TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Määräys 72 työpajat 2020-2021

Määräys 72 A/2018 M sähköisistä tunnistus- ja luottamuspalveluista

Määräys 72 työpajat 2020-2021
Työpaja 6/7 agenda 12.5.2021 klo 9-11.30

- Yleistä: määräysmuutosten valmistelun viimeiset työpajat
- Keskeiset muutokset tunnistuspalvelun vaatimuksiin määräyksessä (asiat, joista säännösehdotusta ei ole käsitelty työpajoissa aikaisemmin, merkitty kalvoilla ja luonnoksissa)
- Luku 4 tunnistuspalvelun arviointikriteerit
- Luku 2 tunnistuspalvelun tietoturvavaatimukset
  - Tullut yksi ennakkopyyntö käsitellä säännöksiä 8 ja 9 ja osapuolten varmentamista
- Luku 3 Tietojen välittäminen luottamusverkostossa
- Tarve jatkotyöpajalle 20.5.2021?
- Viimeinen työpaja 10.6.2021: koko määräys
  - Määräysluonnos ja perustelumuistioluonnos jaetaan ~3.6.2021

12.5.2021 työpajan osallistujat

- Työpajassa oli paikalla 30 henkilöä seuraavista organisaatioista
- Aktia, Danske Bank, Handelsbanken, Nordea, OP, POP-pankit, S-pankki, Säästöpankit, Ålandsbanken
- Telia, Elisa
- Samlink, Ubisecure, Thales
- FA
- DVV, Fiva, KKV

Työpajat

16.12.2020-10.6.2021

Työtapa

- Työpajat ovat avoimia sidosryhmille
- Kutsu viimeistään 1-2 viikkoa ennen työpajaa viraston sähköpostijakeluilla (luottamusverkosto, eidas-tekninen, eidas-yleinen ”tulu”)
- Kutsun kanssa samaan aikaan jaetaan/julkaistaan viraston valmistelumuistio työpajan aiheesta
- Työpajoissa käydään läpi valmistelumuistion muutosehdotukset ja niiden vaikutusten arviointi
- Viimeisessä työpajassa käydään läpi koko muutettu määräys ja perustelumuistio
- Sidosryhmät voivat koko työn ajan toimittaa kirjallisia kommentteja valmisteluun. Kommenttien julkisuus arvioidaan julkisuuslain mukaisesti.
- Virasto voi pyynnöstä järjestää kahdenvälisiä tapaamisia asioissa, joita ei voi niiden luonteen takia käsitellä julkisessa työpajassa

Määräystyöpajojen aikataulu

Aika	Materiaali	Aihe	Lisätyöpaja (tarvittaessa)
KE 16.12.2020 9-11.30	7.12.2020	Tunnistus: rajapinnat ja attribuutit	KE 3.2.2021 9-11
KE 20.1.2021 9-11.30	11.1.2021	Tunnistus: Salaus, osapuolten varmentaminen ja avaintenvaihto	KE 3.2.2021 9-11
KE 10.2.2021 9-11.30	1.2.2021	Tunnistus: tunnistusjärjestelmän tekniset vaatimukset ja arviointi	~~KE 17.2.2021 9-11~~
KE 10.3.2021 9-11.30	1.3.2021	Tunnistus: tunnistusmenetelmä, PSD2-vertailu Blockchain ja SSI	~~KE 17.3.2021 9-11~~
KE 15.4.2021 9-11.30	1.4.2021	Luottamuspalvelut: palveluiden ja arvioinnin ETSI-standardit	~~KE 21.4.2021 TO 22.4. 9-11~~
KE 12.5.2021	~~**3.5.2021**~~ 4.5.2021	**Tunnistuspalvelun vaatimukset: kooste muutosehdotuksista**	**TO 20.5.2021 9-11**
~~TO 10.6.2021~~ 9-11.30	3.6.2021	Koko määräys ja perustelut	

Jatkoaikataulu – muutokset mahdollisia

- 6-8/2021 virkavalmistelu ja käännökset
- **9/2021 lausuntokierros**
- 10/2021 lausuntokooste, mahdolliset muutokset ja niiden käännökset
- **10/2021 palautetilaisuus lausuntokierroksen tuloksista**
- n. 10 – 12/2021 määräyksen EU-notifointi
- n. 1-2/2022 uusi määräys voimaan

Määräyspäivityksen yleiset linjaukset

Määräyspäivityksen yleiset linjaukset

- Määräyksen perusrakenne ja lukujako säilytetään
- Vaatimuksia ja perusteluja selvennetään ja ajantasaistetaan joiltain osin
- Viraston ohjeet ja suositukset pääpiirteissään samoissa asioissa kuin nyt
- Muutoksia harkitaan: attribuutit, salausvaatimukset ja luottamuspalveluiden standardiviitteiden täydennykset
  - mm. uhkat perusteena
  - Lisäys 10.3.2021: tunnistusmenetelmän turvallisuusvaatimusten tarkentamista harkitaan
  - Lisäys 12.5.2021/valmistelun aikana lisätty seuraavia: tunnistusmenetelmän turvallisuusvaatimukset (6), tunnistustapahtuman lisäinformaatio käyttäjälle (6) ja SSO (6), pseudonymisointi (12), viraston ohjeet tai suositukset referenssiksi rajapintaprofiileille (14) ja vaatimuksenmukaisuuden arvioinnille (15)
- Operatiivisia palveluita ei ole säädetty viranomaiselle tehtäväksi (vrt. .FI)
- PSD2-vaatimuksia tarkastellaan referenssinä tunnistusmenetelmän vaatimusten kohdalla (nostoja toimijoilta tarvitaan)
- Blockchain: tilaisuus käsitellä lohkoketjuteknologian suhdetta tunnistuksen teknisiin vaatimuksiin ja arviointivaatimuksiin

Kommentit työpajassa 12.5.2021

- Kysyttiin, tuleeko määräys voimaan kokonaan 2022 alussa vai onko/voiko olla siirtymäaikoja
- Traficom totesi, että:
  - on pyritty arvioimaan valmistelun yhteydessä, tarvitaanko ja onko perusteita siirtymäajoille
  - näistä on tärkeää saada palautetta ja perusteluja toimijoilta
  - siirtymäaikoja ei ole vielä päätetty

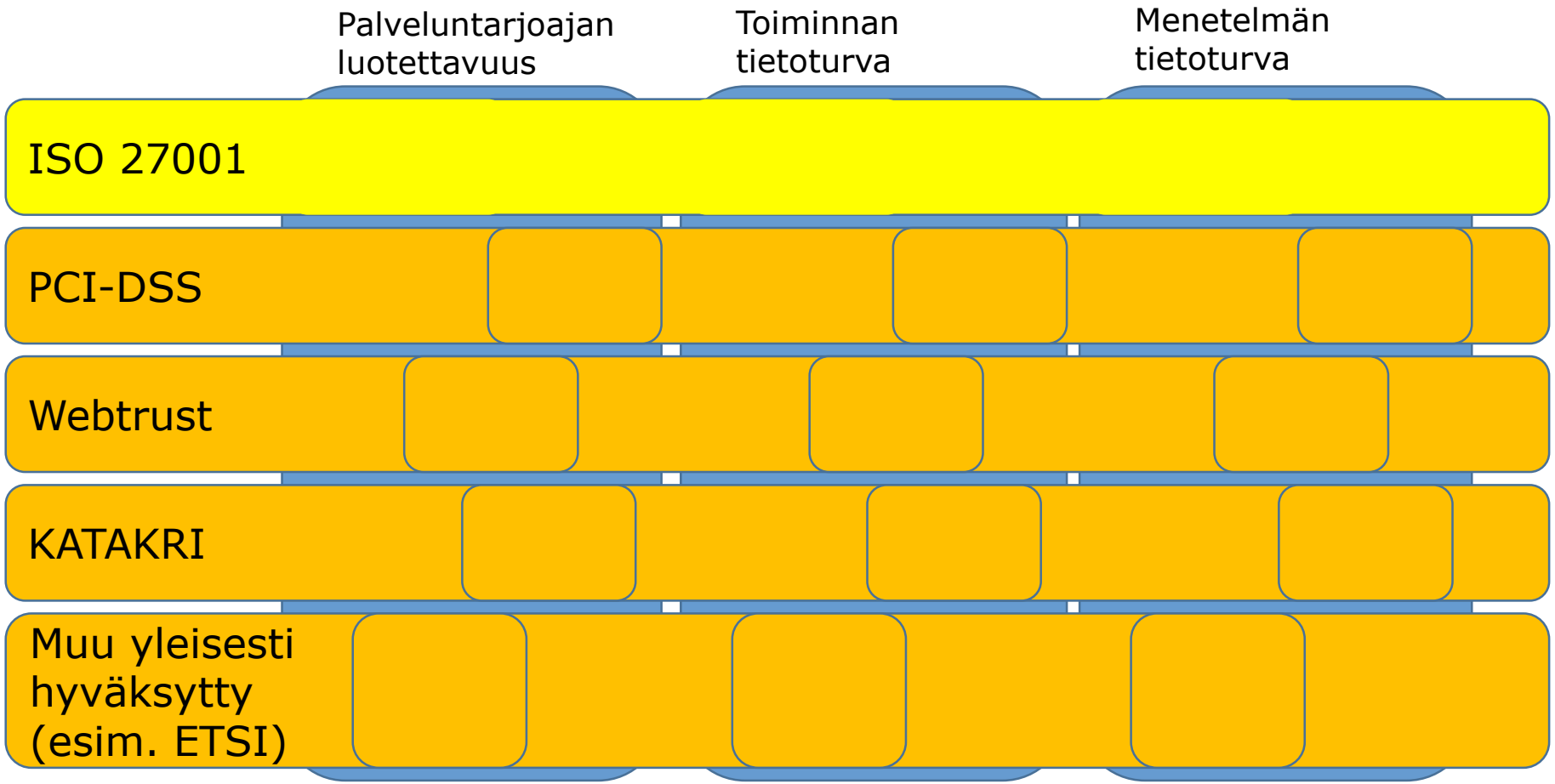
TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

M72 Luku 4
Tunnistuspalvelun arviointikriteerit

Tunnistuspalvelun luotettavuus ja sen osoittaminen

Tunnistuspalvelun tarjoajan luotettavuus Säännös 16	Tunnistusjärjestelmän ja tunnistusmenetelmän luotettavuus ja tietoturvallisuus Säännös 15	Vaatimuksenmukaisuu-den arviointi Säännös 18, 19
Tunnistuspalvelun tarjoajan oma selvitys mm. seuraavista:	**Riippumaton ja pätevä arviointi mm. seuraavista**	**Tunnistuslaissa säädetyt arvioinnin vaatimukset, arviointielimet ja kriteerit**
• Oikeushenkilö, vastuuhenkilöt oikeustoimi- ja liiketoimintakelpoisia • Taloudelliset resurssit, vahinkovastuun kantokyky • Henkilöstöresurssit (24/7, ml. tekninen ja oikeudellinen osaaminen) • Vastuu alihankkijoista • Käyttäjäehdot ja tietosuojaperiaatteet	• Tietoturvallisuuden hallinta (kuten ISO 27001) • Tieto- ja tietoliikennejärjestelmät, ts. tunnistusmenetelmän taustajärjestelmät • Tunnistusmenetelmä ja todentamismekanismi • mm. tietoliikenneturvallisuus, tietojärjestelmäturvallisuus, käyttöturvallisuus, tilaturvallisuus • poikkeamien havainnointi ja hallinta ➢ Tunnistusjärjestelmän ja menetelmän varmuustason mukainen sietokyky tietoturvauhkia vastaan	• Arviointi ennen aloitusilmoituksen tekemistä • Arviointi toiminnan aikana vähintään kahden vuoden välein • Korotetulla varmuustasolla sisäinen tarkastuslaitos tai ulkoinen arviointielin • Korkealla varmuustasolla ulkoinen arviointielin • Arviointikriteerit tarkennettu määräyksellä ja ohjeella

Kalvo v. 2016 Arviointikriteerit – mikään yleisesti käytetty ei yksinään kattane kaikkea



Muutosehdotus
Säännös 15 Vaatimuksenmukaisuuden arviointikriteerit

15.1 Tunnistusjärjestelmän ja tunnistusmenetelmän arvioinnin toiminnot
Tunnistuspalvelun arvioinnin täytyy kattaa vaatimukset, jotka kohdistuvat
1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän)
- *a) tietoturvallisuuden hallintaan*
- *b) tietojen säilyttämiseen*
- *c) tiloihin ja henkilökuntaan*
- *d) teknisiin toimenpiteisiin*
- **[* Ei käsitelty aikaisemmin:]** *e) yhteentoimivuuteen luottamusverkostossa*

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

15.2 Arviointikriteeristö
1. Edellä 15.1 kohdassa mainittujen toimintojen ~~osa-alueiden~~ vaatimuksenmukaisuuden arvioinnin on katettava kaikki ~~perustuttava~~ tunnistus- ja luottamuspalvelulain ja tämän määräyksen vaatimukset.
2. Arviointi voi perustua Liikenne- ja viestintäviraston arviointiohjeeseen tai EU:n tai muun kansainvälisen toimielimen antamiin säännöksiin tai ohjeisiin, julkaistuihin ja yleisesti tai alueellisesti sovellettuihin tietoturvallisuutta koskeviin ohjeisiin tai yleisesti käytettyihin tietoturvallisuusstandardeihin tai menettelyihin. Arviointi voi perustua usean edellä mainitun lähteen yhdistelmään.

