuslain hallintoseuraamukset (korjausvelvoite, huomautus, uhkasakko, kiello tarjota vahvana)
- Ehdotus: Vanhoissa asiointipalvelusopimuksissa rajapinnat olisi muutettava viimeistään **14.9.2019**
 - » Perustelu: Tunnistuspalveluilla 1 v 4 kk lisääikaa kontaktoida vanhat sopimuskumppanit
 - » Perustelu: Sama takaraja kuin PSD2-muutoksissa on tulossa
 - » Perustelu: Antaa asiointipalveluille aikaa tehdä muutokset ja halutessaan kilpailuttaa tunnistuspalvelut (hankkia tunnistusvälityspalveluilta)
 - » Suunnitelma: Viestintävirasto tekee valvontakyselyn syyskuussa. Tarvittaessa harkitaan normaalit tunnistuslain hallintoseuraamukset (korjausvelvoite, huomautus, uhkasakko, kiello tarjota vahvana)

Neuvontaa tunnustuslain 14 § tunnistusperiaatteista

Tunnistuspalvelun tarjoajalla on oltava tunnistusperiaatteet, joissa määritellään tarkemmin, kuinka palveluntarjoaja täyttää tässä laissa säädettyt velvollisuutensa. [...]

Lisäksi tunnistusperiaatteissa on oltava keskeiset tiedot:

2) tarjottavista palveluista ja niiden hinnoista;

3) kaikista sovellettavista ehdoista;

5) palveluntarjoajan tärkeimmistä yhteistyökumppaneista;

7) muista merkityksellisistä seikoista, joiden perusteella palveluntarjoajan toimintaa ja luotettavuutta voidaan arvioida.

[...]

Tunnistuspalvelun tarjoajan on pidettävä tunnistusperiaatteet yleisesti saatavilla ja ajantasaisina.

- Viestintäviraston neuvot:
 - Tunnistusperiaatteet voi laatia melko yleisluonteisesti, jotta ei tarvitse muuttaa tiheästi
 - Tunnistusvälityspalvelut, jotka välittävät tunnistusta, ovat tunnistusvälineen tarjoajan tärkeimpinä yhteistyökumppaneita. Niistä voi halutessaan informoida tunnistusperiaatteissa myös viittaamalla yleisesti rekisteröityihin luottamusverkoston jäseniin nimeämättä kaikkia yksittäisiä yrityksiä.
 - Viestintävirasto on tunnistuspalveluntarjoajien ilmoituksista tekemissään täydennyspyynnöissä edellyttänyt, että tunnistusvälineen tarjoajat informoivat tunnistusperiaatteissa, että tunnistuspalvelu voi olla tarjolla asiointipalveluille myös luottamusverkostoon/Viestintäviraston rekisteriin kuuluvan tunnistusvälityspalvelun kautta. Tämä mahdollistaa käyttäjille ja asiointipalveluille tunnistuspalvelun luotettavuuden arvioinnin ja ymmärtämisen, kun tunnistukseen osallistuu myös tunnistusvälityspalvelu.

Vertailu: Tunnistus- ja maksupalvelusääntelyn aikataulu

Määräys 72/2016 ja 72A/2018 - Vaatimukset luottamusverkosto- ja asiointipalvelurajapinnalle	PSD2 RTS - tunnistusmenetelmän ja dedikoidun maksutoimeksianto- tai tilitietorajapinnan vaatimukset
2.11.2016 määräys 72/2016 M voimaan	
	14.3.2018 komissio antaa RTS:n
Ehdotus: n. 14.5.2018 72A/2018 M voimaan, siirtymäajan jatkaminen	
Ehdotus: 1.10.2018 määriteltävä tekninen toteutus	
Ehdotus: 1.1.2019 saatettava muutetut rajapinnat tarjolle luottaville osapuolille (sekä korjattava TLS 1.0)	
	14.3.2019 art. 30 dedikoidut testirajapinnat tarjolle
Ehdotus: 14.9.2019 toteutettava myös vanhoissa asiointipalvelusopimuksissa	14.9.2019 tunnistusmenetelmän muutokset ja TPP-rajapinnat tuotannossa



Määräys 72/2016 nykyinen siirtymäsäännös

25 § Voimaantulo ja siirtymäsäännökset

Tämä määräys tulee voimaan 2.11.2016 ja on voimassa toistaiseksi.

[...]

Jos tunnistuspalvelun rajapinnoissa käytetään TUPAS-protokollaa, 2 luvun 7 §:n 4 momentin ja 8 §:n 3 momentin vaatimukset henkilötietojen sanomatasoisesta salauksesta sekä 9 §:n 2 momentin vaatimus henkilötietojen suojaamisesta asiointipalvelu- ja päätelaiterajapinnassa tulee toteuttaa viimeistään 18.9.2018.

[...]

Määräys 72A/2018 25 § 3 mom. muutosehdotus

25 § Voimaantulo ja siirtymäsäännökset

Tämä määräys tulee voimaan 14.5.2018 ja on voimassa toistaiseksi.