Muutosehdotus
Säännös 16 Selvitys tunnistuspalvelun tarjoajan ja julkaistujen tietojen luotettavuudesta ~~muiden vaatimusten täyttämisestä~~

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

1) *julkaistut ilmoitukset ja käyttäjätiedot, kuten tunnistusperiaatteet, sopimusehdot ja hinnastot*

2) **[* Ei käsitelty aikaisemmin:]** *tunnistuspalvelusta vastaava vakiintunut oikeushenkilö* ~~*organisaatio*~~

3) *valmius ottaa vahinkoriskejä*

4) *riittävät taloudelliset varat*

5) *vastuu alihankkijoista*

6) *suunnitelma toiminnan päättämisen varalta*

Perustelut Luku 4 Tunnistuspalvelun arviointikriteerit

- Säännös 15 Vaatimustenmukaisuuden arviointikriteerit
  - Sanamuotojen selkeytys
  - lisätään yhteentoimivuus
  - Lisätään viittaus viraston arviointiohjeeseen
- Säännös 16 Selvitys tunnistuspalvelun tarjoajan ja julkaistujen tietojen luotettavuudesta
  - Sanamuodon selkeytys

Kommentit työpajassa 12.5.2021/15

- Kysyttiin, voisiko arvioinnin kohdistaa tiettyihin osiin tai kohtiin? Auditointia tehdään koko ajan ja se vie aikaa, joten onko tarpeen, että arviointi kohdistuu jokaisella kerralla koko kokonaisuuteen?
  - Traficom: reunaehdot (kuten 2 vuoden väli) tulee lainsäädännöstä. Traficom on pohtinut ja esittänyt neuvontamuistioissa painotuksia.
- Kysyttiin, onko Traficom huomioinut jo komissiolta tulleen tekoälyasetusluonnoksen? Luonnoksessa on myös pakollinen vaatimuksenmukaisuuden arviointi tekoälysovellluksille ja erityisesti korkean riskin tekoälysovelluksille. Korkean riskin sovelluksia olisi esim. biometriikan osalta. Tuleeko vaikuttamaan biometriikkaa hyödyntäviin tunnistusratkaisuihin?
  - Traficomin käsityksen mukaan tekoälyasetusluonnos painottaa hieman eri asioita (esim. valvontaa).
  - Muitakin muutostekijöitä tulevaisuudessa
  - Tällä hetkellä kuitenkin VM:n digihanke meneillään, joka voi tulevaisuudessa aiheuttaa muutoksia usealle osa-alueelle.
  - Määräystä muutetaan tarvittaessa tunnistuslain ja eIDAS-asetuksen mukaisesti.
- Kohta 16 – ei kommentteja

M72 Luku 2
Tunnistuspalvelun tietoturvavaatimukset

M72 Luku 2 Tunnistuspalvelun tietoturvavaatimukset

- Säännös 4 Tunnistuspalvelun tarjoajan tietoturvallisuuden hallinnan vaatimukset
- Säännös 5 Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet
- Säännös 6 Tunnistusmenetelmän tietoturvavaatimukset
- Säännös 7 Tunnistusjärjestelmän ja rajapintojen salausvaatimukset
- Säännös 8 Tietoliikenteen osapuolten varmentaminen
- Säännös 9 Tunnistussanomien eheys ja luottamuksellisuus
- Säännös 11 Tunnistuspalveluntarjoajan häiriöilmoitukset Liikenne- ja viestintävirastolle

Tietoturvallisuuden hallinta

Säännös 4

Muutosehdotus: Säännös 4 Tunnistuspalvelun tarjoajan tietoturvallisuuden hallinnan vaatimukset

4.1 Tietoturvallisuuden hallinnan standardi

Tunnistuspalveluntarjoajan on noudatettava ~~käytettävä~~ tunnistusjärjestelmän tietoturvallisuuden hallinnassa ISO/IEC 27001 -standardia tai muuta yleisesti tunnettua vastaavaa tietoturvallisuuden hallinnan standardia. Tietoturvallisuuden hallinta voi perustua myös useamman standardin yhdistelmään.

4.2 Tietoturvallisuuden hallinnan kattavuus

Tietoturvallisuuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osa-alueet

1) tunnistuspalveluntarjoajan toimintaympäristö kokonaisuutena;

2) tietoturvallisuuden hallinnan johtaminen, organisointi ja ylläpito;

3) tunnistuspalvelun tarjontaan liittyvien tietoturvallisuusriskien hallinta;

4) tietoturvallisuuden resursointi, pätevyys, henkilöstön tietoisuus tietoturvallisuudesta, viestintä ja dokumentointi sekä dokumentoidun tiedon hallinta;

5) tunnistuspalvelun tarjonnan suunnittelu ja ohjaus tietoturvavaatimusten täyttämiseksi; ja

6) tietoturvallisuuden hallinnan tehokkuuden ja toimivuuden arviointi.

Perustelujen täydennykset - Säännös 4.2 …tietoturvallisuuden hallinnan kattavuus

- Yhdenmukaistettu ISO 27001 -viittaukset ja soveltamisohje arviointiohjeen 211/2019 kanssa
- *3) tunnistuspalvelun tarjontaan liittyvien tietoturvallisuusriskien hallinta;*
  - Riskinhallintamallin perustelujen tarkennukset, standardiviitteet/otteet
  - Sama malli koskee säännöksen 6 tunnistusmenetelmän erityisen uhka- ja riskiarvion tekemistä

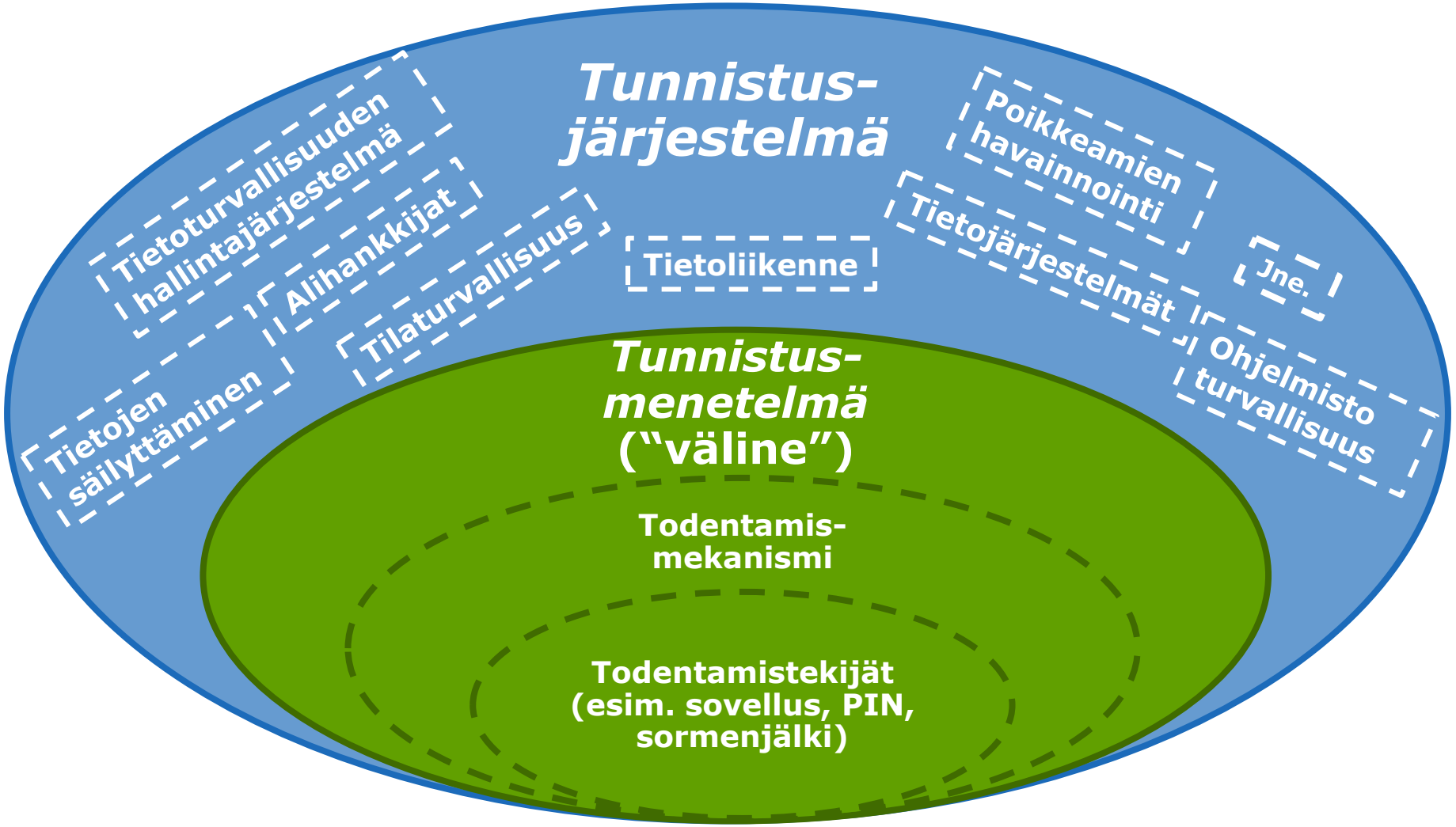
Kommentit työpajassa 12.5.2021/säännös 4

- Ei kommentteja

Tunnistusjärjestelmä

Säännös 5

Tunnistusjärjestelmä ja tunnistusmenetelmä



Muutosehdotus
Säännös 5 Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet

5.1 Tunnistusjärjestelmän turvallisuus ja luotettavuus

Tunnistusjärjestelmän

tietoliikenne, tietojärjestelmät ja niiden käyttö on

suunniteltava, toteutettava ja jatkuvasti ylläpidettävä koko elinkaaren ajan siten, että

tunnistuspalvelun eheys ja luottamuksellisuus on suojattu

tunnistuspalvelun varmuustason mukaista sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.3 tarkoitettua kohtuullisen tai korkean vakavuustason uhkaa ja hyökkäyspotentiaalia vastaan.

Muutosehdotus: Säännös 5 Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet

5.2 Tietoliikenneturvallisuus

Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä

a) verkon rakenteellinen turvallisuus
b) tietoliikenneverkon vyöhykkeistäminen
c) suodatussäännöt vähimpien oikeuksien periaatteilla
d) suodatuksen ja valvontajärjestelmien hallinnointi ~~koko elinkaaren ajan~~
e) turvalliset hallintayhteydet

5.3 Tietojärjestelmäturvallisuus

Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä

a) pääsyoikeuksien hallinta vähimpien oikeuksien periaatteella
b) järjestelmien käyttäjien yksilöity tunnistaminen
c) järjestelmien koventaminen
d) haittaohjelmasuojaus
e) turvallisuuteen liittyvien tapahtumien jäljityskyky- ja jäljitysprosessi
f) poikkeamien havainnointikyky ja korjausprosessi ~~toipuminen~~
g) kansainvälisesti tai kansallisesti suositellut salausratkaisut sen lisäksi, mitä 7 ja 9 kohdassa määrätään

5.4 Käyttöturvallisuus

Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä

a) huolellinen muutosten hallinta
b) tiedon luokitteluun perustuva salassa pidettävän aineiston käsittely-ympäristö ja säilytys
c) etäkäytön ja –hallinnan suojaaminen etäkäyttöympäristön uhkilta
d) ohjelmistokehityksen ja ohjelmistohaavoittuvuuksien hallinta
e) varmuuskopiointi

Ei muutoksia
Säännös 5.5 Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet

5.5 Tunnistusjärjestelmän tuotantoverkon hallinta- ja etäyhteydet

Tuotantoverkko ja sen edellä 5.2.e ja 5.4.c alakohdissa tarkoitetut hallintayhteydet ja etäkäyttö- ja etähallinta on toteutettava siten, että organisaation muiden palveluiden kuten sähköpostin tai web-selailun kautta aiheutuvat tietoturvauhat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvauhat on

a) korotetulla varmuustasolla erityisesti arvioitu ja minimoitu ja

b) korkealla varmuustasolla kokonaisuutena arvioiden estetty.

- Perusteluissa soveltamisohje vuodelta 2016, ei muutoksia

Perustelut säännös 5

- 5.3. g) Vielä pohdittava, miten muotoillaan säännökseen se, että salausratkaisujen oltava laadukkaita myös 5.2 tietoliikenteessä ja 5.4 operoinnissa

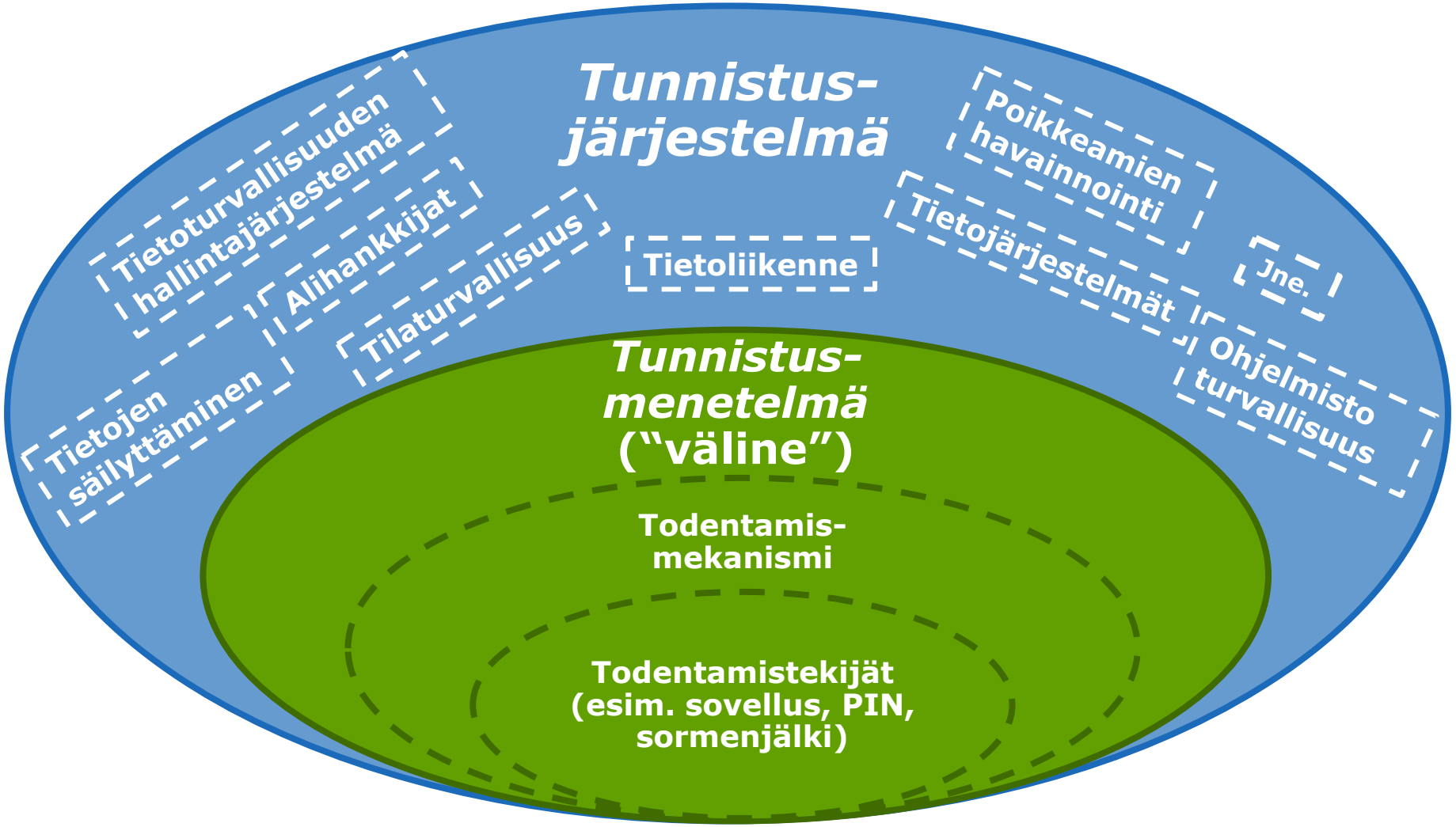
Kommentit työpajassa 12.5.2021/säännös 5

- Ei kommentteja

Tunnistusmenetelmä

Säännös 6

Tunnistusjärjestelmä ja tunnistusmenetelmä



Muutosehdotus: Säännös 6.1 Tunnistusmenetelmän ominaispiirteet ja tekniset turvatoimenpiteet

*1. Tunnistusmenetelmän **todentamistekijät, todentamismekanismi ja turvatoimenpiteet** on suunniteltava, toteutettava ja ylläpidettävä siten, että ne suojaavat menetelmän eheyden ja luottamuksellisuuden vähintään varmuustasoon suhteutetulta hyökkäyspotentiaalilta. Suojautumiskyvyn on perustuttava **uhka- ja riskiarvioon**, jossa arvioidaan erikseen hallussapitoon, tietoon ja ominaisuuteen perustuviin todentamistekijöihin ja todentamismekanismiin kohdistuvat uhkat sekä uhkilta suojaavat turvatoimenpiteet.*

*2. Tunnistusmenetelmän ominaispiirteiden ja turvatoimenpiteiden on estettävä se, että yhden todentamistekijän vaarantuminen vaarantaisi muiden todentamistekijöiden luotettavuuden. Tunnistusmenetelmän turvatoimenpiteillä on **eriytettävä ja suojattava todentamistekijät** erityisesti, jos niitä käytetään samalla päätelaitteella.*

[* Ei käsitelty aikaisemmin:] *3. Tunnistusmenetelmässä ja todentamisessa on käytettävä kansainvälisesti tai kansallisesti suositeltuja **salausratkaisuja**. Tunnistusvälineen ja tunnistusjärjestelmän välisellä tietoliikenneyhteydellä on käytettävä teknisesti soveltuvin osin ja 1 kohdan uhka- ja riskiarviossa edellytetyllä tavalla määräyksen 7 kohdan mukaisia suositeltuja salausratkaisuja.*

Perustelut, säännös 6.1.1 uhka- ja riskiarvio

- Yleiset ja todentamistekijätyyppikohtaiset uhkat
  - Poiminta standardeista ja LOA guidancesta
- Riskiarvio
  - Riskinhallintamalli kuten säännös 4.2 3)
  - Riskin hyväksyttävyys arvioidaan suhteessa hyökkäyspotentiaaliin
- Turvakontrollit
  - Poimittu esimerkkejä kontrolleista
  - 6.1.3 salauksen määrätty keino

Perustelut 6.1.3 salaus tunnistusmenetelmässä

- Tietoliikenne- ja sanomasalaus tunnistuspalveluiden ja luottavan osapuolen välillä säännökset 7 ja 9, myös jos välitys näiden välillä käyttäjän selaimen tai päätelaitteen kautta
- 6.2.3=> kaikki muut tunnistusmenetelmän ja todentamisen/autentikoinnin salausratkaisut
- Yleisesti luotettavaksi tunnettuja salausmenetelmiä täytyy käyttää tunnistusvälineeseen liittyvien
  - haltijakohtaisten salaisuuksien luomisessa ja ylläpidossa,
  - haltijakohtaisen salaisuuden (yleensä yksityisen avaimen) suojaamisessa päätelaitteessa tai taustajärjestelmässä
  - ylipäätään kaikissa tunnistusmenetelmän eheyteen ja luottamuksellisuuteen vaikuttavissa toiminnoissa
- Määräyksen säännöksen 7 mukaiset tietoliikenteen salausvaatimukset koskevat
  - käyttäjän hallinnassa olevan tunnistusvälineen ja tunnistusjärjestelmän välistä tietoliikennettä eli tunnistusvälineen haltijan autentikointia siltä osin, kuin sanomia eivät koske säännöksen 9 vaatimukset sanomien suojaamisesta. Verrattuna säännöksessä 9 määrättyyn sanomien salaamiseen säännöksessä 6.1.3 tarkoitetaan esimerkiksi niitä haaste-vaste -sanomia, joita todentamisessa käytetään tunnistusvälineen haltijan ja tunnistusvälineen tarjoajan järjestelmän välillä.
  - Esimerkkinä arviointiohjeesta 211/2019 voi poimia hard fail certificate pinningin mobiilisovelluksen sovelluksen ja taustajärjestelmän välillä

Kommentit työpajassa 12.5.2021/säännös 6.1

- Siirtymäaika riskiarviolle – ennakkokommentit, että ei tarvita
- Kysyttiin 6.1 kappaleen kolmannesta alakohdasta, joka tuli uutena määräykseen. Onko tarpeen käsitellä määräyksessä näin syvällisesti tekniikkaa, kuten kohdassa 7?
- Kommentoitiin salausratkaisujen vaatimuksia ja epäsymmetrisiä salausalgoritmeja
  - Traficomin käsityksen mukaan epäsymmetriset salausalgoritmit ovat edelleen käytössä
- Keskusteltiin siitä, mikä olisi vaihtoehtona epäsymmetrisille? Yleisenä mielipiteenä, että epäsymmetriset salausalgoritmit ovat edelleen päteviä, Traficomilla on omat kansalliset suositukset, jossa ne hyväksytään. Ei nostettu esiin lähdettä, joka osoittaisi että tilanne kehittymässä toiseen suuntaan
- Traficomin mukaan määräyksen ei ole tarkoitus esittää yksityiskohtaista poissulkevaa listaa asiasta.