[...]

Jos tunnistuspalvelun rajapinnoissa käytetään TUPAS-protokollaa, 2 luvun 7 §:n 4 momentin ja 8 §:n 3 momentin vaatimukset henkilötietojen sanomatasoisesta salauksesta sekä 9 §:n 2 momentin vaatimus henkilötietojen suojaamisesta asiointipalvelu- ja päätelaiterajapinnassa ~~tulee toteuttaa viimeistään 18.9.2018.~~ on toteutettava kaikilta osin [kaikissa sopimussuhteissa] viimeistään 14.9.2019. Tunnistuspalvelun tarjoajan on määriteltävä tämän määräyksen vaatimukset täyttävä toteutus teknisesti viimeistään 1.10.2018 ja saatettava muutetut rajapinnat tarjolle luottamusverkostossa sekä luottaville osapuolille viimeistään 1.1.2019.

[...]

- Kysymys: onko selvempää sanoa "kaikilta osin" vai "kaikissa sopimussuhteissa"?

Määräys 72/2016 M koko nykyinen siirtymäsäännös

25 § Voimaantulo ja siirtymäsäännökset

Tämä määräys tulee voimaan 2.11.2016 ja on voimassa toistaiseksi.

Tällä määräyksellä kumotaan Viestintäviraston määräys 7 B/2009 M tunnistuspalvelun tarjoajien ja yleisölle laatuvarmenteita tarjoavien varmentajien ilmoitusvelvollisuudesta Viestintävirastolle, annettu 27.8.2009, ja määräys 8 C/2010 M tunnistuspalvelun tarjoajien ja laatuvarmenteita tarjoavien varmentajien toiminnan luotettavuus- ja tietoturvallisuusvaatimuksista, annettu 20.10.2010.

Jos tunnistuspalvelun rajapinnoissa käytetään TUPAS-protokollaa, 2 luvun 7 §:n 4 momentin ja 8 §:n 3 momentin vaatimukset henkilötietojen sanomatasoisesta salauksesta sekä 9 §:n 2 momentin vaatimus henkilötietojen suojaamisesta asiointipalvelu- ja päätelaiterajapinnassa tulee toteuttaa viimeistään 18.9.2018.

Määräyksen 3 lukua sovelletaan 1.5.2017 alkaen lukuun ottamatta 12 §:n 2 momenttia, jonka mukaiset vaatimukset tulee täyttää viimeistään 18.9.2018.

Määräys 72A/2018 koko muutosehdotus siirtymäsäännökseksi

25 § Voimaantulo ja siirtymäsäännökset

Tämä määräys tulee voimaan 14.5.2018 ja on voimassa toistaiseksi.

Tällä määräyksellä kumotaan Viestintäviraston 2.11.2016 antama määräys 72/2016 M sähköisistä tunnistus- ja luottamuspalveluista.

Jos tunnistuspalvelun rajapinnoissa käytetään TUPAS-protokollaa, 2 luvun 7 §:n 4 momentin ja 8 §:n 3 momentin vaatimukset henkilötietojen sanomatasoisesta salauksesta sekä 9 §:n 2 momentin vaatimus henkilötietojen suojaamisesta asiointipalvelu- ja päätelaiterajapinnassa on toteutettava kaikilta osin [kaikissa sopimussuhteissa] viimeistään 14.9.2019.

Tunnistuspalvelun tarjoajan on määriteltävä tämän määräyksen vaatimukset täyttävä toteutus teknisesti viimeistään 1.10.2018 ja saatettava muutetut rajapinnat tarjolle luottamusverkostossa sekä luottaville osapuolille viimeistään 1.1.2019.

Määräyksen 12 §:n 2 momentin tietojen määrittely rajapinnassa käytettävässä protokollassa on tehtävä viimeistään 1.10.2018. Edelleen 12 §:n 2 momentin 1 alakohdan tarkoittaman tiedon on oltava välitettävissä määräyksen 8 §:n, 9 §:n ja 13 §:n tarkoittamissa rajapinnoissa 1.1.2019.

Kuulemistilaisuudessa 26.3.18 esitetyt kommentit

- Rajapintojen suunnittelu/määrittelyn määräaika 1.10.2018
 - » Ks. kommentit valinnaisten attribuuttien kohdalla, SAML- ja/tai OIDC-määrittelyjä on jo tehty.
- Uuden rajapinnan tarjolle saattamisen määräaika 1.1.2019
 - » Kommentoitiin, että määräajan asettaminen vuodenvaihteeseen tarkoittaa käytännössä sitä, että rajapinnat täytyisi saada tuotantoon jo joulukuussa, koska vuodenvaihteessa on IT-muutoksissa tyypillisesti tauko. (=> Täydennys toimialalta tilaisuuden jälkeen: tauko voi olla jopa 2 kk 1.12.-31.1.)
 - » Kommentoitiin sitä, että jos välineen tarjoajan ja välityspalvelun täytyy saada uudet rajapinnat tarjolle samaan aikaan, testaamiselle ei jää aikaa. Kommentoitiin kuitenkin, että koska vanhat rajapinnat saavat olla rinnalla käytössä, ei ole määräyksessä tarpeen porrastaa määräaikaa. (=> Täydennys toimialalta tilaisuuden jälkeen: välityspalveluilla on jo nyt valmiuksia tarjota asiointipalveluille SAML- ja OIDC-rajapintaa).