Muutosehdotus
Säännös 6.2 Erityiset turvatoimenpiteet

*1. Tunnistuspalvelun on näytettävä tunnistusvälineen käyttäjälle tunnistustapahtumassa tieto, jonka perusteella käyttäjä voi yhdistää tunnistusvälineeseen saamansa vahvistuspyynnön asiointitapahtumaan (**session binding**). Tieto on näytettävä vain sellaisessa tunnistusmenetelmässä, jossa se on teknisesti mahdollista.*

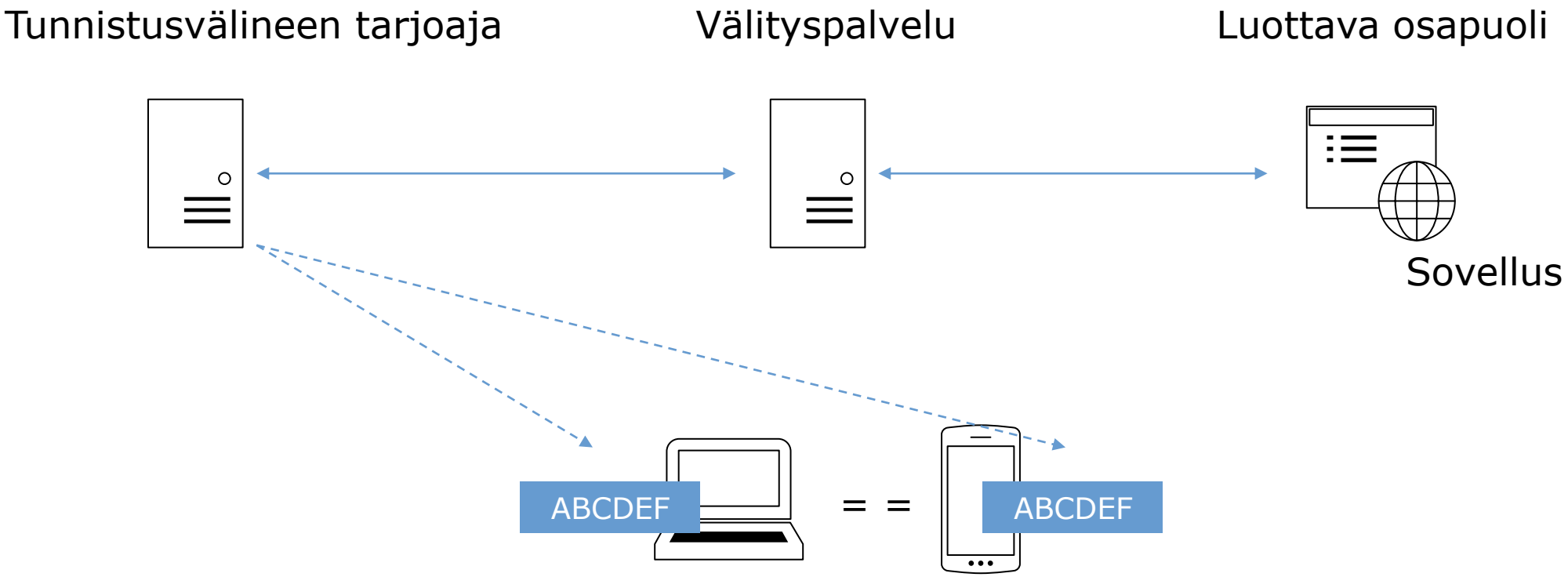
*2. Tunnistuspalvelun on näytettävä tunnistusvälineen käyttäjälle tunnistustapahtumassa **tieto luottavasta osapuolesta**, jolle tunnistus välitetään. Tieto on näytettävä vain sellaisessa tunnistusmenetelmässä, jossa se on teknisesti mahdollista.*

***[* Ei käsitelty aikaisemmin:]** 3. **Kertakirjautumisella** tarkoitetaan tässä määräyksessä sitä, että tunnistuspalvelu tarjoaa useammalle kuin yhdelle luottavalle osapuolelle vahvistuksen yhden vahvalla sähköisellä tunnistusmenetelmällä tehdyn tunnistusvälineen haltijan todentamisen perusteella. Tunnistuspalvelun on kertakirjautumisen suunnittelussa, toteutuksessa ja ylläpidossa huolehdittava 2 alakohdan mukaisten **luottavien osapuolten** tietojen näyttämisestä sekä kertakirjautumiseen liittyvien **istuntojen keston, siirtämisen ja lopettamisen hallintaan perustuvista turvatoimenpiteistä** .*

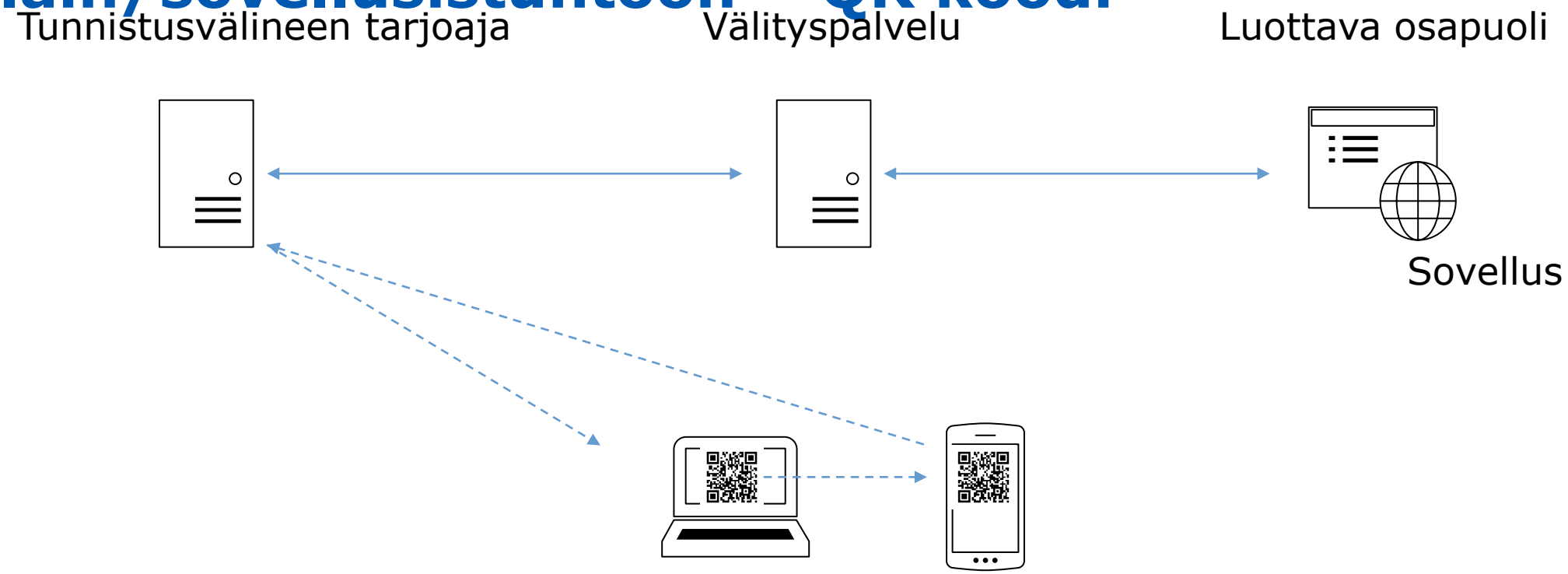
Perustelut, 6.2.3 SSO

- Ei vaadita: 6.2.1 tunnistustapahtuman/asiointitapahtuman tiedon (istuntotunniste, session binding)
- Vaaditaan: 6.2.2 luottavan osapuolen nimi
- Vaaditaan turvallisuuden ylläpito/perustelut:
  - Kertakirjautumisen turvallinen ylläpito edellyttää, että istunnon enimmäiskestolle määritellään riskiarvioon perustuva raja.
  - Kertakirjautumisen/federoinnin tulee olla ennalta suunniteltua ja sen hyödyntämisestä tulee sopia luottavien osapuolten kanssa.
  - Tunnistuspalvelutarjoajan vastuulla on varmistua siitä, että luottava osapuoli kykenee teknisesti toteuttamaan kertauloskirjautumiseen vaadittavan pyynnön tunnistuspalvelutarjoajalle. Kertauloskirjauspyynnön perusteella on viivytyksettä suljettava kerralla kaikki tunnistukseen liittyvät istunnot ja mitätöitävä tokenit. On syytä huomioida tarvittaessa myös luottavien osapuolten mahdollisesti pyytämä ja edellyttämä tunnistamisen varmuustaso.
- Muut ohjauskeinot
  - Kertakirjautumiseen on liittynyt paljon oikeudellisia tulkintakysymyksiä ja tekniseen toteuttamiseen ja turvallisuuteen liittyvää tiedonvaihtoa. Virasto on antanut asiassa neuvontaa tulkinnoista ja teknisiä seikkoja on työstetty yhdessä tunnistuspalveluiden kanssa. Tämä työ jatkuu ja virasto harkitsee työn edetessä tarkoituksenmukaiset ohjauskeinot. Tunnistuspalveluiden eriävien näkemysten takia lähinnä viraston ohje, suositus tai [illegible]lkintalinjaukset näyttävät tarkoituksenmukaisilta.

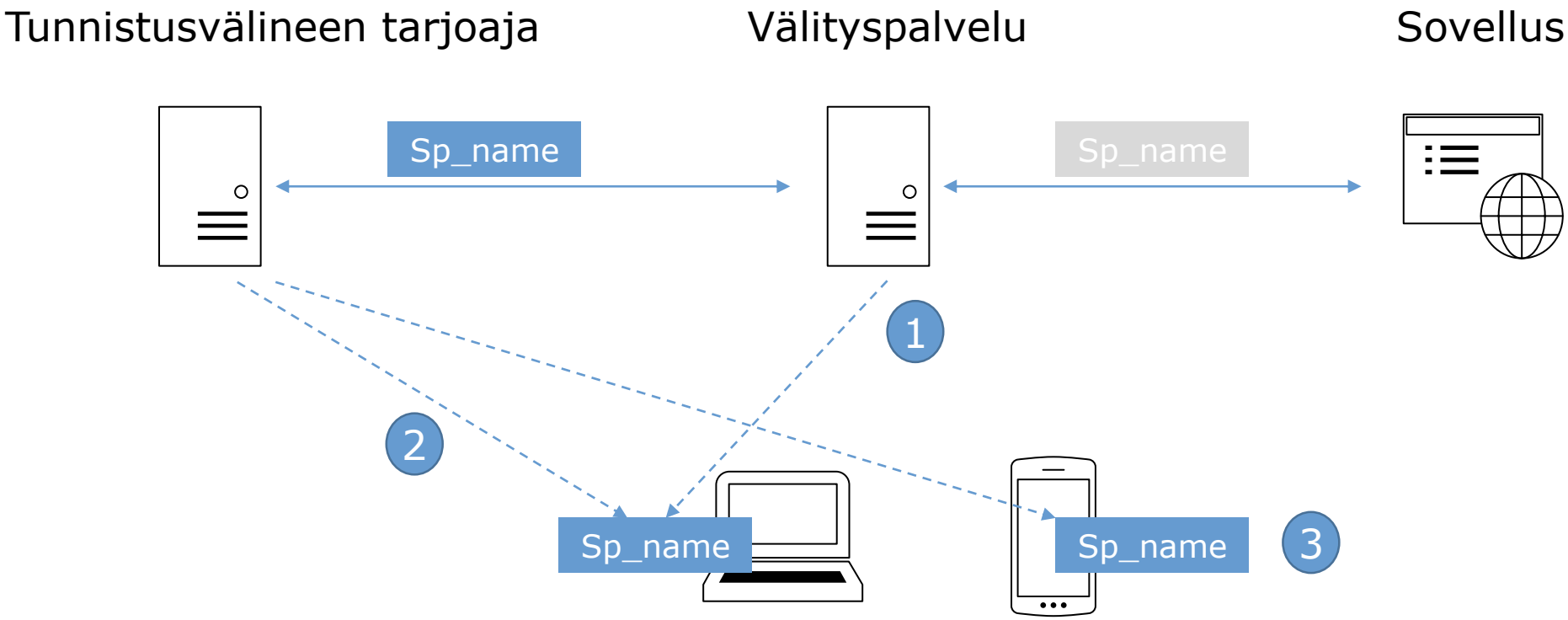
LISÄTTY KUVA 20.5.
6.2.1: Tunnistuksen sitominen selain/sovellusistuntoon - merkkijono



LISÄTTY KUVA 20.5.
6.2.1: Tunnistuksen sitominen selain/sovellusistuntoon – QR koodi