Kuulemistilaisuudessa 26.3.18 esitetyt kommentit

- Asiointipalveluiden rajapinnan muuttamisen takaraja vanhoissa sopimuksissa 14.9.2019
 - » Kommentoitiin, että asiointipalveluiden kontaktointi ja toimet vievät aikaa. Vertailun vuoksi pankkialan SEPA-muutoksessa oli siirtymäaikaa 2 vuotta ja vielä lähellä takarajaa oli 60 000 asiointipalvelua siirtymättä uuteen järjestelmään.
 - » Kommentoitiin, että asiointipalvelulla voi mennä aikaa myös tunnistuspalveluiden kilpailutukseen.
 - » Ehdotettiin määräajaksi kuun vaihdetta, joka voisi olla asiointipalvelusopimusten kannalta toimivampi kuin kuukauden puoliväli 14.9.19 ja näin PSD2-muutokset eivät tulisi tuotantoon samanaikaisesti.
 - » Viestintävirasto totesi, että määräaika voi toki yhtä hyvin olla 1.9.19 tai 1.10.19

TLS 1.0 korjausaikataulu

Valvonta- ja viestintäasia, ei määräysmuutos

Harkinnassa oleva korjausaikataulu

- Määräyksessä 72/2016 vaaditaan tietoturvallisuussyistä tunnistuspalvelussa TLS-protokollan vähintään TLS 1.1-version käyttöä
- TLS 1.0 ei siis ole 2.11.2016 lähtien täyttänyt vaatimuksia. Osalla toimijoista TLS 1.0 on edelleen käytössä.
- Viestintävirasto tulee vaatimaan toteutusten korjaamista. Määräajaksi harkitaan **1.1.2019. Kysymys ei siis ole määräysmuutoksesta vaan vaatimusten noudattamisen valvonnasta.**
- Tämä tarkoittaa sitä, että käyttäjät eivät enää voi käyttää vahvaa tunnistusta selaimilla ja päätelaitteilla, jotka eivät tue vähintään TLS 1.1-versiota.
- Virasto käsittelee korjausaikataulua nyt toimijoiden kanssa määräystyön yhteydessä, koska TLS 1.0 sulkeminen vaikuttaa käyttäjiin ja käyttäjäviestintää olisi hyvä pohtia yhdessä.
- Monet toimijat ovat kuitenkin jo vaatimusten mukaisesti sulkeneet TLS 1.0 -käytön vahvassa tunnistamisessa.
- Viestintävirasto ei ole saanut toistaiseksi lisää tietoa jäljellä olevien TLS 1.0 -käyttäjien määrän arviointiin
- Myös Viestintävirasto tiedottaa asiasta.

Kuulemistilaisuudessa 26.3.18 esitetyt kommentit

- Kommentoitiin, että Viestintävirastolta toivotaan myös viestintää asiasta, jotta toimijat voisivat viitata viralliseen neutraaliin lähteeseen.
- Viestintävirasto tiedottaa asiasta.
- Tilaisuuden alkuosan viestintätyöpajassa keskusteltiin myös siitä, miten ne pankit, joita TLS 1.0 -tuen poistuminen vielä koskee, informoivat asiakkaitaan muutoksesta.
 - » Toivottiin, että nämä pankit selvittäisivät, pystyisikö tuen poistumisesta informoimaan käyttäjiä esimerkiksi niin, että jos käyttäjällä havaitaan olevan vain TLS 1.0 -protokollaa tukeva päätelaite, käyttäjä saisi jonkinlaisen ilmoituksen tuen poistumisesta tunnistuspalvelun tai verkkopankin käytön yhteydessä esimerkiksi kirjautumissivulla.

Lausuntokierros ja uutisointi määräysmuutoksesta 72A/2018 M

Lausuntokierros 9.4.-20.4.18

Lausuntokierros määräysmuutoksesta

- Lausuntopyyntö, luonnos määräyksestä 72 A/2018 M ja luonnos MPS72A julkaistaan Viestintäviraston lausuntopyyntösivulla n. 9.4.2018.
- Ainakin määräys käännetään ruotsiksi lausuntokierrokselle. Pyritään kääntämään myös MPS. Englanninkieliset versiot tulevat myöhemmin.
- Lausuntopyynnöstä informoidaan lisäksi sähköpostilla eidas-ryhmää, luottamusverkoston yhteistoimintaryhmää, relevantteja viranomaisia sekä muita tahoja
- Viestintävirasto tiedottaa/uutisoi n. 9.4.2018 muutoksesta ja lausuntopyynnöstä
- Lausuntoaika tulee olemaan 9.-20.4.2018
- Viestintävirasto pyrkii julkaisemaan lausuntokoosteen ja kommenttinsa siihen n. 2.5.2018
- Viestintävirasto viimeistelee määräyksen ja MPS:n ja pyrkii julkaisemaan sen viimeistään 14.5.2018.

Kuulemistilaisuudessa 26.3.18 esitetyt kommentit

- Kysyttiin, voiko määräysmuutoksesta lausua mikä tahansa?
- Viestintävirasto totesi, että lausua voi kuka tahansa ja lausuntoja toivotaankin erityisesti asiointipalveluilta tai näiden edustajilta. Virasto pyrki saamaan näitä mukaan kuulemistilaisuuksiin, mutta ei saanut toimijoita juurikaan paikalle. Mm. tästä syytä virasto uutisoi asian lausuntokierrosvaiheessa.

TYÖPAJA

Tekninen tarkastelu:

Asiointipalvelun rajapinnan muutos Tupaksesta
SAMLiin ja/tai OIDC:hen

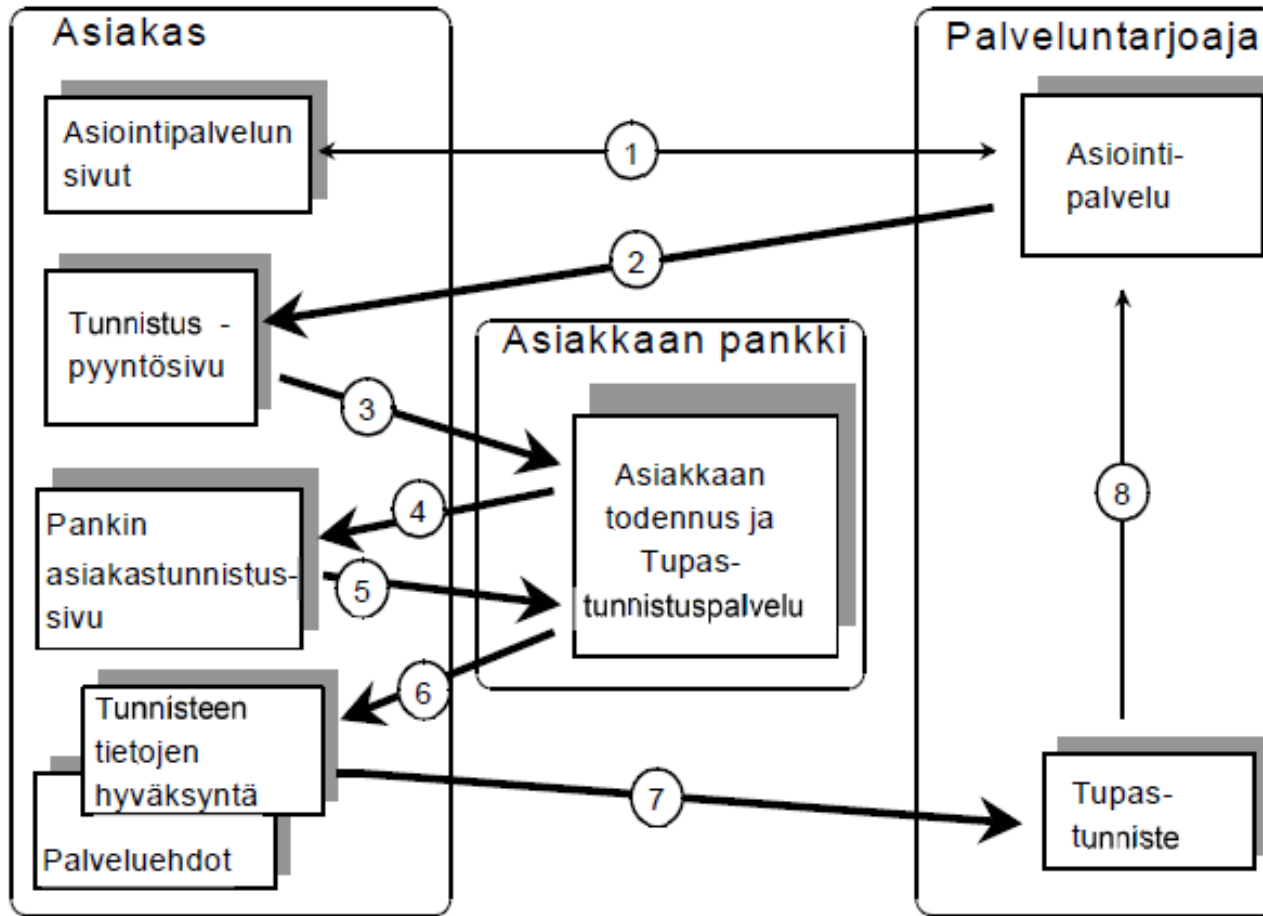
Session tarkoitus

- Selventää sitä, millaisia konkreettisia muutoksia asiointipalvelussa tarvitaan

Nykytilanne, tietojen suojaus verkon ylitse lähetettäessä, Tupas/E-tunniste