LISÄTTY KUVA 20.5.
6.2.2: SP name

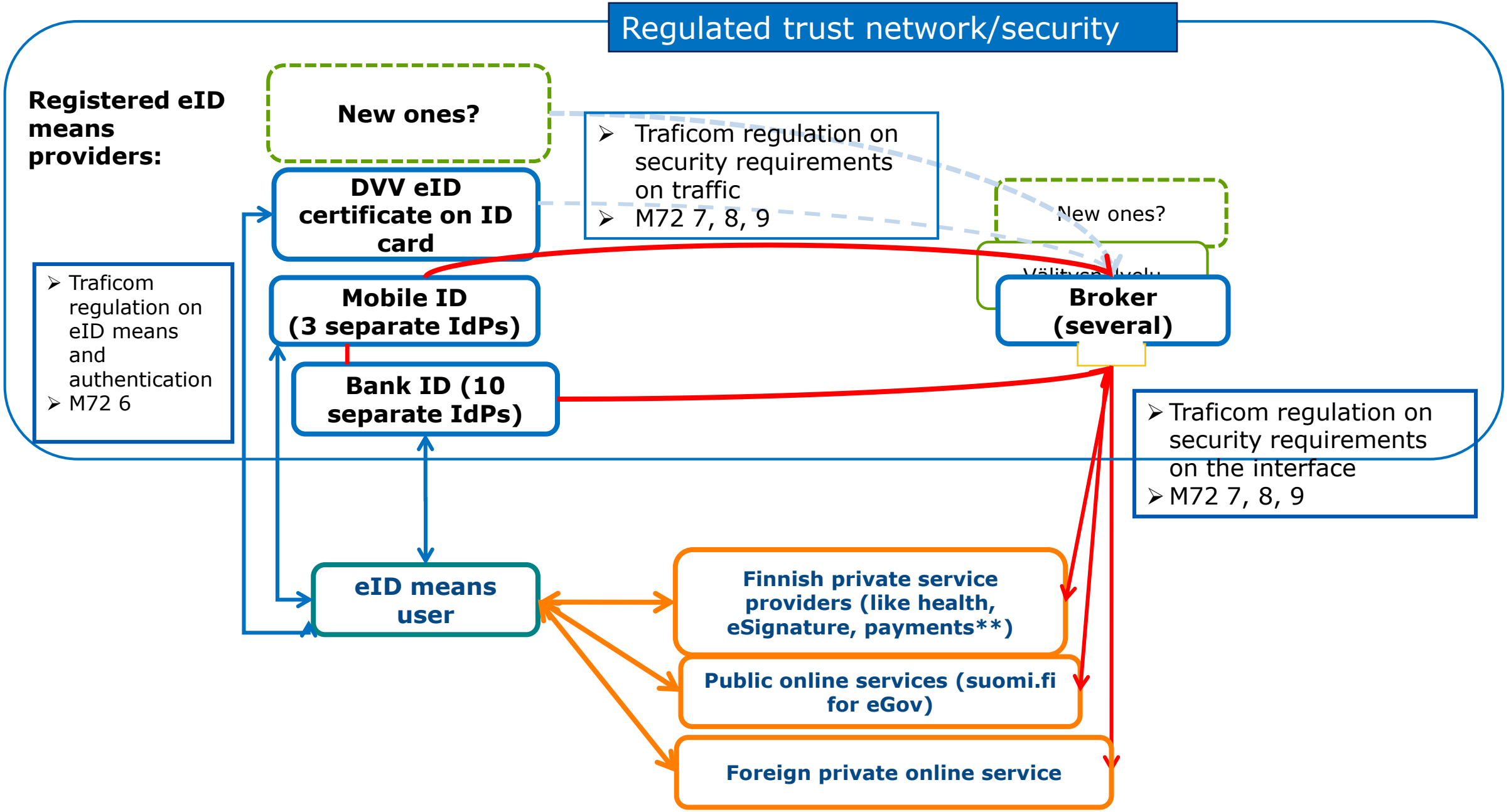


Kommentit työpajassa 12.5.2021/säännös 6.2

- Kysyttiin, onko kohdassa 1 huomioitu OIDC suositukset? Muuten jää tunnistuspalveluiden tarjoajien ja välityspalveluiden keskenään sovittavaksi?
  - Traficomin mukaan suositukset ja arviointikriteeristöt uusittava myös määräysuudistuksen myötä.
- Kysyttiin, onko kustannusten ja todellisten hyötyjen suhdetta pohdittu?
  - Kommenttina: eikö mobiilivarmenteessa ole ollut session binding -koodi jo pitkään? Ja myös joillakin pankeilla?
- Kysyttiin, kenen tehtäväksi tulee valvoa sitä, mitä palvelunimiä käytetään ja näytetään?
  - Traficomin mukaan tunnistusvälityspalvelun tehtävä.
- Kysyttiin kohdasta 2: Määritelläänkö jossain tarkemmin se, mitä on tarpeen näyttää? Pitääkö näyttää välityspalvelu? Missä järjestyksessä? Mikä on olennaisin tieto? Muuten riskinä ristiriitaiset tulkinnat siitä, miten käyttöliittymän pitäisi toimia.
  - Traficomin mukaan käytäntöjä voidaan käsitellä luottamusverkoston yhteistoimintaryhmässä..
- Lisätyöpajassa 20.5 toivottiin havainnollistavia kuvia lisää, tapahtumajärjestyksessä

Salaus

Säännökset 7, 8 ja 9


Regulated trust network/security
Registered eID means providers:
New ones?
DVV eID certificate on ID card
Mobile ID (3 separate IdPs)
Bank ID (10 separate IdPs)
Traficom regulation on security requirements on traffic
M72 7, 8, 9
Traficom regulation on eID means and authentication
M72 6
New ones?
Broker (several)
Traficom regulation on security requirements on the interface
M72 7, 8, 9
eID means user
Finnish private service providers (like health, eSignature, payments**)
Public online services (suomi.fi for eGov)
Foreign private online service

Muutosehdotus Säännös 7.1 Tietoliikenteen salaus

7.1. Tunnistuspalveluntarjoajien välisten ja tunnistuspalveluntarjoajan ja luottavan osapuolen asiointipalvelun välisten rajapintojen liikenne on salattava. Salauksessa, avaintenvaihdossa, varmenteissa sekä salaukseen liittyvässä allekirjoituksessa on noudatettava seuraavia menetelmiä:

1) Avaintenvaihto: Avaintenvaihdossa on käytettävä DHE-menetelmiä tai elliptisiä käyriä käyttäviä ECDHE-menetelmiä. Laskutoimituksissa käytetyn äärellisen kunnan (finite field) koon tulee olla DHE-menetelmässä vähintään 2048 bittiä ja ECDHE-menetelmässä vähintään 224 bittiä.

2) Allekirjoitus tai epäsymmetrinen salaus: Käytettäessä RSA:ta sähköiseen allekirjoitukseen tai salaukseen, avaimen pituuden tulee olla vähintään 2048 bittiä. Käytettäessä elliptisen käyrän menetelmiä ECDSA:ta tai EdDSA:ta alla olevan äärellisen kunnan koon tulee olla vähintään 224 bittiä.

3) Symmetrinen salaus: Salausalgoritmin on oltava AES, tai Serpent tai ChaCha20. Avaimen pituuden tulee olla vähintään 128 bittiä. Salausmoodin on oltava CBC, CCM, GCM, ~~XTS~~ tai CTR.

4) Tiivistefunktiot: Tiivistefunktion tai autentikaatiokoodin on oltava SHA-2, SHA-3, Whirlpool tai Poly1305. ~~SHA-2:lla tarkoitetaan funktioita SHA224, SHA256, SHA384 ja SHA512.~~

- jatkuu

Muutosehdotus Säännös 7.1 Tietoliikenteen salaus

7.1.1 5) Edellä kohdissa 1-4 mainittujen lisäksi voidaan noudattaa menetelmiä ja arvoja, jotka on arvioitu turvallisiksi mainituissa kohdissa tarkoitettuun käyttöön seuraavien asiakirjojen ajantasaisissa versioissa:

a) Liikenne- ja viestintävirastossa toimivan salaustuotteiden hyväksyntäviranomaisen (Crypto Approval Authority) ohje Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset turvallisuusluokat (Dnro 190/651/2015), tai

b) eräiden Euroopan unionin tai ETA-alueen jäsenvaltioissa toimivien sertifiointielinten välisen SOGIS-MRA (Senior Officers Group for Information Systems, Mutual Recognition Agreement) asiakirja SOG-IS Crypto Evaluation Shceme Agreed Cryptographic Mechanisms.

2. Salausasetukset tulee teknisesti pakottaa edellä lueteltuihin vähimmäistasoihin, jotta yhteyskättelyissä ei päädyttäisi vähimmäistasoja heikompiin asetuksiin.

Kommentit työpajassa 12.5.2021/säännös 7.1

- Kysyttiin: Kuvausten mukaan avaintenvaihdossa voidaan käyttää epäsymmetristä salausta, mutta ristiriita 2K ja 3K välillä? Onko vaatimuksena 128-bittinen, jolloin ei voida heikommalla vaihtaa salausavaimia?
  - Traficom: Linjattu ja perustelumuistiossa todettu, että 112 bitin vahvuus riittää, eli kaksikiloinen RSA riittää.
- Todettiin, että kohta 5. on erittäin hyvä, koska viitataan ulkopuolisiin suosituksiin. Kysyttiin kuitenkin, onko määräys oikea paikka määritellä näin tarkasti kryptoalgoritmit ja cypherit, kun on kuitenkin olemassa myös erilliset tekniset työryhmät?
  - Traficom: asia käsitelty ja perusteltu aiemmin. Ei muuteta.

Muutosehdotus Säännös 8 Tietoliikenteen osapuolten varmentaminen ~~turvavaatimukset tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa~~

8.1 Tietoliikenneyhteyden osapuolten tunnistaminen

Tunnistuspalveluiden välisessä sekä

tunnistuspalvelun ja luottavan osapuolen välisessä

tietoliikenneyhteyden perustamisessa

on todennettava tietoliikenteen tai sanomien salaamisessa käytettävien varmenteiden ja avainten aitous ja eheys sekä niiden haltijat.

Todentamisen on perustuttava

[* Ei käsitelty aikaisemmin:] *eIDAS-asetuksen mukaiseen hyväksyttyyn sähköiseen allekirjoitukseen tai hyväksyttyyn sähköiseen leimaan*

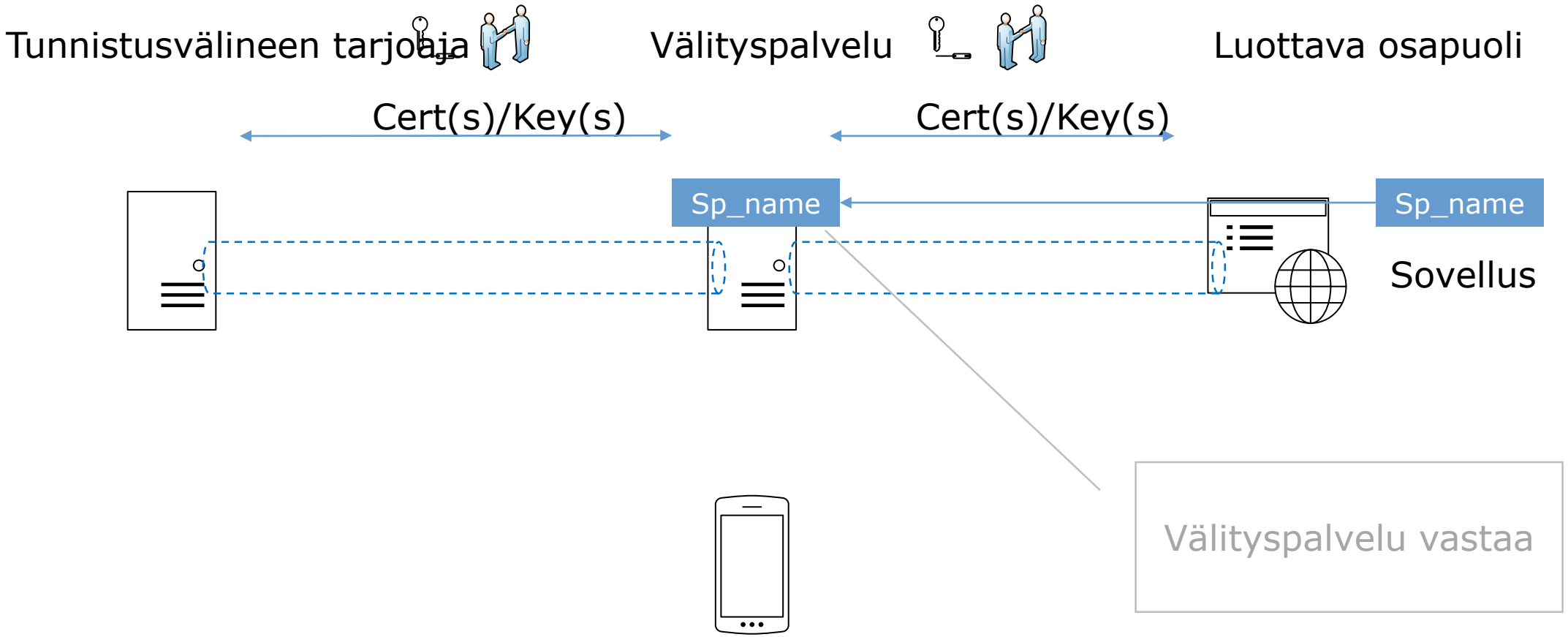
taikka suoraan kahdenväliseen menettelyyn

eikä se voi perustua pelkästään osapuolen yleisesti luotettuun varmenteeseen.

Perustelut säännös 8.1

- Vaatimukset ovat samat luottamusverkoston toimijoiden välillä ja tunnistuspalvelun ja luottavan osapuolen eli asiointipalvelun välillä. Luottavan osapuolen todentaminen on yksi olennainen keino suojata tunnistusvälineen käyttäjää petollisten tunnistuspyyntöjen vahvistamiselta.
- Hyväksytty sähköinen allekirjoitus tai leima ok
- *Suora kahdenvälinen menettely* määräyksessä tarkoittaa sitä, että osapuolen varmenne ja salausavaimet on toimitettava siten, että haltijasta voidaan nimenomaisesti varmistua.
- Kahdenvälisen menettelyn vaatimus merkitsee voimassa olevan vaatimuksen tiukentamista.
- Määräyksessä ei oteta tyhjentävästi kantaa menettelyn yksityiskohtiin ja siihen, mikä on riittävä tapa tunnistaa toinen osapuoli.
  - Esimerkiksi vahvan sähköisen tunnistamisen käyttäminen on hyvä käytäntö.
  - Toimijoiden välillä tehdään aina sopimus, joten käytännön toimet on mahdollista yhdistää sopimusprosessiin.
- Virasto katsoo, että muutoin varmenne ei sinänsä osoita, että sen varmentama avain-pari on oikealla haltijalla.

LISÄTTY KUVA 20.5.
8.1: Avaintenvaihto - perustaminen



Kommentit työpajassa 12.5.2021/säännös 8.1

- Kommentoitiin, että vaikea toteuttaa käytännössä, vaatii manuaalista työtä osapuolten välillä ja se aiheuttaa häiriöitä ja kustannuksia. Päivityksiä on tiheästi, aiheuttaa kustannuksia.
- Kommentoitiin, että sähköisiä allekirjoituksia tai leimapalveluita ei juuri taida olla käytössä paitsi DVV:llä. Turvasähköpostikaan ei käy, eli joudutaanko hakemaan käyntiasioinnilla avaimet paperilla?
- Lisätyöpajassa 20.5 kommentoitiin, että aiheuttaa vaikutuksia varsinkin avaintenvaihdossa asiointipalveluiden suuntaan. Prosesseihin vaikuttaa se, että palveluita on ulkoistettu ja joudutaan antamaan neuvontaa
- Lisätyöpajan 20.5 johtopäätöksenä, että avaintenvaihdossa perustamisvaihe ei ole erityisen ongelmallinen, vaan vaikutukset kohdistuvat päivittämiseen.

Muutosehdotus Säännös 8.2 Varmenteiden ja avainten uusiminen

Edellä kohdassa 8.1 tarkoitetut varmenteet ja avaimet on uusittava säännöllisesti joko:

a) 8.1 kohdan mukaisella menettelyllä,

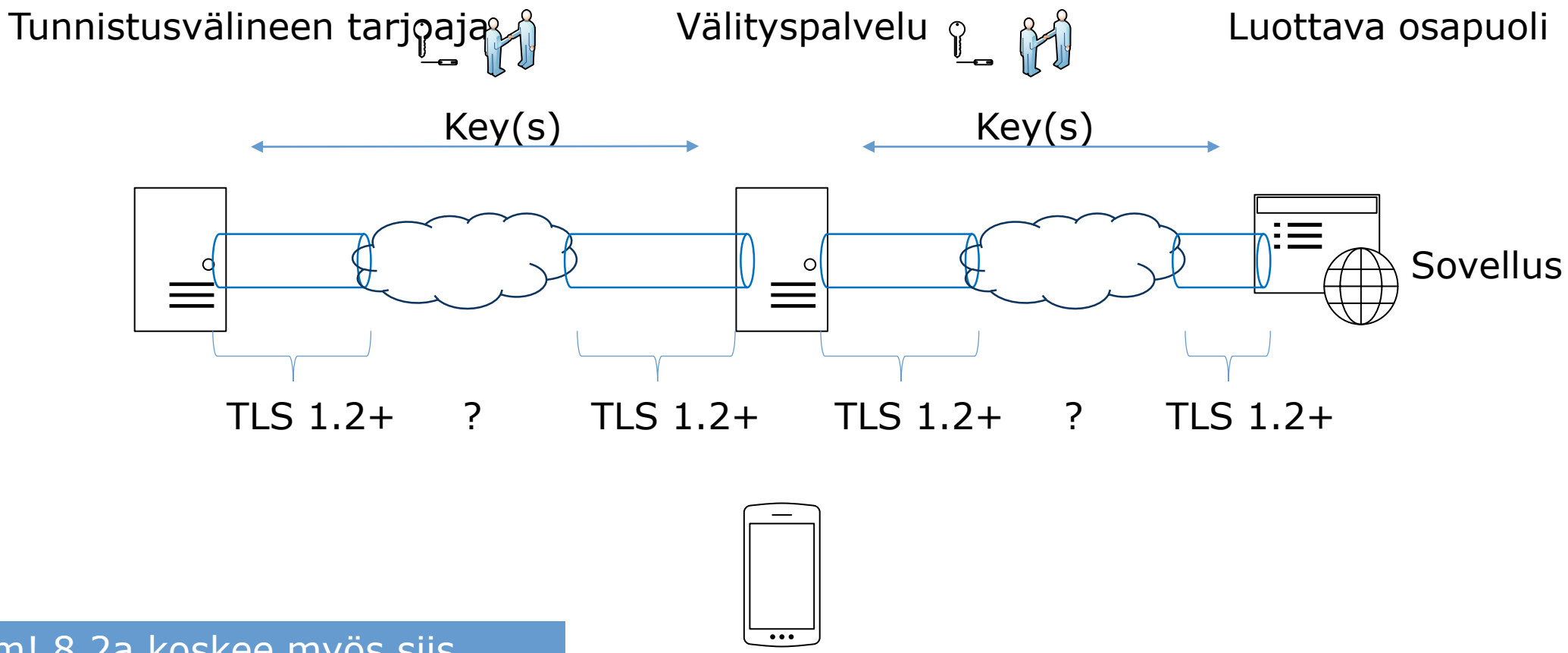
b) allekirjoittamalla uudet avaimet 8.1 kohdan mukaisesti toimitetulla avaimella tai

c) toimittamalla uudet avaimet tietoliikenneyhteydellä, jonka eheys ja luottamuksellisuus on varmistettu sitomalla osapuolten tietoliikenne kohdan 8.1 mukaisesti toimitettuihin varmenteisiin tai avaimiin (certificate pinning tai key pinning).

Perustelut 8.2

- *Yhteenveto säännöksen 8.2 teknisestä soveltamisesta.* Virasto arvioi, että ainakin seuraavat standardin mukaiset vaihtoehdot ovat käytettävissä.
  - Sanomatason salausvaatimus ja kohdan 8.1 mukainen salausavainten vaihto, jos käytössä on TLS suojattu yhteys, jossa ei ole käytössä certificate tai key pinning.
  - käytössä on TLS suojattu yhteys, jossa 8.1 mukainen certificate pinning (tietty palvelinvarmenne) tai key pinning, tällöin sanomatason salaus ei ole pakollista ja salausavaimen vaihto voidaan automatisoida (JWKS, ja avainrotaatio)
  - Sanomatason salausvaatimus on aina voimassa silloin kun tunnistusviestit kierrätetään käyttäjän selaimen tai päätelaitteen kautta (esim. SAML front-channel)

LISÄTTY KUVA 20.5.
8.2a sanomatason salaus- ja allekirjoitusavainten uusiminen (JWKS) – ilman pinnausta



Huom! 8.2a koskee myös siis pinnausvarnteiden/avainten uusimista

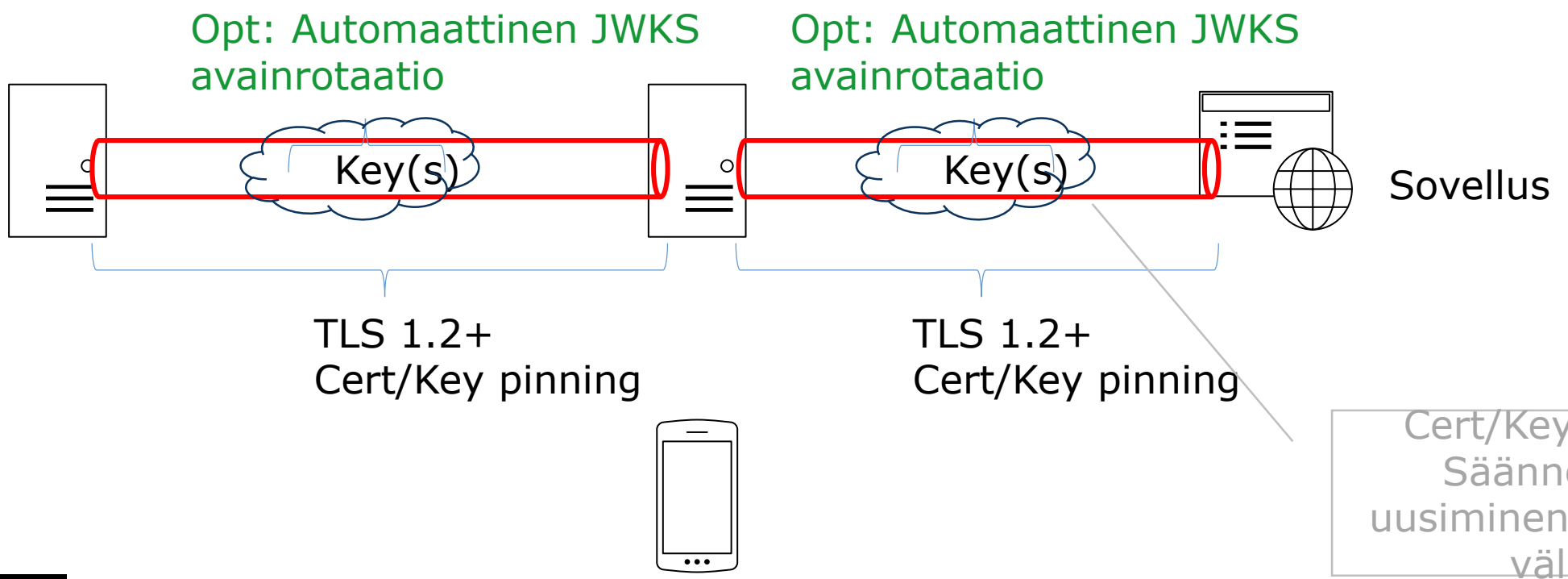
LISÄTTY KUVA 20.5.
8.2b (*certificate pinning, key pinning, mTLS* tms.) sanomatason salaus- ja allekirjoitusavainten uusiminen – JWKS rotaatio (OIDC)

JWKS rotation
Uusiminen automaattisesti esim. 2kk välein

Tunnistusvälineen tarjoaja

Välityspalvelu

Luottava osapuoli



Cert/Key pinning
Säännöllinen uusiminen X vuoden välein

Kommentit työpajassa 12.5.2021/säännös 8.2

- Kommentoitiin varmennevaihtoehtoja ja teknisiä seikkoja
- voisiko käyttää itse allekirjoitettuja varmenteita.
- EV-varmenteet myös vain vuoden voimassa, jolloin ollaan takaisin päivityskysymyksessä.
- Viitattiin SAML ja OIDC-standardien perusmenettelyihin, joissa esim. varmenne on ”vain kääre avaimen kuljettamiseen”.
- OIDC:Ssa mahdollista vaihtaa avaimia luotteulla varmenteella allekirjoittamalla.