- Pankki toimittaa palveluntarjoajalle palvelun käytön edellyttämän tarkisteavaimen (MAC-avain) palvelukuvauksensa mukaisesti
- Tunnistussanomien eheys tarkistetaan MAC-avaimeen perustuen
 - » Tietojen luottamuksellisuutta suojataan vain salaamalla tietoliikenne
- Jatkossa henkilötietoja sisältävien sanomien eheys ja luottamuksellisuus on suojattava liikenteen salauksen lisäksi myös sanomatasolla
- Tarkentuneet salauksen algoritmivaatimukset
 - » Mikäli yhteyskäytännössä käytetään TLS-protokollaa, tulee käyttää vähintään TLS versiota 1.2 tai uudempaa versiota. TLS-versiota 1.1 voi käyttää ainoastaan, jos käyttäjän päätelaite ei tue uudempia versioita.

Nykytilanne



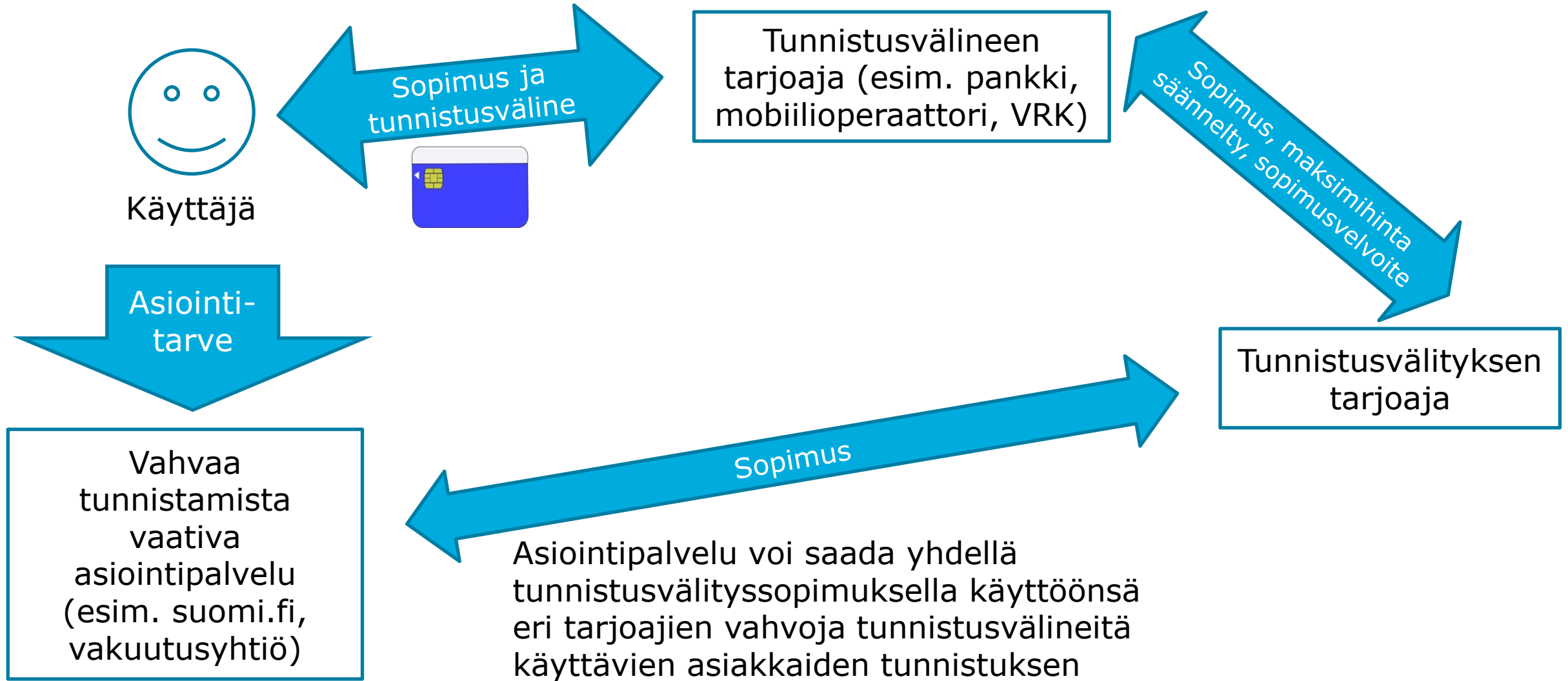
Suositeltuja protokollia/metodeja jatkossa:
* 2 ja 6: OIDC, SAML, tai muu M72 vaatimukset täyttävä. Ks. Vivin suositukset 212 ja 213 / 2018

* 4 ja 5: tunnistusvälineestä riippuva

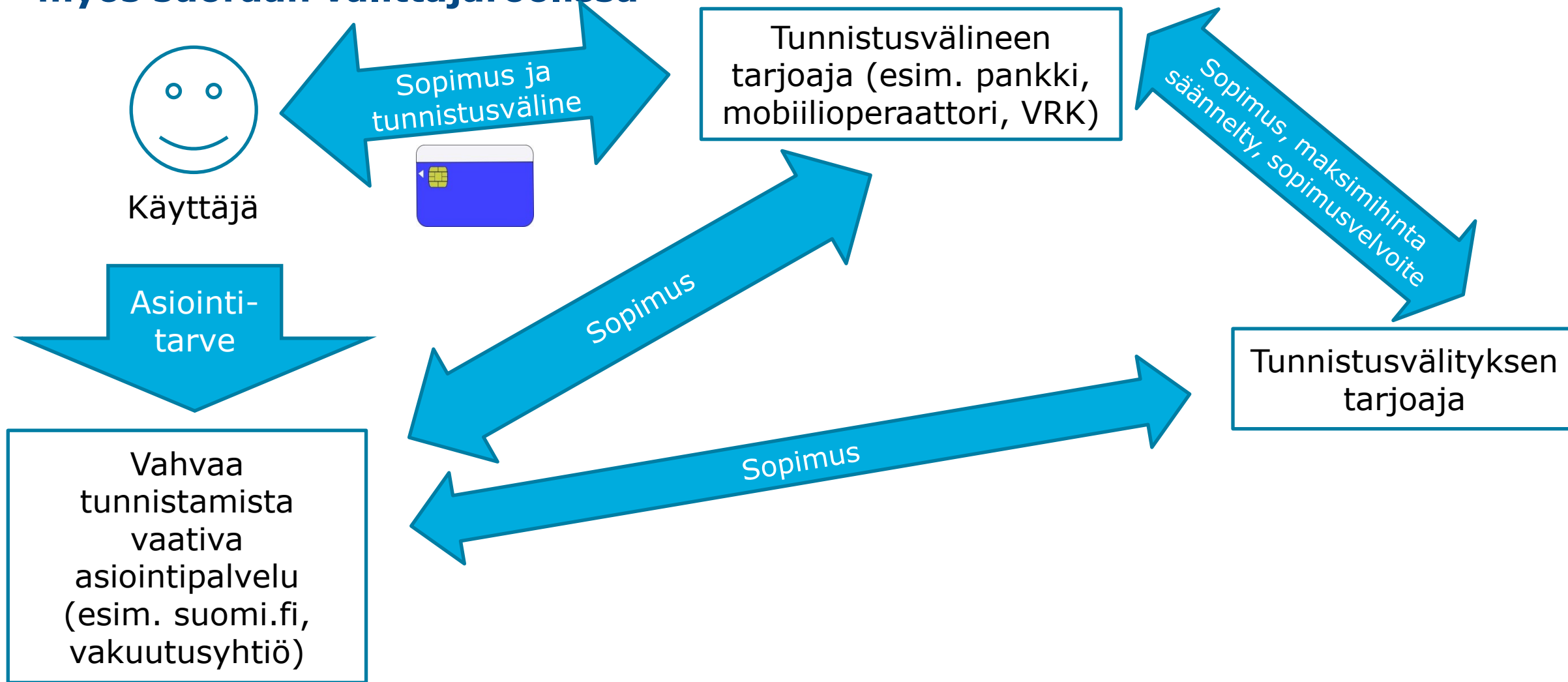
SAML/OIDC eroja Tupas-tunnistamiseen

- Kaikissa käytössä tietoliikennetasolla TLS-salaus
 - » Tarjoaa suojaa lähinnä tunnistustapahtuman ulkopuolisia vastaan
- Tunnistustapahtuman ja henkilötietojen eheyden ja luottamuksellisuuden suojaus sovellustasolla
 - » Tupas: jaettu (symmetrinen) pitkäaikainen avain, jota käytetään pyyntöjen ja vastausten MAC-tarkisteen laskemiseen SHA-256-tiivistealgoritmillä
 - Eheyssuojaus sekä pyynnöille että vastauksille, ei suojaa luottamuksellisuutta
 - Henkilötietoja voi jäädä URL:eista selaimen historiaan, www/proxy/tls-mitm-palvelimien lokitietoihin, jne
 - » OIDC/SAML: julkisen avaimen tekniikkaan perustuvat pitkäaikaiset avaimet, jokaisella osapuolella omansa
 - Pyynnot eheyssuojattuja, vastaukset (joissa henkilötietoja) lisäksi myös salattuja lyhytaikaisella avaimella
 - Algoritmit tavanomaisia vahvoja nykypäivänä käytettyjä, tyypillisimmin RSA 2k, AES 128, SHA-256
 - Myös asiakkaan toimitettava julkiset avaimensa OIDC/SAML-palveluntarjoajalle, Tupasissa riittää, että palveluntarjoaja toimittaa asiakkaalle jaetun yhteisen avaimen
- Tupas ja SAML välittää kaiken käyttäjän selaimen kautta, OIDC:ssä henkilötietoja sisältävät sanomat kulkevat suoraan OIDC-asiakkaan ja -palvelimen välillä

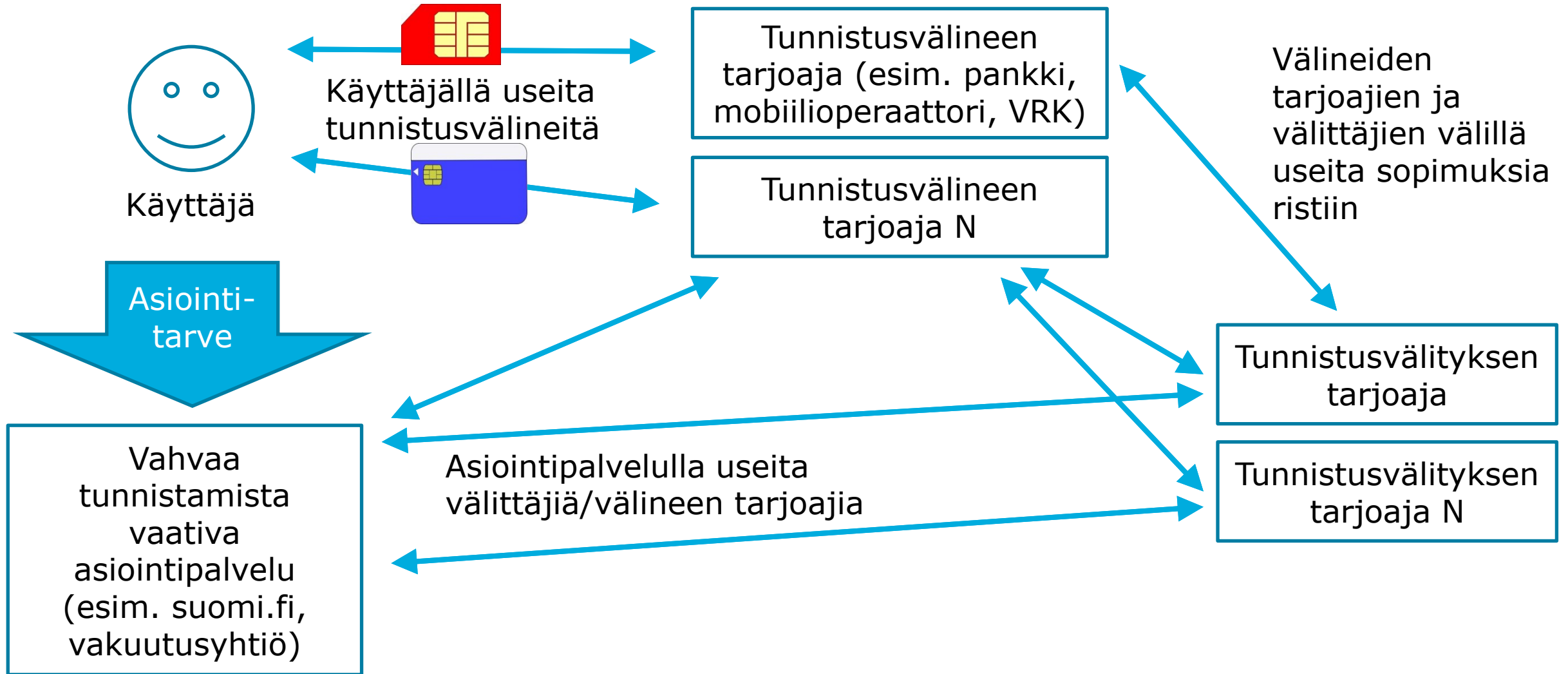
Sopimukset välityspalvelumallissa, perustapaus



Sopimukset välityspalvelumallissa, välineen tarjoaja voi olla myös suoraan välittäjäroolissa



Sopimukset välityspalvelumallissa, redundanssia

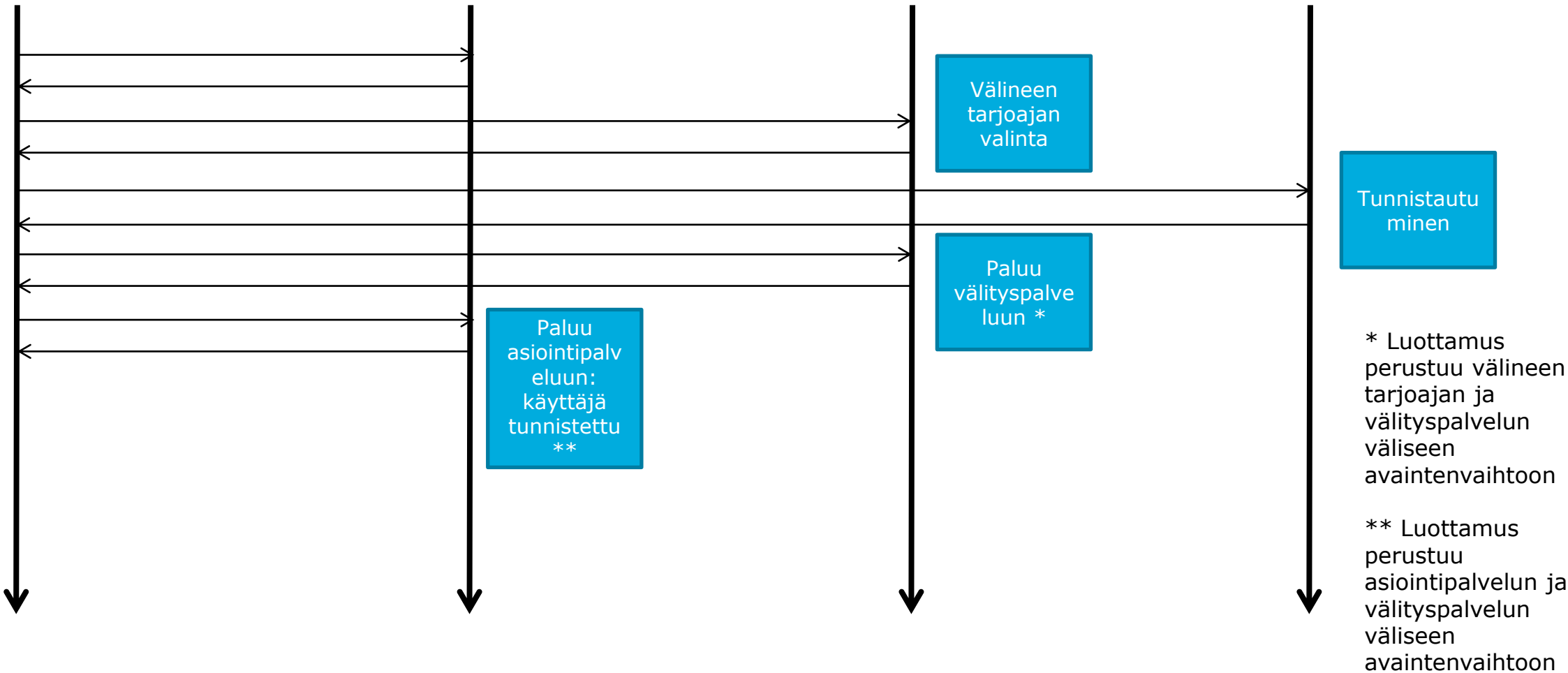


Tunnistautuja

Asiointipalvelu

Tunnistusvälitys

Välineen
tarjoaja



Yhteenveto

- Vahva tunnistus vaatii vaihtoa Tupaksesta SAML:iin tai OpenID Connectiin
 - » Tehtävä uusi varmenteiden vaihto ja luotava oma varmenne
- Jos hankkii kaikki tunnistuspalvelut samalta palveluntarjoajalta, on tehtävä vain yksi sopimus ja yksi varmenteiden vaihto

Kuulemistilaisuuden työpajassa 26.3.18 esitetyt kommentit

- Teknistä esitystä voisi tarkentaa ja käyttää apuna viestintämateriaalin valmistelussa asiointipalveluille
- Keskusteltiin siitä, kuinka paljon avaintenvaihtoja tulee. Käytännössä yhtä paljon kuin sopimuksia.
- Keskusteltiin osapuolten tunnistamisesta.
 - » Verrattiin, että PSD2 RTS:ssä vaaditaan eIDAS-asetuksen mukaista palvelinvarmennetta.
 - » Keskusteltiin siitä, että olisi yhteisesti sovittu CA luottamusverkostolle. Välityspalvelu – asiointipalvelu –väli olisi eri asia.

Kuulemistilaisuuden työpajassa 26.3.18 esitetyt kommentit

- Keskusteltiin siitä, että asiointipalveluissakin on luotava jatkossa avaimet ja toimitettava julkinen avain luotettavasti välityspalvelulle.
- Todettiin, että olisi hyvä laatia luottamusverkostossa neuvontaa/hyvät käytänteet niistä avaimen luomisen käytännöistä, joilla asiointipalvelu luo oman avaimensa. Neuvonnassa olisi huomioitava, voiko avaimen luoda asiointipalvelun alihankkija vai onko se luotava itse, mitkä ovat luotettavia työkaluja avaimen luomiseen ja miten avain toimitetaan tunnistuspalvelulle. On huomattava, että tunnistusvälityksen avain takaa eheyden ja on siten kriittisempi.
- Viestintävirasto käynnistää nopeasti käytänteen valmistelun ja kutsuu luottamusverkoston toimijat mukaan. Jotkin paikalla olleet toimijat lupasivat toimittaa pohtimiaan vaihtoehtoja käytänteiksi.



eidas@ficora.fi

www.viestintävirasto.fi