- Kommentoitiin, että voidaan käyttää mTLS:ää
- Kommentoitiin edelleen, että jos yleisesti internetissä luotettuun varmenteeseen ei saa luottaa avaintenvaihdossa, miten todentamisvaatimukset suhtautuvat esim. turvasähköpostiin
- Lisätyöpajassa 20.5 kommentoitiin vastuun jakautumista ja sitä, joudutaanko toteuttamaan kumppanikohtaisesti erilaisia sääntöjä. Pohdittiin myös, miten avainten vaatimukset vaikuttavat, avaimia ei vaihdeta tarpeeksi usein, jos se on liian työlästä
- Siirtymäaika pohdittavaksi

Muutosehdotus Säännös 9 Tunnistussanomien eheys ja luottamuksellisuus ~~Tietoturvavaatimukset asiointipalvelurajapinnassa~~

9.1 Sanomien suojaaminen tunnistuspalveluiden ja luottavan osapuolen välillä

1. Tunnistuspalveluiden välisessä ja tunnistuspalvelun ja luottavan osapuolen välisessä tietoliikenteessä on suojattava henkilötietoja sisältävien tunnistussanomien eheys ja luottamuksellisuus joko:

a) varmistamalla tietoliikenneyhteyden eheys ja luottamuksellisuus sitomalla osapuolten tietoliikenne kohdan 8 mukaisesti toimitettuihin varmenteisiin tai avaimiin (certificate pinning tai key pinning) tai

b) salaamalla ja allekirjoittamalla sanomat kohdan 8 mukaisella menettelyllä toimitetulla avaimella.

[* Ei käsitelty aikaisemmin:] *2. Tunnistusvälityspalvelun ja luottavan osapuolen välisessä tietoliikenteessä tunnistusanomat on todennettava allekirjoittamalla .*

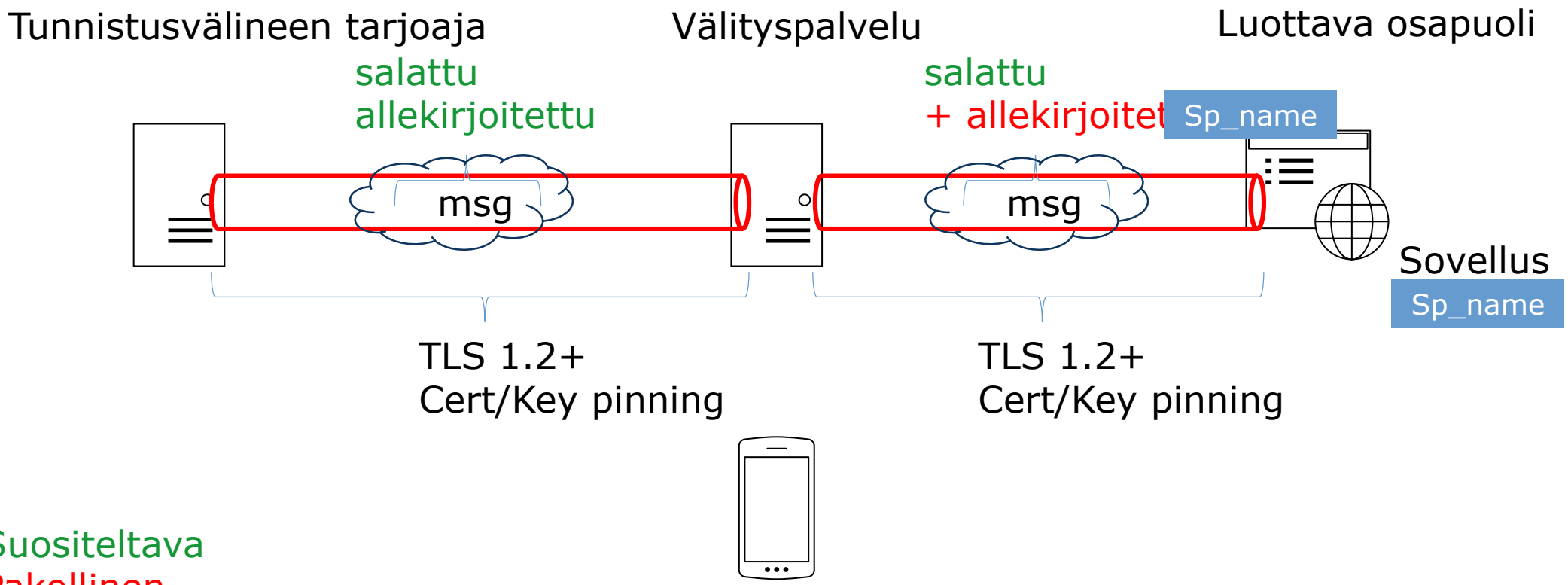
9.2 Sanomien suojaaminen käyttäjärajapinnassa

Jos tunnistussanomat välitetään käyttäjän selaimen tai päätelaitteen kautta, sanomat on salattava ja allekirjoitettava 9.1.b alakohdan mukaisesti.

Perustelut säännös 9

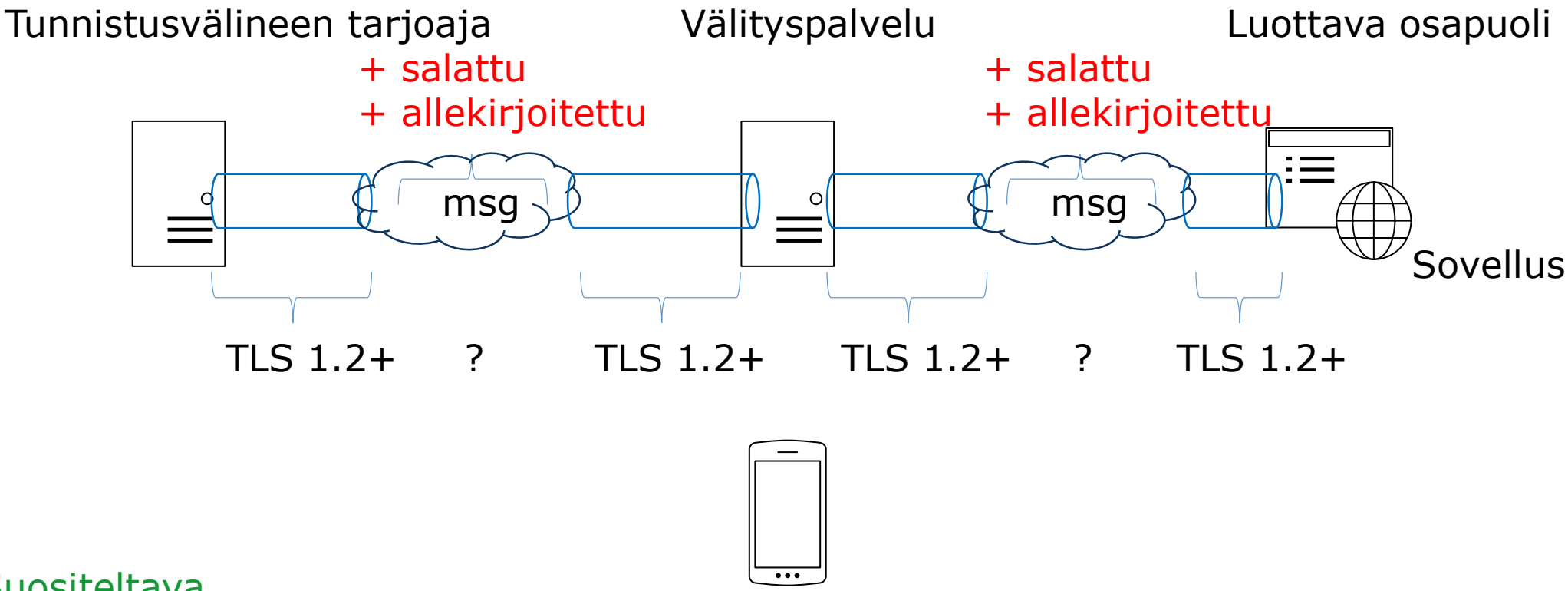
- *Henkilötiedot*. Henkilötiedoiksi katsotaan yleisen tietosuojasääntelyn kannalta kaikki tiedot, jotka ovat suoraan tai välillisesti yhdistettävissä henkilöön eli myös esim. pseudonyymit tai transaktiotunnisteet, jotka ovat eri lähteistä koottuna/yhdistettynä yhdistettävissä henkilöön.
- 9.1 a) alakohdan mukaan tunnistussanomien eheys ja luottamuksellisuus voidaan toteuttaa varmistamalla tietoliikenneyhteyden eheys ja luottamuksellisuus sitomalla osapuolten tietoliikenne molemmissa päissä säännöksen 8 mukaisesti toimitettuihin varmenteisiin. Tällöin pystytään varmistamaan päästä-päähän sekä tietoliikenneyhteyden molempien päiden varmenteen luotettavuus ja se, että liikennettä ei pureta muualla kuin osapuolten tunnistuspalvelun tuottamiseen liittyvissä järjestelmissä.
- 9.1 b) vastaa nykyistä määräystä
- Uusi: 9.1.2, sanomien allekirjoitus, Tarkoitus on todentaa se, että luottavan osapuolen tunnistuspyyntö tulee oikealta järjestelmältä ja todentaa luottavan osapuolen nimen ilmaiseva SPname -attribuutti, joka säännöksen tunnistusvälityspalvelun tarjoajan on säännöksen 12.1 mukaan varmennettava.

Lisätty kuva 20.5.
9.1.1a: Sanomatason salaus ja allekirjoitus – pinnattu TLS



Suositeltava
Pakollinen

Lisätty kuva 20.5.
9.1b: Salaus ja allekirjoitus – ei pinnausta



Suositeltava
Pakollinen

Kommentit työpajassa 12.5.2021/säännös 9.1 ja 9.2

- 8 ja 9 yhdistettyä keskustelua
- Kommentoitiin, että iso riski siihen, että avaintenvaihtoväli tulee pidentymään, koska vaihto on hankala. Aiheuttaa myös ohjelmistomuutoksia kaikilla osapuolilla.
- Sanomatason avaintenvaihdosta on puhuttu paljon OIDC -työryhmässä. Ei ole sanomatasollakaan löydetty konsensusta. Jos viedään sama keskustelu tietoliikenteen suojaamisen tasolle, johtaa siihen, että toteutukset sovitaan kahdenvälisesti. Nyt sekoitetaan eri tasojen suojausta ja salausta keskenään. Miten näistä sovitaan.
  - Traficom toteaa, että riittää TLS tai sanomataso. Ajatuksena on se, että pitäisi olla muutakin, kun yleisesti internetissä luotetut CA:t. Ne eivät ole tarpeeksi luotettavia.
- Kysyttiin, voisiko Traficom perustaa oman CA:n?
- Kommentoitiin, että arvioitava, onko tekniikka vai ihminen (manuaalinen työ) luotettavampi. Kuinka luotettavia ovat manuaaliset prosessit, jos niistä ei ole yhteistä konsensusta verrattuna siihen, että käytetäisiin standardin menetelmiä?
- Kysyttiin, mikä on se uhka, jolta tässä suojaudutaan ja onko tämä ainoa keino? Avaako tämä muita uhkia ja mikä on kokonaisuhkatason kannalta lopulta paras tapa toimia? Pitäisi ensin varmistaa edes nykyisen tason saavuttaminen kaikkien toimijoiden kesken.

Muutosehdotus Säännös 9.3 Salausalgoritmit ja menettelyt

Sanomien salaamisessa ja allekirjoittamisessa on käytettävä soveltuvin osin 7.1 kohdan mukaisia menettelyjä.

~~*Tunnistusvälityspalvelun tarjoajan ja asiointipalvelun välisen rajapinnan tulee täyttää edellä 7 §:n 1 - 4 momentissa määrätyt vaatimukset.*~~

Kommentit työpajassa 12.5.2021/säännös 9.3

- Ei kommentteja

Häiriöilmoitus

Säännös 11 Tunnistuspalveluntarjoajan häiriöilmoitukset Viestintävirastolle

11.1 Ilmoitettavat tiedot

Liikenne- ja viestintävirastolle tunnistus- ja luottamuspalvelulain 16 §:n mukaisesti tehtävässä merkittävää uhkaa tai häiriötä koskevassa ilmoituksessa on annettava vähintään seuraavat tiedot:

1) tunnistusväline tai välityspalvelu, johon häiriö vaikuttaa;

2) kuvaus häiriöstä ja sen tiedossa olevista syistä;

3) kuvaus häiriön vaikutuksista, mukaan lukien vaikutus uusien tunnistusvälineiden myöntämiseen, käyttäjiin, luottaviin osapuoliin, muihin luottamusverkoston toimijoihin ja rajat ylittävään käyttöön;

4) kuvaus korjaustoimenpiteistä; sekä

5) kuvaus häiriöstä tiedottamisesta luottaville osapuolille, tunnistusvälineiden haltijoille, luottamusverkostolle ja tieto ilmoittamisesta muille viranomaisille.

11.2 Merkittävät häiriöt

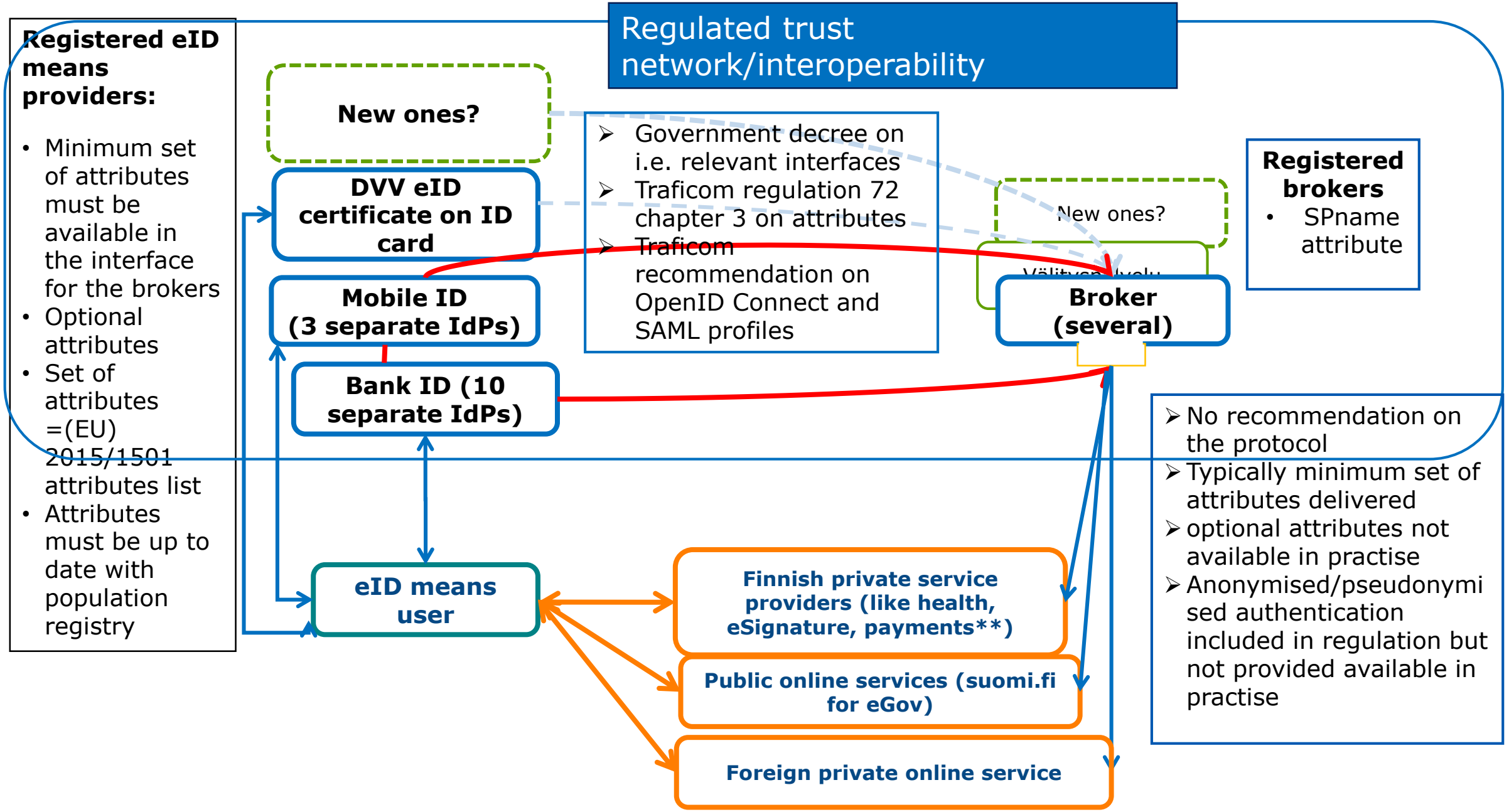
Merkittäviä tunnistuspalvelun häiriöitä ovat tapahtumat, jotka liittyvät sähköisen henkilöllisyyden virheellisyyteen tai väärinkäyttöön tai tietoturvauhkaan tai -häiriöön, joka vaarantaa tunnistamisen eheyden ja luotettavuuden. Merkittäviä ovat myös ennakoimattomat toimivuushäiriöt, joilla on vähäistä suurempia haittavaikutuksia luottamusverkostoon.

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

M72 Luku 3
Tietojen välittäminen luottamusverkostossa

Säännökset 12 ja 14

Attribuutit


Registered eID means providers:
• Minimum set of attributes must be available in the interface for the brokers
• Optional attributes
• Set of attributes =(EU) 2015/1501 attributes list
• Attributes must be up to date with population registry
Regulated trust network/interoperability
New ones?
DVV eID certificate on ID card
Mobile ID (3 separate IdPs)
Bank ID (10 separate IdPs)
eID means user
➢ Government decree on i.e. relevant interfaces
➢ Traficom regulation 72 chapter 3 on attributes
➢ Traficom recommendation on OpenID Connect and SAML profiles
New ones?
Broker (several)
Registered brokers
• SPname attribute
➢ No recommendation on the protocol
➢ Typically minimum set of attributes delivered
➢ optional attributes not available in practise
➢ Anonymised/pseudonymised authentication included in regulation but not provided available in practise
Finnish private service providers (like health, eSignature, payments**)
Public online services (suomi.fi for eGov)
Foreign private online service

Muutosehdotus Säännös 12 Luottamusverkostossa välitettävät vähimmäistiedot

12.1 Pakolliset tiedot

Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on välitettävä:

1) luonnollista henkilöä koskevassa tunnistustapahtumassa ainakin tunnistusvälineen tarjoajan varmistama henkilön yksilöivä tunniste, henkilön etunimi, henkilön sukunimi ja henkilön syntymäaika;

2) oikeushenkilöä koskevassa tunnistustapahtumassa ainakin tunnistusvälineen tarjoajan varmistama oikeushenkilöä edustavan luonnollisen henkilön yksilöivä tunniste, henkilön sukunimi, henkilön etunimi ja organisaation yksilöivä tunniste; sekä

3) tieto tunnistusvälineen korotetusta tai korkeasta varmuustasosta; sekä

4) tunnistusvälityspalvelun varmistama tieto luottavasta osapuolesta.

Muutosehdotus Säännös 12 Luottamusverkostossa välitettävät vähimmäistiedot

12.2 Valinnaiset tiedot

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

[alakohdat 1-3 ei muutoksia]

[* Ei käsitelty aikaisemmin:] *12.3 Tunnistuksen pseudonymisointi*

Edellä 1 ja 2 kohdassa määrätyt velvoitteet koskevat tunnistusvälineen ja tunnistusvälityspalvelun välistä rajapintaa ja tunnistusvälineen käyttäjän todentamista siinäkin tapauksessa, että tunnistusvälityspalvelu ilmoittaa tunnistus- ja luottamuspalvelulain 8 §:n 2 momentissa tarkoitetulla tavalla luottavalle osapuolelle vain tunnistusvälineen käyttäjän salanimen tai rajoitetun määrän henkilötietoja .

Kommentit työpajassa 12.5.2021/säännös 12

- Kysyttiin pseudonymisoinnista: Jos sitä ei standardoida, niin eikö silloin vähennetä mahdollisuutta kilpailulle?
  - Traficomin mukaan laissa määriteltyä, eli ei voida vaikuttaa.
- Kysyttiin, onko kohdassa 12.1 tulossa tunnistusvälineen tarjoajalle uusi velvollisuus?
  - Traficom: ei ole kysymys attribuutin tarkistamisen luotettavuudesta vaan todetaan neutraalisti, mikä taho ne tarjoaa. 12.1 ja 12.2 vaatimukset eivät muutu muutoin, vain SP-attribuutti lisätään.

Rajapintaprotokolla

Muutosehdotus Säännös 14 Tiedonsiirrossa käytettävä protokolla ja muut vaatimukset

[* Ei käsitelty aikaisemmin:] *14.1 Tiedonsiirrossa käytettävä protokolla*

Tunnistuspalvelun tarjoajan on

osaltaan mahdollistettava

ensitunnistamisen ketjuttaminen ja tunnistustapahtumien välitys luottamusverkostossa

vähintään Open IDConnect- tai SAML -protokollan mukaisella rajapinnalla, joka täyttää 7-9 kohdissa ja 12 kohdassa määrätyt vaatimukset .

14.2 Rajapinnan muut ominaisuudet

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

Kommentit työpajassa 12.5.2021/säännös 14

- Ei kommentteja

Kommentit 12.5.2021 /seuraavat työpajat, valmisteluprosessi

- Onko lisätyöpaja tunnistusasioista tarpeen to 20.5. 9-11
- DVV:n kanssa sovitaan erikseen säännösten 10, 13 ja 17 läpikäynti
- Viimeinen valmistelutyöpaja 10.6.2021
  - Koko määräys
  - ~3.6.2021 määräys- ja perustelumuistioluonnos
- kahdenvälisiä tapaamisia voi pyytää, jos on tarpeen käsitellä asioita, joita ei voi tuoda esille avoimissa työpajoissa

- Todettiin, että on tarpeen pitää jatkotyöpaja säännöksistä 8 ja 9
- Pidetään jatkotyöpaja vain rajatusti luottamusverkoston yhteistoimintaryhmän organisaatioille

Kiitos osallistumisesta, olkaa yhteydessä

eidas@traficom.fi

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus