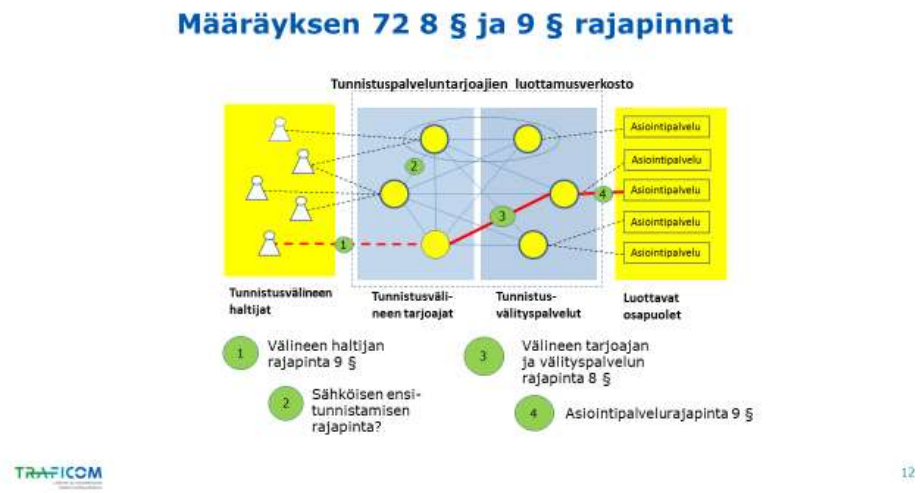
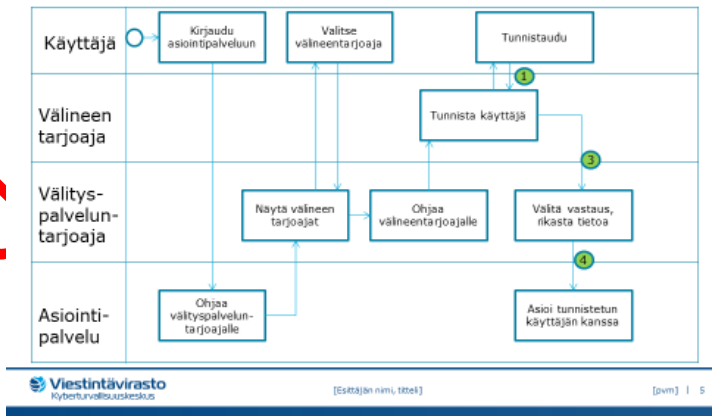
Dnro
TRAFICOM/245890/03.04.05.00/2020
13.1.2021

Määräys 72 valmistelumuistio 2021
Salausvaatimukset ja avaintenvaihto

Contents

1 Kuva


Määräyksen 72 8 § ja 9 § rajapinnat
Tunnistuspalveluntarjoajien luottamusverkosto
Asiointipalvelu
Asiointipalvelu
Asiointipalvelu
Asiointipalvelu
Asiointipalvelu
Tunnistusvälineen haltijat
Tunnistusväli-neen tarjoajat
Tunnistus-välityspalvelut
Luottavat osapuolet
1 Välineen haltijan rajapinta 9 §
2 Sähköisen ensi-tunnistamisen rajapinta?
3 Välineen tarjoajan ja välityspalvelun rajapinta 8 §
4 Asiointipalvelurajapinta 9 §
TRAFICOM
12


Käyttäjä
Kirjaudu asiointipalveluun
Valitse välineentarjoaja
Tunnistaudu
Välineen tarjoaja
Tunnista käyttäjä
Välitys-palvelun-tarjoaja
Näytä välineen tarjoajat
Ohjaa välineentarjoajalle
Välitä vastaus, rikasta tietoa
Asiointi-palvelu
Ohjaa välityspalvelun-tarjoajalle
Asioi tunnistetun käyttäjän kanssa
Viestintävirasto
Kyberturvallisuuskeskus
[Esittäjän nimi, titteli]
[pvm] | 5

2 Säännös ja perustelut (voimassa olevat)

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

Tähän on koottu myös säännösten perustelut ja soveltamisohjeet **perustelumuistiosta MPS72.** Perustelumuistion 14.5.2018 päivätyssä versiossa ovat mukana vuoden 2016 perustelut ja 2018 osittaismuutoksen perustelut. Perustelut päivitetään muutoksen yhteydessä.

Koko määräys ja perustelumuistio Finlexissä https://www.finlex.fi/fi/viranomaiset/normi/480001/42947

2.1 Säännös 5 § *Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet*

5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet

Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän

2) tietojärjestelmäturvallisuus

g) kansainvälisesti tai kansallisesti suositellut salausratkaisut muutoin kuin 7 §:ssä säädetyltä osin

2.1.1 Perustelumuistio

Perustelut

Pykälässä tarkennetaan tietoturvallisuuden toteuttamisessa tarvittavia toimenpiteitä.

Vaatimuksista säädetään yleisellä tasolla tunnistus- ja luottamuspalvelulain 8.1 §:n 4 alakohdassa, jossa viitataan EU:n varmuustasoasetuksen liitteen kohtiin 2.2.1, 2.3.1 ja 2.4.6.

Kohdassa 2.3.1 edellytetään korotetulla varmuustasolla todentamismekanismille tietoturvatoimenpiteitä vakavuusasteeltaan kohtuullisten tietoturvauhkien (arvaaminen, salakuuntelu, toisto, manipulointi) estämiseksi.

Kohdassa 2.4.6 säädetään toimenpiteistä tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi, sähköisen viestinnän kanavien suojaamisesta salakuuntelua, manipulointia ja toistoa vastaan, salausteknisen aineiston suojaamisesta, valmiudesta reagoida riskin muutoksiin, poikkeamiin ja tietoturvaloukkauksiin sekä laitteiden ja välineiden tietoturvallisuudesta.

Pykälän 1 momentin tietoliikenne-, tietojärjestelmä- ja käyttöturvallisuus turvaavat säädännössä vaaditun tietoturvallisuuden toteutumista.

Soveltaminen

1 momentin 2 g alakohdassa tarkoitettuja salausratkaisuja löytyy esimerkiksi seuraavista lähteistä:

- *ENISA [16],*

- *Viestintäviraston kyberturvallisuuskeskuksen NCSA:n (National Communications Security Authority, NCSA-FI) tuottama aineisto [17],*
- *NISTin (National Institute of Standards and Technology) FIPS-standardit (Federal Information Processing Standards) [18] tai*
- *SANS (The SANS Institute) [19].*

2.2 Säännös 7 § Tunnistusjärjestelmän ja rajapintojen salausvaatimukset

7 § Tunnistusjärjestelmän ja rajapintojen salausvaatimukset

Tunnistuspalveluntarjoajien välisten ja tunnistuspalveluntarjoajan ja asiointipalvelun välisten rajapintojen liikenne on salattava. Salauksessa, avaintenvaihdossa 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**: Käytettäessä RSA:ta sähköiseen allekirjoitukseen, avaimen pituuden tulee olla vähintään 2048 bittiä. Käytettäessä elliptisen käyrän menetelmää ECDSA:ta alla olevan kunnan koon tulee olla vähintään 224 bittiä.*

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

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

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

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.

Henkilötietoja sisältävien sanomien eheys ja luottamuksellisuus on suojattava edellä 1 momentissa tarkoitetun liikenteen salauksen lisäksi sanomatasolla 1 momentin mukaisesti.

Tunnistusjärjestelmässä säilytettävien tietojen eheydestä ja luottamuksellisuudesta on huolehdittava. Jos tiedon suojaaminen perustuu ainoastaan niiden salaukseen, sovelletaan edellä 1 momentissa allekirjoittamisen, symmetrisen salaamisen ja tiivistefunktioiden vaatimuksia.

2.2.1 Perustelumuistio ja soveltaminen

Pykälässä määrätään salauksen vähimmäisvaatimukset, joita on sovellettava tunnistuspalveluntarjoajien välillä ja tarvittaessa myös tiedon säilyttämisessä tunnis-

tusjärjestelmässä. Vaatimukset liittyvät tiedon salaamiseen sekä tietoa säilytettäessä että siirrettäessä. Salausvaatimuksilla halutaan turvata tunnistustapahtumien ja -lokien eheys ja luottamuksellisuus.

Vaatimukset vaikuttavat myös asiointipalvelu- ja käyttäjärajapinnassa, mitä käsitellään 9 pykälässä.

Vaatimukset vastaavat sitä, mitä eIDAS-sääntelyssä edellytetään kansallisten solmupisteiden välillä dokumentissa eIDAS - Cryptographic requirements for the Interoperability Framework, TLS and SAML [20].

Pykälässä käytettyjä lyhenteitä:

AES = Advanced Encryption Standard (symmetrinen salausmenetelmä)
DH = Diffie-Hellman (avaintenvaihtoprotokolla)
DHE = DH ephemeral-avaimilla
ECDH = Elliptic Curve Diffie-Hellman (avaintenvaihtoprotokolla)
ECDHE = ECDH ephemeral-avaimilla
ECDSA = Elliptic Curve Digital Signature Algorithm (allekirjoitusmenetelmä)
RSA = Rivest-Shamir-Adleman (epäsymmetrinen salaus- ja allekirjoitusmenetelmä)
SHA = Secure Hash Algorithm (tiivistefunktio)
(SSL/)TLS = Transport Layer Security (salausprotokolla)

Pykälän 1 momentissa määrätään tietoliikenteen salauksesta. Vaatimukset koskevat tietoliikennettä erityisesti silloin kun tietoliikenne kulkee suojatun fyysisen tilan ulkopuolella. Niitä sovelletaan myös, kun tietoa siirretään alihankkijalle. Momentin alakohdat ja niiden järjestys perustuu tyypilliseen kryptografian suunnittelujärjestykseen ja vaatimuksiin.

Pykälän 1 momentissa vaaditut arvot on otettu Viestintäviraston NCSA:n suosituksesta [17], joka on laadittu salaustuoteratkaisujen turvallisuuden arviointia varten niissä tilanteissa, joissa tietoa siirretään ei-luotetussa verkossa. Ei-luotetulla verkolla tarkoitetaan suosituksessa internetiä tai toimistoverkkoa tai muuta verkkoa, jonka tietoturvallisuutta ei ole kattavasti arvioitu.

Pykälän 1 momentin 1 alakohdan avaintenvaihdolla tarkoitetaan menetelmiä, jotka itsessään kuuluvat esim. TLS-protokollaan. Määräyksessä määritellään tarkemmin avaintenvaihdossa käytettävät salausmenetelmät. Määrätyt avaintenvaihdon vaatimukset voi täyttää käyttämällä IANAn (Internet Assigned Numbers Authority) IKEv2-määritysten mukaisia DH-ryhmiä 14 - 21, 23, 24 ja 26 [21].

Pykälän 1 momentin 2 alakohdan perusteena on se, että RSA on NCSA:n arvioima ja suosittelema standardi ja ECDSA tarjoaa vastaavan luotettavuustason. Muita vaihtoehtoja ei Viestintäviraston arvion mukaan käytännössä ole tarjolla.

Pykälän 1 momentin 3 alakohdassa on hyvä huomata, että 3DES on jätetty pois luettelosta. Se on poistettu suosituksista kesällä 2016.

Pykälän 2 momentin vaatimus salausasetusten teknisestä pakottamisesta tarkoittaa sitä, että järjestelmiä konfiguroitaessa ei saa sallia heikompia oletusarvoja tai sallia sitä, että järjestelmä voisi ohittaa vaatimukset. Ohjelmistojen ja laitteiden oletustoiminnot perustuvat usein toimivuuden tukemiseen joustavasti mahdollisimman monilla vaihtoehtoisilla määrityksillä, mutta tunnistusjärjestelmän salauksissa asetuksissa on estettävä heikompi salaus.

Pykälän 3 momentissa käsitellään tietoliikenneprotokollan vaatimuksia. Määräystä valmisteltaessa pykäläluonnoksissa mainittiin SSL/TLS, IPsec ja SSH. Määräykseen on jätetty ainoastaan TLS, koska se on vallitseva protokolla. Jos toimija käyttää eheyden ja luottamuksellisuuden varmistamiseen muuta kuin TLS-protokollaa, toteutuksen on tarjottava vastaava kryptografinen vahvuustaso.

Määräyksessä vaaditaan pääsääntönä TLS:n versio 1.2 tai uudemman käyttämistä, koska ne ovat tietoturvallisempia kuin sitä vanhemmat versiot. Versiota 1.1 saa käyttää vain, jos käyttäjän päätelaite ei tue uudempaa versiota. Vanhempia versioita ei saa käyttää. Määräyksessä sallitaan TLS 1.1 käyttö poikkeuksena pääsääntöön siksi, että mobiilipäätelaitteet eivät vielä kattavasti tue versiota 1.2, vaikka yleisesti ottaen selaimet ovat tukeneet 1.2 -versiota jo vuodesta 2011.

TLS:ää käytettäessä 1 momentin vaatimukset täyttäviä ciphersuiteja ovat mm. seuraavat [21]:

- *TLS_DHE_RSA_WITH_AES_128_CBC_SHA256*
- *TLS_DHE_RSA_WITH_AES_256_CBC_SHA256*
- *TLS_DHE_RSA_WITH_AES_128_GCM_SHA256*
- *TLS_DHE_RSA_WITH_AES_256_GCM_SHA384*
- *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384*
- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*

Jotta salausvaatimukset käytännössä järjestelmässä täyttyvät, on ciphersuiten määrittämisen lisäksi TLS-konfiguraatiossa varmistettava myös mm. DH-parametrien ja epäsymmetristen avainten ja varmenteiden riittävästä vahvuudesta.

Pykälän 4 momentin mukaan sen lisäksi, että tietoliikenneyhteys on salattu 1 momentin mukaisesti, henkilötietoja sisältävät sanomat on salattava. Vastaava vaatimus koskee sanomia kansallisten solmupisteiden välisessä liikenteessä. Salausvahvuuden on täytettävä 1 momentin vaatimukset. Sanomatason salausvaatimus koskee liikennettä, säilytettävästä tiedosta säädetään 5 momentissa.

Pykälän 5 momentti koskee tunnistusjärjestelmässä säilytettäviä tietoja. Tietojen luokittelua ei käsitellä tarkemmin tässä pykälässä. Toimijan on luokiteltava tiedot hyvien tietoturvallisuuskäytäntöjen mukaisesti ja yleisesti ottaen henkilötietojen lisäksi esimerkiksi tunnistusjärjestelmän hallintaan liittyvien salaisten tietojen eheys ja luottamuksellisuus on erityisesti suojattava.

Jos suojattavia tietoja säilytetään järjestelmissä siten, että niiden luottamuksellisuutta ja/tai eheyttä suojataan ainoastaan tai pääasiassa kryptografisin menetelmin, on käytettävä 1 momentissa määriteltyjä menetelmiä lukuun ottamatta avaintenvaihdon vaatimuksia. Ne eivät sovellu, koska levysalauksessa ei tyypillisesti käytetä avaintenvaihtoa. Vaihtoehtoisesti voidaan hyödyntää esimerkiksi huolellista pääsynhallintaa.

2.3 MPS2016: Viestintävirasto suositus korkean varmuustason salausvaatimuksista

Korkealla varmuustasolla tunnistusjärjestelmässä suositellaan sovellettavaksi määräyksessä 7 §:n 1 momentissa edellytettyjen korotetun varmuustason vaatimusten sijaan seuraavassa esitettyjä suluissa olevia arvoja:

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~~ (korkealla varmuustasolla **3072**) bittiä ja ECDHE-menetelmässä vähintään ~~224~~ (korkealla varmuustasolla **256**) bittiä.*

   *IANA:n IKEv2-määritysten mukaiset DH-ryhmät ~~14 -~~ 21, ~~23, 24 ja 26~~ (korkealla varmuustasolla **15 - 21**) toteuttavat edellä mainitut edellytykset.*

2) ***Allekirjoitus**: Käytettäessä RSA:ta sähköiseen allekirjoitukseen, avaimen pituuden tulee olla vähintään ~~2048~~ (korkealla varmuustasolla **3072**) bittiä. Käytettäessä elliptisen käyrän menetelmää ECDSA:ta, alla olevan kunnan koon tulee olla vähintään ~~224~~ (korkealla varmuustasolla **256**) bittiä.*

3) ***Symmetrinen salaus**: Salausalgoritmin on oltava AES tai Serpent (korkealla varmuustasolla **AES tai Serpent**). Avaimen pituuden tulee olla vähintään 128 (korkealla varmuustasolla **128**) bittiä. Salausmoodin on oltava CBC, GCM, XTS tai CTR.*

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

2.4 Säännös *8 § Tietoturvavaatimukset tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa*

8 § Tietoturvavaatimukset tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa

Salausmenetelmien tulee täyttää edellä 7 §:n 1 - 4 momentissa määrätyt vaatimukset.

Osapuolten tunnistamisessa ja tunnistamisessa tarvittavan tiedon välityksessä tulee käyttää metadataa tai vastaavia menettelyitä, jotka takaavat vastaavan tietoturvatason.

Kaikki henkilötiedot tulee salata ja allekirjoittaa sanomatasolla.

2.4.1 Perustelumuistio

Pykälän tarkoitus on selkeyttää sitä, että tunnistusvälineen ja tunnistusvälityksen tarjoajien välisissä rajapinnoissa on noudatettava määräyksen mukaisia salausvaatimuksia ja toimittava muutoinkin tietoturvallisesti.

Salausmenetelmien vaatimusten perustelut on käsitelty edellä 7 §:n kohdalla.

Pykälän 2 momentin mukaan osapuolten tunnistamisessa ja tunnistamistiedon välityksessä täytyy käyttää metadataa tai vastaavia menettelyitä. Metadatan tarkoitus on kahdenvälisen luotetun, jollain varmenteella allekirjoitetun, "kättelytiedon" vä-

littäminen luottamussuhdetta perustettaessa. SAML-protokollassa metadata sisältää esimerkiksi tunnistuspalveluntarjoajan (idP:n) pysyvän tai muuttuvan nimen ja varmenteen viestinnän salaamiseen ja allekirjoittamiseen. Open ID Connectissa metadatan toteutus on hieman erilainen, mutta perustarkoitus on sama.

Kaikki henkilötiedot tulee salata ja allekirjoittaa sanomatasolla. Pelkkä siirtotien salaus ei siis riitä. Asiaa käsitellään vaikutusarvioinnin (ks. A osa) luvussa 3 TUPAS-tarkastelun yhteydessä.

2.5 Säännös *9 § Tietoturvavaatimukset asiointipalvelurajapinnassa*

9 § Tietoturvavaatimukset asiointipalvelurajapinnassa

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

Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tulee huolehtia henkilötietojen luottamuksellisuudesta ja eheydestä asiointipalvelu- ja käyttäjärajapinnassa.

2.5.1 Perustelumuistio

Pykälän tarkoitus on selkeyttää sitä, että määräyksen vaatimukset vaikuttavat myös asiointipalvelu- ja käyttäjän päätelaiterajapintaan. Käyttäjän selain on asiointi- ja tunnistustapahtuman aikana yhteydessä asiointipalveluun, tunnistusvälitykseen ja tunnistusvälineen myöntäjään. Luotettavalla salauksella halutaan suojata henkilötietoja koko prosessissa.

Salausmenetelmien vaatimusten perustelut on käsitelty edellä 7 §:n kohdalla.

Pykälän 1 momentti koskee tunnistusvälityspalvelun ja asiointipalvelun välistä rajapintaa. Toinen momentti koskee tunnistusvälineen tarjoajan, tunnistusvälityspalvelun ja asiointipalvelun käyttäjärajapintaa. Määräys ei koske asiointipalvelun ja käyttäjän välistä rajapintaa muutoin, mutta velvoittaa tunnistusvälineen ja tunnistusvälityspalvelun tarjoajan toteuttamaan tunnistuspalvelunsa siten, että henkilötietojen luottamuksellisuudesta huolehditaan käyttäjän päätelaiterajapinnassa.

Pykälän 2 momentin vaatimus perustuu vaikutusarvioinnin (ks. A osa) luvussa 3 kuvattuun henkilötunnuksen käsittelyn vaatimuksiin. Vaatimukseen liittyvää siirtymäaikaa TUPAS-protokollaa käytettäessä käsitellään 25 §:n kohdalla. Vaatimuksen tarkoitus on estää se, että henkilötunnus tai muut henkilötiedot välitetään päätelaiterajapinnassa siten, että ne voivat tallentua selkokielisinä esimerkiksi päätelaitteen selailuhistoriaan.

2.6 Säännös *10 § Tietoturvavaatimukset kansallisen solmupisteen rajapinnassa*

10 § Tietoturvavaatimukset kansallisen solmupisteen rajapinnassa

Tunnistusvälityspalvelun tarjoajan ja kansallisen solmupisteen välisen rajapinnan tulee täyttää edellä 7 §:n 1 - 4 momentissa määrätyt vaatimukset.

2.6.1 Perustelumuistio

Kansallisella solmupisteellä tarkoitetaan EU:n sähköisen tunnistamisen yhteentoimivuusjärjestelmään liittyvää kansallista rajapintaa. Tunnistus- ja luottamuspalvelulain mukaan solmupistettä ylläpitää Väestörekisterikeskus. eIDAS-asetuksen mukainen, rajat ylittävä tunnistaminen notifioiduilla tunnistusvälineillä toteutetaan

kansallisten solmupisteiden välityksellä. Tässä pykälässä säädetään siitä, että luottamusverkoston ja kansallisen solmu-pisteen välillä täytyy noudattaa samoja salausvaatimuksia kuin muissakin luottamusverkoston sisä- tai ulkorajapinnoissa.

Kansallisten solmupisteiden välisten rajapintojen vaatimukset määritellään asiakirjassa eIDAS - Cryptographic requirements for the Interoperability Framework, TLS and SAML, Version 1.0, 6 November 2015 [20].

2.7 Perustelujen tekstiä MPS72 2016 käyttäjärajapinnasta

MPS72 2016 *12.3.2 Tunnistusvälineen haltijan ja tunnistusvälineen tarjoajan välinen rajapinta*

Tunnistusvälineen haltijan selain on tunnistustapahtuman kuluessa yhteydessä asiointipalveluun, tunnistusvälityspalveluun ja tunnistusvälineen tarjoajan palveluun. Tunnistusvälineen haltijan ja asiointipalvelun välisellä yhteydellä voinee olla aluksi käytössä http, mutta tunnistamistapahtumassa kaikilla tunnistusvälineyhteyksillä tulee olla käytössä https ja määräyksen 7 §:n mukaisesti TLS versio 1.2. tai poikkeustapauksissa versio 1.1. Vaatimukset ovat tältä osin käytännössä samat kuin tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välillä.

Määräyksenantovaltuus ulottuu vain tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan rajapintaan, joita nämä tarjoavat luottamusverkostosta ulospäin asiointipalvelulle ja tunnistusvälineen haltijalle. Koska tunnistusvälineen haltijan kannalta tunnistustapahtuman eri yhteydet tehdään samalla selainistunnolla, em. rajapinnoille asetetut vaatimukset koskevat käytännössä välillisesti myös asiointipalvelun ja tunnistusvälineen haltijan välistä rajapintaa.

3 Lähteet 2021 vaikutusarviointiin

3.1 Yleiskuvaus lähtötilanteesta, viraston arvio kyselyssä 2020

Määräyksen 5 §:n 1 momentin 2g) kohdassa määrätään yleisesti salausratkaisuista ja 7 §:ssä määrätään tunnistuspalveluntarjoajien välisten ja tunnistuspalveluntarjoajan ja asiointipalvelun välisten rajapintojen liikenteen salauksesta. 5 §:n yleinen vaatimus koskee siis esimerkiksi tunnistuspalvelun ja sen alihankkijan välisiä yhteyksiä ja tunnistuspalvelun omia järjestelmiä.

Määräyksen 7 §:ssä määrätään TLS-salauksessa hyväksyttävistä salausmenetelmistä, parametreista ja salausprotokollista. Vuonna 2016 päädyttiin salauksen sääntelymallien vaikutusarvioinnissa siihen, että turvallisten algoritmien kehitys on sen verran hidasta, että tarkat vaatimukset voidaan määrätä pykälässä ja määräystä muuttaa tarvittaessa. Valvonnassa virastolle on tullut vastaan uusia algoritmejä kuten Poly1305 ja ChaCha20 ja on selvää, että 7 §:n vaatimusten ajantasaisuutta on tarkasteltava.

Salausalgoritminen yksityiskohtaisen sääntelyn sijaan voidaan ottaa tarkasteltavaksi myös muita mahdollisia dynaamisempia malleja, jos sellaisia löytyy. Virasto pitää kuitenkin valvontakokemusten perusteella tarpeellisena varmistaa vaatimusten tarkkuus ja ennakoitavuus, sillä esimerkiksi tietoturvattomasta TLS 1.0 -protokollasta tai 3DES-algoritmistä luopuminen ei vuosien jälkeenkään ole täysin toteutunut.

Tietoliikennerajapintojen turvallisuusvaatimukset koostuvat lähinnä 7 §:n salausvaatimuksista.

Määräyksen 8 §:ssä selvennetään, että vaatimukset koskevat tunnistusvälineen ja tunnistusvälityspalvelun rajapintaa. Näiden välillä edellytetään 8 §:ssä myös tietoliikenteen osapuolten tunnistamista.

Määräyksen 9 §:ssä selvennetään, että vaatimukset koskevat tunnistuspalveluiden ja asiointipalveluiden sekä tunnistuspalvelun ja tunnistusvälineen käyttäjän välistä rajapintaa. Asiointipalvelun tunnistamisesta ei ole määrätty, mutta vaatimus sanomatason salauksesta edellyttää salausavainten vaihtoa tunnistuspalvelun ja asiointipalvelun välillä, mikä pyrkii varmistamaan myös sen, että muut kuin tunnistusvälityksen kanssa sopimuksen tehneet asiointipalvelut eivät voi käyttää vahvaa tunnistuspalvelua (oikeudettomasti esiintyä asiointipalveluna).

Etenkin Tupas-siirtymä ja sanomatason salauksen käyttöönotto ja siihen liittyvä avaintenhallinta asiointipalvelun kanssa aiheuttivat muutostarpeita vuoden 2019 aikana.

Virasto arvioi, että määräysvalmistelussa on arvioitava ainakin tarkempia teknisiä keinoja estää käyttäjien huijaaminen tunnistautumaan väärään asiointipalveluun.

3.2 Vuonna 2016 ja 2018 vaikutusarvioinneissa linjatut asiat

3.2.1 Algoritmit ja sääntelyn tarkkuus

3.6.2 Tunnistuspalveluiden tietoturva: salausvaatimukset (MPS72 2016)

Arvioitava kysymys: Määrätäänkö vähimmäisvaatimukset eri rajapinnoissa käytettävälle salausalgoritmille, tiivistealgoritmille ja avainpituuksille sekä mikä on vaatimustaso? Voidaanko korotetulle ja korkealle varmuustasolle määritellä eri vähimmäisvaatimukset?

Arvioinnin lähtökohdat

Tunnistuslain 8.1 §:n 4 alakohdassa säädetään tunnistusjärjestelmän turvallisuus- ja luotettavuusvaatimuksista. Laissa viitataan myös EU:n varmuustasoasetuksen liitteen kohtiin 2.2.1, 2.3.1 ja 2.4.6. Kohdassa 2.3.1 säädetään todentamismekanismin kyvykkyydestä suojautua ulkoiselta uhalta; korotetulla tasolla vakavuusasteeltaan kohtuulliselta (moderate) ja korkealla tasolla vakavuusasteeltaan korkealta (high).

Viestintävirasto voi määrätä tunnistusjärjestelmän 8 §:n 1 momentin 4 kohdan mukaisista turvallisuutta ja luotettavuutta koskevista vaatimuksista.

Salausmenetelmien tasosta on käytettävissä eri lähteitä kuten ENISAn vuosittainen raportti tai eIDAS-asetuksen kansallisia solmupisteitä koskevat määrittelyt. Viestintäviraston tehtäviin kuuluu muun säädännön perusteella salaustuotteiden arviointi ja menetelmien arvioinnissa voidaan hyödyntää myös tässä tehtävässä työstettyä tietoa.

Vaatimusten määrittelyssä on huomioitava käytettävyys ja käyttäjien käytössä olevien selainten versiot. Lisäksi on huomioitava tunnistuspalveluntarjoajille ja asiointipalveluiden tarjoajille aiheutuvat muutostarpeet. Vaatimusten taso täytyy suhteuttaa uhkiin.

eIDAS-asetukseen liittyvissä spesifikaatioissa ei ole eroteltu korotetun ja korkean tason salausvaatimuksia.

Linjaukset

Määrätään salausmenetelmien vaatimustasot siten, että ne perustuvat pääsääntöisesti vähintään TLS 1.2 versioon, joka on ollut oletuksena yleisissä käyttäjien käyttämissä selaimissa jo vuodesta 2011 ja jolle on ollut olemassa tuki jo vuodesta 2009. Mobiilipäätelaitteet eivät kuitenkaan samassa laajuudessa tue TLS versiota 1.2, joten myös versio 1.1 on sallittava tarvittaessa.

Vaatimukset määritellään verraten yksityiskohtaisesti määräyksessä. Salausmenetelmien vahvuus kehittyy sen verran hitaasti, että määräystä voidaan muuttaa tarvittaessa. Määrittelyssä hyödynnetään Viestintäviraston työstämää tietoa salausmenetelmien vahvuudesta huomioiden, ettei aseteta tiukempia

vaatimuksia kuin eIDAS-asetukseen liittyvässä ohjeistuksessa. Korotettua ja korkeaa tasoa ei erotella määräyksessä pakottavissa vaatimuksissa, mutta korkealle tasolle annetaan suositus.

Määräyksen 7 § ja B-osan luvussa 7.2 oleva Viestintäviraston suositus korkean varmuustason salauksesta on laadittu näiden linjausten mukaisesti.

Määräykselle vaihtoehtoiset ohjauskeinot

Suositus/ohje. *Valmistelussa on arvioitu, että vähimmäisvaatimukset pystytään muotoilemaan yleispätevästi määräykseen. Korkean tason salausvaatimukset annetaan suosituksena.*

Yhteissääntely. *Ei ole tarkasteltu.*

Informaatio-ohjaus. *Ei liene relevantti, sillä tietoturvallisuuden vähimmäistaso ei ole kilpailuasia.*

3.2.2 Sanomatason salaus

3.4.6 Rajapinnat: TUPAS-kysymykset

Henkilötietojen välitys TUPAS -asiointipalvelurajapinnassa

Arvioitava kysymys: Vaaditaanko määräyksellä muuttamaan nykyistä TUPAS-protokollaa ja sen käyttöä siten, ettei henkilötunnuksen välittäminen selväkielisenä ole enää sallittua, vaan on käytettävä protokollassa ennestään määriteltyjä muita tapoja? Jos vaaditaan, kuinka pitkä siirtymäaika määrätään?

Asiointipalvelun ja tunnistusvälityspalvelun välisen rajapinnan määrittelyt vaikuttavat siihen, miten asiointipalvelun täytyy toteuttaa oma järjestelmänsä. Rajapinnassa on tunnistettu valmistelussa TUPAS-protokollalle ominainen tietoturvakysymys, joka liittyy HETUn toimittamiseen selkokielisenä URLissa asiointipalvelulle. TUPAS-protokolla sinänsä mahdollistaa HETUn siirrolle useamman vaihtoehdon, myös turvallinen vaihtoehto on siis määritelty. Käytännössä toteutus kuitenkin sopeutetaan asiointipalvelun vaatimuksiin ja vallitseva tapa on HETUn selväkielinen välitys.

Viestintävirasto arvioi, että salaamattoman HETUn välittäminen ei täytä EU:n varmuustasoasetuksen seuraavia vaatimuksia:

2.4.6 Tekniset tarkastukset (LUE: Kontrollit tai toimenpiteet)

MATALA

1. Käytössä on oikeasuhteiset tekniset tarkastukset palvelujen turvallisuuteen kohdistuvien riskien hallitsemiseksi ja käsiteltävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi.

2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät sähköisen viestinnän kanavat on suojattu salakuuntelulta, manipuloinnilta ja toistolta.

5. Kaikki laitteet ja välineet, jotka sisältävät henkilötietoja, salattuja tietoja tai muita arkaluonteisia tietoja, säilytetään, kuljetetaan ja hävitetään turvallisella ja varmalla tavalla.

Commented [LA1]: Tässä oli kopiointivirhe MPS2016:ssa

Soveltamisohje:

On tärkeää pitää erillään luottamuksellisuuden ja eheyden suojaamista koskevien vaatimusten arviointi. Eheyden (tai aitouden) suojaaminen määräytyy periaatteessa varmuustason mukaan, mutta henkilöihin liittyvän tiedon luottamuksellisuuteen vaikuttavat myös tietojen tyyppi sekä mahdolliset suojaamista koskevat lainsäädännölliset vaatimukset.

Henkilötietojen luottamuksellisuus on suojattava ja käytössä on oltava turvatoimenpiteitä, jotka pohjautuvat riskiperusteista lähestymistapaa hyödyntävään arviointiin valitun tietoturvallisuuden hallintajärjestelmän mukaisesti. Turvatoimenpiteiden kattamia osa-alueita ovat esimerkiksi tietomurrot, väärinkäytökset, palvelunestohyökkäykset ja hajautetut palvelunestohyökkäykset.

2.3.1 Todentamismekanismi

MATALA

2. Jos henkilön tunnistetiedot tallennetaan osana todentamismekanismia, nämä tiedot on suojattu niiden menetykseltä ja vaarantamiselta, mukaan lukien analyysi verkkoympäristön ulkopuolella.

Soveltamisohje:

Tallennettuihin henkilötietoihin pääsyä on valvottava huolellisesti. Henkilön tunnistetietojen suojaamisessa käytettäviä menetelmiä ovat esimerkiksi Euroopan unionin verkko- ja tietoturvaviraston ENISAn "Algorithms, Key Sizes and Parameters Report" -asiakirjan, kansallisten salausohjeiden tai muiden hyvien toimintatapojen mukainen salaaminen ja tiivistäminen.
Käyttöoikeuksia on aina valvottava.

Henkilötunnus on henkilötietolain perusteella katsottavat tunnisteeksi, jota on käsiteltävä erityisen huolellisesti. Edellä poimituista kohdista voidaan ainakin EU:n varmuustasoasetuksen 2.4.6 kohdan 1 alakohdan katsoa soveltuvan suoraan myös asiointipalvelurajapintaan. Vaikka tämän ja muiden poimittujen kohtien vaatimukset kohdistuvat suoranaisesti tunnistuspalveluntarjoajan omiin järjestelmiin, tukevat ne myös henkilötiedon suojaamista asiointipalvelurajapinnassa. Jos henkilötunnusta on suojattava tiukasti palveluntarjoajan järjestelmässä, ei ole suhteessa näihin vaatimuksiin, jos sen voi luovuttaa asiointipalvelurajapinnassa tavalla, joka altistaa tunnuksen luottamuksellisuuden menettämiselle.

Nykyisen menettelyn säilyttäminen asiointipalvelurajapinnassa vaarantaa siis henkilötunnuksen tietoturvallisuuden. Selaimeen tallentuneet henkilötunnukset voivat paljastua muille selaimen käyttäjille, mikä on ainakin yhteiskäyttöisillä päätelaitteilla huomionarvoinen riski. Siirtyminen HETUn salaamiseen asiointipalvelurajapinnassa parantaisi selvästi henkilötunnuksen tietoturvaa.

Asiointipalvelun kannalta siirtyminen henkilötunnuksen salattuun välittämiseen edellyttäisi muutoksia asiointipalveluiden omissa järjestelmissä (kyvykkyyttä purkaa salaus). Tunnistuspalvelun tarjoajan kannalta muutos edellyttäisi nykyisen asiointipalvelusopimuskannan muutoksia. Ongelmana tilanteessa on se, että asiointipalveluilla ei ole kannustinta siirtyä turvallisempaan menettelyyn.

Tunnistuspalveluntarjoajien olisi siirryttävä turvallisempaan menettelyyn yhtenäisesti, jotta nykykäytännön jatkaminen ei antaisi perusteetonta kilpailuetua. Vain joidenkin toimijoiden siirtyminen uuteen käytäntöön saattaisi johtaa siihen, että asiointipalvelut eivät enää hyväksyisi näitä tunnisteita, mikä rajoittaisi joidenkin tunnistusvälineen haltijoiden mahdollisuuksia käyttää vahvaa sähköistä tunnistettaan asiointipalveluissa.

***Viestintävirasto arvioi edellä mainituilla perusteilla, että ainoa keino sysätä tietoturvallisuuden kehitystä tältä osin eteenpäin on määrätä henkilötunnuksen salaaminen asiointipalvelulle välitettäessä pakolliseksi.** Tämä olisi myös eIDAS-asetuksen mukainen sääntelyratkaisu. Vaatimukselle olisi määrättävä siirtymäaika, jotta asiointipalveluilla ja tunnistuspalveluntarjoajilla olisi mahdollisuus tehdä muutokset aiheuttamatta katkoksia toimintaan ja jaksottamalla vaadittavaa muutostyötä. Siirtymäaika voisi kestää esimerkiksi 18.9.2018 asti, jolloin jäsenvaltioiden on viimeistään oltava valmiita vastaanottamaan toisista jäsenvaltioista tulevat notifioidut tunnisteet.*

Suhteessa muuhun lainsäädäntöön on otettava huomioon, että henkilötunnuksen ja muiden henkilötietojen käsittelyä sääntelään henkilötietolaissa, jonka korvaa parin vuoden kuluttua EU:n tietosuoja-asetus. Näissä sääntelään henkilötietojen käsittelyn tietoturvallisuutta ja tietosuoja-asetus tuo mukanaan myös huomattavat seuraamusmaksut. Henkilötietolakia ja vastaisuudessa tietosuoja-asetusta valvoo tietosuojavaltuutettu. Suhteessa henkilötietosäädäntöön eIDAS, tunnistuslaki ja tämä määräys ovat erityissäädäntöä. Henkilötietosäädäntö soveltuu siltä osin, kun erityissäädännössä ei ole säädetty muuta.

Tietosuojavaltuutettu on todennut [2016] määräysvalmistelun yhteydessä antamassaan lausunnossa, ettei henkilötietolainsäädäntö estä määräämästä tunnistuspalvelun tietoturvavaatimuksista Viestintäviraston määräyksessä.

3.3 Lähteet/referenssit/standardit

- NCSA-toiminnon Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset suojaustasot (ohje 28.11.2018 ~~11.11.2015~~ dnro 190/651/2015)
    - https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf

  - tämä on edelleen käyttökelpoinen referenssi turvallisten algoritmien listaamisessa, mutta olisi sellaisenaan tarpeettoman tiukka (esim. TL IV edellyttää 3K avaimia), joten on tarpeen modifioida määräyksessä

- SOGIS-MRA
  - https://www.sogis.eu/uk/supporting_doc_en.html#:~:text=The%20document%20%C2%AB%20SOG%2DIS%20Crypto,by%20all%20SOG%2DIS%20participants.
  - SOGIS Agreed Cryptographic Mechanisms (version 1.2 January 2020) https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf
  - Tällä hetkellä tuoreempi kuin NCSA-FI:n lista ja on enemmän algoritmejä, joita ei vielä hyväksytty/listattu Suomessa. Päivitetään joka toinen vuosi.
- eIDAS Cryptographic Requirements for the Interoperability Framework, TLS and SAML, Version 1.2, 31 August 2019
  - https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20Cryptographic%20Requirement%20v.1.2%20Final.pdf?version=2&modificationDate=1571068651805&api=v2
- ENISA, The European Union Agency for Network and Information Security www.enisa.europa.eu, esim. Study on cryptographic protocols 2014 https://www.enisa.europa.eu/publications/study-on-cryptographic-protocols
  - Päivitetään harvoin, ei kovin ajantasainen verrattuna SOGIS MRA:n tai NCSA-FI:n dokumentteihin
- NISTin (National Institute of Standards and Technology) FIPS-standardit (Federal Information Processing Standards) www.nist.gov
  - Paljon materiaalia ja yksityiskohtaisia dokumentteja. Mahdollista poimia dokumentteja, mutta mitkä olisivat relevantteja tai hyödyllisiä?
- ~~KATAKRI, Tietoturvallisuuden auditointityökalu viranomaisille, löytyy esim.~~
  - Päivitetty 2020 https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille
  - On nykyisessä MPS:ssä viiteluettelossa, mutta onko tässä kohtaa relevantti
- SANS (The SANS Institute) www.sans.org
  - On nykyisessä MPS:ssä viiteluettelossa, mutta onko hyödyllisiä lähteitä
- IANAn (Internet Assigned Numbers Authority)
  - IKEv2-määritykset http://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml
  - IANAn ciphersuitet: http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4
- RFC 8446…[TLS 1.3]
- RFC 7905 ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS)

- https://tools.ietf.org/html/rfc7905

- ETSIn standardit tai spesifikaatiot https://ec.europa.eu/cefdigital/wiki/display/EIDTECHSUB/Security+Profile+v+1.3
  - Feb 2019 - ETSI TS 119 312 V1.3.1 (2019-02) "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites"
- NIST SP 800-52 Rev. 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
  - https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
- Globalsign verkkoartikkeli TLS Protocol Compatibility, June 21, 2018
  - Esimerkki TLS - versioiden yhteensopivuuskoostetta TLS 1.2-ajalta (selaimet, clientit, palvelimet, kirjastot)
  - https://support.globalsign.com/ssl/general-ssl/tls-protocol-compatibility
- Liikenne- ja viestintäviraston kyberturvallisuuskeskuksen NCSA (National Communications Security Authority, NCSA-FI),
  - yleistä NCSA-FI tietoa https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/ncsa
  - NCSA-toiminnon hyväksymät salausratkaisut (27.4.2016 dnro 238/651/2013) https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/NCSA_salausratkaisut.pdf
- Haavoittuvuuksien seurantalähteet, mitkä olisivat relevantteja:
  - Määräyksen 5 §:n turvallisuuden ylläpitoon liittyen
  - NIST, SOGIS -päivitykset, NCSA
  - CVE https://cve.mitre.org/ ja https://cwe.mitre.org/

3.4 Toimialakysely 2020 muutostarpeista

Seuraavaan on koottu viraston elokuussa 2020 tekemästä muutostarvekyselystä aiheeseen liittyviä kysymyksiä ja vastauksia. Vastauksia on tässä koosteessa osittain niputettu ja anonymisoitu.

14) **Salaus.** Onko 5 §:n määrittely salausvaatimuksista ja määräyksen perusteluissa olevat referenssit (ENISA, NIST, NCSA-FI, SANS) riittäviä? Olisiko määräystä tai perusteluja tarpeen muuttaa jotenkin? Mikä on mielestänne hyödyllisin referenssi suositelluista salausratkaisuista?

DVV

- *Perusteluissa olevat referenssit ovat riittävät. Emme näe tarvetta määräyksen muuttamiselle. Hyödylliseksi ja hyväksi referenssiksi on todettu NCSA-FI tuottamat kryptografiset vahvuusvaatimukset sekä hyväksytyt salausratkaisut. Olisi kuitenkin tarpeen täydentää näitä dokumentteja selkeillä viittauksilla tunnistuspalvelun varmuustasojen edellytyksiin sekä luottamuspalvelujen vaatimuksiin nähden.*

15) **Salaus.** Ovatko tietoliikenneyhteyden salausvaatimukset 7 §:ssä mielestänne ajan tasalla? Mitä muutoksia salausmenetelmiin, niiden parametreihin tai määräyksessä mainittuihin salausprotokolliin olisi tehtävä? Miten määräyksen perusteluissa olevia ciphersuiteja olisi mahdollisesti päivitettävä?

DVV

- *Mielestämme vaatimukset ovat tällä hetkellä riittävät.*

Findy-konsortio

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

Muut

- *on viitteitä siitä, että määräyksessä 72 ja perustelumuistiossa luetellut ja viitatut algoritmit ovat osin vanhentuneita ja kaikki luetellut komponentit eivät viimeisimmän tutkimuksen perusteella ole luotettavia [1.https://docs.microsoft.com/enus/dotnet/standard/security/vulnerabilities-**cbc-mode**].*
- *perustelumuistiossa on viittauksia dokumentteihin, joiden saatavuus on heikkoa [viraston] organisaatiomuutosten jälkeen. Kokonaiskäsityksen muodostaminen viranomaisen tarkoituksesta on haastavaa, kun viitemateriaalit eivät ole saatavilla tai ovat vaikeasti löydettävissä.*
- *ChaCha20 ja Poly1305 olisi aiheellista sallia mahdollisimman pian. Pidämme niitä vähintään yhtä turvallisina kuin nykyisen määräyksen sallimia algoritmeja. Lisäksi näiden algoritmien puuttuminen sallittujen listalta estää tällä hetkellä joidenkin hyödyllisten pilvipohjaisten hajautettujen edustapalveluiden hyödyntämisen luottamusverkoston palveluissa.*

16) **Salaus.** Onko määräyksen perustelumuistiossa oleva suositus korkean varmuustason algoritmeista mielestänne ajan tasalla? Olisiko suositus muutettava velvoittavaksi ja siirrettävä se määräykseen? Miten tämä vaikuttaisi korkean varmuustason tunnistuksen käytettävyyteen, yhteentoimivuuteen ja asiointipalveluihin?

DVV

- *Suositukset ovat tällä hetkellä riittävät.*
- *Kokonaisuuden kannalta olisi kuitenkin tarpeen arvioida mahdollisuutta noudattaa sekä korotetulla että korkealla tasolla samoja vaatimuksia, etenkin tilanteissa, joissa heikommalla algoritmilla ei saavuteta merkittävää toiminnallista hyötyä.*

Muut

- *Viittaus edelliseen kysymykseen, mitä tulee määräyksen algoritmimääritysten ajantasaisuuteen*

17) **Salaus.** Onko 7 §:n salausvaatimusten toteutettavuudessa teknisiä ongelmia tai ristiriitaisuuksia? Miten olette ratkaisseet ne ja miten määräystä tulisi mielestänne muuttaa?

DVV

- *Emme ole tunnistaneet ristiriitaisuuksia.*

Nixu Corporation

- *Osoituksena liian yksityiskohtaisen teknologiasääntelyn vaaroista on määräyksen edellisen version (72/2016) kohta, jossa TLS 1.1 on sallittu (tietyissä tilanteissa), mutta TLS 1.1 tuloksena oli aina tiivistealgoritmi, joka aina oli määräyksen vastainen. TLS 1.1 ei tue SHA2:tä (vain SHA1 ja MD5 on tuettuja RFC 4346:ssä) eli M72/2016 7§3 eksplisiittinen poikkeaman salliminen sallii implisiittisesti 7§1 k4 poikkeamisen. TLS 1.1 on siis sallittu (7§3) ja kielletty (7§1 k4 ei salli yhtään TLS 1.1:n käyttämistä tiivisteistä). Ilmeisesti lainsäätäjän tarkoitus on ollut sallia TLS 1.1, joten 7§1 k4 oli väistyvä.*
- *Toinen esimerkki liian yksityiskohtaisen sääntelyn ongelmista koski SHA1-tiivistefuntion käyttöä muissa tarkoituksissa kuin tiivisteen laskennassa. M72 7§1 4) sallii tietyt tiivistefuntiot. Tarkoituksena oli, että mainitut tiivisteiden laskennassa kyseiset algoritmit ovat sallittuja. Niitä kun voidaan käyttää muuten. SHA1 käytettiin pseudosatunnaisuuden luomiseen, ja tämä käyttötapa on määräyksen sanamuodon takia kielletty. Todettakoon, että tästä ei aiheutunut mitään oikeaa ongelmaa, sillä Traficom tarkensi kohtaa, kun asi*asta tiedusteltiin.

Muut

- *Määräyksen 7 § on tulkittavissa kirjaimellisesti niin, että edes julkista avainta tai sertifikaattia ei saisi siirtää sellaisen TLS-yhteyden yli, jossa ei ole pakotettua perfect forward secrecyä (DHE tai ECDHE). Ottaen huomioon että DHE ja ECDHE turvaavat nimenomaan tiedonsiirron pysyvää luottamuksellisuutta, ei tällainen kirjaimellinen tulkinta ole mielekäs kun jaetaan täysin julkista sisältöä. Määräystä voisi täsmentää, että määrättyjä menetelmiä on käytettävä kaikissa niissä yhteyksissä, joiden yli siirretään henkilötietoja tai muita luottamuksellisia tietoja.*

18) **Salaus.** Olisiko salausvaatimusten säätelylle mielestänne vaihtoehtoisia malleja sen sijaan, että vaatimukset määritellään nykyisellä tavalla pykälässä? Mitä yhdenmukaisesti mitattavissa ja määriteltävissä olevia (sääntelyn vaatimusten kannalta ennakoitavia) malleja ja referenssejä määräyksessä voisi mielestänne käyttää?

DVV

- *SSL/TLS-varmenteiden osalta vastaavista vaatimuksista ohjeistaa monelta osin CA/Browser Forum. Käytännössä kaikki varmentajat noudattavat CA/Browser Forumin julkaisemia Baseline Requirements -ohjeita. Nämä ohjeet päivittyvät useita kertoja vuodessa ja reagoivat sääntelyä tai standardeja nopeammin havaittuihin ongelmiin ja puutteisiin. Vastaavaa mallia voisi harkita sovellettavaksi salausvaatimuksien osalta.*

Nixu Corporation

- *Traficom pitää yllä listaa kryptografisista vahvuusvaatimuksista: Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen – kansalliset suojaustasot (Dnro: 190/651/2015). Traficomin on syytä harkita, voidaanko 7§ korvata viittauksella Traficomin ohjeeseen tai muuhun listaan yleisesti turvallisena pidetyistä algoritmeistä.*
- *kun uusi salausratkaisu todetaan hyväksi (ja se voi jopa saada Traficomin CAA:n hyväksynnän), mutta tätä ole 7§ mainittu, on ratkaisua käyttävä palvelu turvallinen mutta laiton. Esimerkiksi ChaCha on uusi, mutta ilmeisesti hyvä salaus.*
- *Salausalgoritmeissä (yleensä sen toteutuksessa, ei perusmatematiikassa) havaitaan heikkouksia aina silloin tällöin. Mikäli joku 7§ pykälän algoritmi*

todetaan heikoksi, on tilanne nurinkurinen: salausta käyttävä palvelu on turvaton, mutta lain mukainen.
- *On varsin mahdollista, että TLS 1.3-versio ja uusien salausalgoritmien myötä muutos turvallisesta turvattomaan tapahtuu aiempaa nopeammin, mikä puoltaa nopeampaa reagointia myös lain säätäjän puolelta.*

Muut
- *Sallittujen algoritmien luetteloa olisi hyvä tarkastella ja päivittää useammin kuin nykyisellä useiden vuosien syklillä*
- *salausvaatimukset olisi hyvä tällä tarkkuudella määritellä toisaalla. Määräyksessä tulisi riittää vaadittavaksi rajapinnan tietoturvatason mukainen vaatimustaso, joka tarkennetaan erikseen*
- *salausvaatimusten määrittely tarkkuudella, jota on käytetty määräyksen 72 pykälässä 7, sisältää riskejä. Määräys on luonteeltaan staattinen ja päivittyy raskaiden prosessien kautta. Sen sijaan viime vuosina salausratkaisut ovat kehittyneet vauhdikkaasti ja on myös löytynyt yllättäviä salaustoteutusten haavoittuvuuksia, jotka ovat pakottaneet tekniset toimijat päivittämään toteutuksiaan tiheään.*
- *toteutukset siirtyvät yhä enemmän alustaratkaisuihin, joissa rajapinnan ulospäin asiakkaalle ja verkoston muille osapuolille näkyvä päätepiste toteutetaan dynaamisesti muuttuvana esimerkiksi siten, että alustaratkaisun toteuttaja asettaa tarjolle joukon kulloinkin yleisesti hyväksyttyjä ja turvalliseksi todettuja salausvaihtoehtoja, joista toteuttaja valitsee palvelussa käytettävät salausratkaisut.*
- *saatetaan joutua tilanteeseen, jossa määräyksessä hyväksytyksi määriteltyä joukkoa salausvaihtoehtoja ei ole saatavilla, kun alustatoimittajan turvalliseksi todettu joukko on edennyt määräyksen määritelmiä pidemmälle.*
- *Määräyksen salausvaatimukset saattavat aiheuttaa jopa sen, että toimija joutuu valikoimaan vähemmän turvallisen rajapintatoteutuksen, kuin mikä olisi mahdollista alustatoimittajan tarjoamalla turvallisemmalla joukolla salausvaihtoehtoja.*
- *salausvaatimusten määrittely ja valvonta olisi hyvä eriyttää määräyksestä erilliseksi, mahdollisesti yleisemmäksi ei pelkästään tunnistamisen toteuttamista koskevaksi viranomaistoiminnokseen*

19) **Salaus.** Onko tietoliikenneyhteyksillä muita relevantteja yhteyskäytäntöjä kuin TLS? Pitäisikö ne huomioida sääntelyssä tai soveltamisohjeissa?

DVV
- *Emme ole tunnistaneet tällaista tarvetta toistaiseksi.*

Muut
- *TLS:llä voidaan taata riittävän luotettavat tietoliikenneyhteydet. Muiden yhteyskäytäntöjen mukaan ottaminen lisäisi byrokratiaa (esim. IP-pohjaiset rajoitteet)*
- *FTN-tunnistamisessa käytetään työnkulkuja, jotka edellyttävät interaktiota loppukäyttäjän selaimessa ja ne käyttävät HTTPS-yhteyskäytäntöä myös muiden osapuolien välillä. Ei muita varteenotettavia vaihtoehtoja kuljetuskerroksen salaamiseksi, kuin TLS.*

20) **Tietoliikenteen osapuolten varmentaminen.** Ovatko luottamusverkoston sisäiset tietoliikenneyhteyksien varmentamisvaatimukset 8 §:ssä mielestänne selkeät?

DVV
- *Eivät täysin ole [selviä]*

- *Kuinka usein tunnistuspalvelun tarjoajan tulee hakea tietojen suojaamisen käytettävää jwks_uri tietosisältöä? (Jokaisen tunnistustapahtuman yhteydessä, kerran tunnissa vai harvemmin?)*
- *Pitääkö jwks_uri tarjota kiinteästä IP-osoitteesta, jotta kutsuja voi tehdä erikseen palomuuriavauksen kohde-IP perusteisesti.*
- *Nykymallissa on teknisiä piilovaatimuksia tietoliikenteen osapuolille/hyödyntäville organisaatioille.*
- *Vaatimukset tulisi kirjata näkyville pakollisiksi vaatimuksiksi ja kaikkia osapuolia sitovaksi, tai sitten kuvata niin, että kohde/lähde IP-osoite perusteista varmennusta ei tule, tai saa käyttää, tietystä ajanhetkestä lähtien osapuolien välisessä kommunikaatiossa*

Muut

- *Voisi olla aiheellista painottaa säännöllisen avaintenvaihdon merkitystä joko suosituksella tai määräyksellä.*
- *osapuolien tunnistamiseen käytettävän avaimen vaihdon käytänne on siinä määrin yksityiskohtainen tekninen asia, että sitä ei tulisi säätää määräyksessä 72. Käytänne olisi hyvä määrittää suosituksessa 213/2018 S.*
- *avainten vaihtoon osapuolien tunnistamiseksi liittyvät käytänteet olisi hyvä harkita uudelleen ja asiakokonaisuus tulisi olennaisena asiana huomioida myös uudistettaessa määräystä 72.*
- *avainten vaihtoon ja osapuolien tunnistamiseen ei saatu yksiselitteistä ohjeistusta ja käytäntöä. Ohjeiston puuttuessa osapuolet ovat tulkinneet määräystä vaihtelevasti.*
- *Osapuolien tunnistamisesta ja avaintenvaihdosta määritettiin tarkemmin ainakin suosituksessa 213/2018 S kappaleessa 3.2.1.*
    - *…Huomionarvoista on, että kyse on aivan eri tarkoituksessa tapahtuvasta avaintenvaihdosta, kuin mitä määritetään M72 pykälässä 5.*
    - *…osapuolten tunnistamiseen käytettävät avaimet määritellään kiinteästi*
    - *…vaihtaminen edellyttää manuaalisia, ihmisen toimesta suoritettavia toimenpiteitä ja etukäteistä kommunikaatiota ja sopimista*
    - *…manuaalisesti suoritettavat toimenpiteet ja ihmisten välinen kommunikointi on vikaherkkää*
    - *…mahdollisista palvelukatkoista, kun osapuolet saattavat vaihtaa avaimia ilmoittamatta siitä etukäteen*
    - *… Nykyiseen määritykseen avainten vaihdosta on päädytty…siitä syystä, että teollisuusstandardia ei koettu riittävän turvalliseksi, mutta kuitenkaan vaihtoehtoista yhteisesti hyväksyttyä toimintamallia ei löytynyt.*
    - *nykykäytänne on näennäisesti turvallinen, mutta toisaalta aiheuttaa riskin palvelun saatavuudelle ja siten verkoston yleiselle luotettavuudelle.*
    - *…hankala avainten vaihdon käytäntö saattaa johtaa siihen, että osapuolet eivät uudista salaisia avaimiaan säännöllisesti.*
    - *Kokonaisuutena arvioiden nykyinen käytäntö ei ole täysin luotettava ja sen käytännön turvallinen toteutus on myös kyseenalaista*
- *Etenkin OIDC-tunnistuskäytännössä on teollisuusstandardeiksi kehittyneet toimivat mallit avaimien vaihtoon.*
    - *Mallit toimivat sujuvasti ilman edellytystä etukäteiseen ihmisten väliseen kommunikaatioon osapuolien välillä.*
    - *OIDC-tunnistuskäytännössä tulisi käyttää osapuolien tunnistukseen private_key_jwt -menetelmää, kuten suosituksessa todetaan.*

- *Tunnistuksessa käytettävät julkiset avaimet olisi hyvä voida noutaa osapuolen jwks_uri -osoitteesta, kuten tunnistuskäytännössä yleisesti on tapana sen sijaan, että avaimet ovat kiinteästi sidottuja.*
- *tämä käytäntö olisi riittävän turvallinen varmistaen samalla palvelun saatavuuden*

- *Vaikka useimmat toimijat käyttävät OIDC-protokollaa, osa ei ole ottanut käyttöön JWKS-rajapintojen kautta vaihdettavia avaimia tai edes muuten määritelleet avainten vaihdon menettelyprotokollaa.*

21) **Asiointipalveluyhteydet.** Onko tietoliikenneyhteyden varmentaminen ja avaintenvaihtokäytännöt asiointipalveluiden kanssa saatu toteutettua? Miten? Tarvitaanko asiasta teknistä ohjausta suosituksella, ohjeella tai määräyksellä?

DVV

- *Edellisen kohdan haasteet pätevät myös tässä.*
- *Nykytilanteessa on tullut myös esille, että tunnistuspalvelun tarjoaja (OIDC OP) määrää millä tunnisteella OIDC RP:n on käytettävä tietojen suojaamiseen käytettävää avainta, mikä lähtökohtaisesti kuuluu OIDC RP itsenäiselle ylläpitovastuulle. Ts. julkinen avain on rekisteröitävä etukäteen OIDC OP:lle, jotta saadaan selville tunniste mitä kyseistä OP:ta kohden pitää käyttää, ennen kuin avainta voi ylipäätään ottaa käyttöön. Muutos avaimen nimeämisessä voi johtaa palvelujen toimimattomuuteen esim. avaimen revokointitilanteessa.*

Muut

- *vastaus kysymyksessä 20 on sovellettavissa myös yhteyksissä asiointipalveluihin*
- *Sama ongelma koskee niin luottamusverkoston jäsenten välisiä kuin asiointipalveluiden yhteyksiä.*

22) **Käyttäjärajapinnat.** Onko käyttäjärajapinnan vaatimuksia mielestänne tarpeen muuttaa jotenkin? Miten ja miksi?

DVV

- [asiointipalvelun nimen liittyvä kommentti käsitellään attribuuttimuistiossa]
- *Uhkat, fraud…Hyökkääjä voi perustaa klooni-sivuston tunnistusvälineen tarjoajasta ja toimia ns. man-in-themiddle. Tavallisella kansalaisella ei ole keinoa havannoida kyseistä tilannetta, ellei esimerkiksi muistaa ulkoa "pankin" verkkotunnusta jota on mahdollisesti aikaisemmin käyttänyt vahvasti tunnistautumiseen.*

23) Palvelut. Onko määräyksessä vaatimuksia, joita on vaikea sovittaa yhteen käyttäjille tai asiointipalveluille tarjoamiinne tunnistuspalveluihin tai jotka hankaloittavat niiden kehittämistä?

Ficom Ry

- *Määräyksen 2 luvun tunnistusjärjestelmän ja rajapintojen salausvaatimuksia koskevan 7 §:n 4 momentin sekä tietoturvavaatimuksia tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa koskevan 8 §:n 3 momentin vaatimuksiin henkilötietojen sanomatasoisesta salauksesta ehdotetaan lisättäväksi seuraavanlainen muotoilu:*

- *Sanomatason salaus ei kuitenkaan ole välttämätön, mikäli viestiliikenne tapahtuu suoraan palvelinten välillä käyttämättä henkilön selainta kuriirina ja mainittu yhteys on salattu edellä kuvattujen vaatimusten mukaisesti.*
- *Sama voidaan myös muotoilla aloittamalla "Vaatimus sanomatason salauksesta ei koske…." ja lisäksi tarvittaessa korostaa, että "henkilötietoja sisältävä viestiliikenne tapahtuu….". Kuten kyselyssäkin on todettu, etenkin Tupas-siirtymä ja sanomatason salauksen käyttöönotto ja siihen liittyvä avaintenhallinta asiointipalvelun kanssa aiheuttivat muutostarpeita vuoden 2019 aikana. Ehdotettu muutos määräykseen mahdollistaisi nykyisin käytetyn ETSI-liikenteen.*

Muut

- *Kaksinkertainen salaus (TLS + sanomakohtainen salaus) henkilötietoja sisältävissä sanomissa vaikeuttaa havaintojemme mukaan selvästi asiointipalveluiden kehittämistä, mutta ei tuo ainakaan tavanomaisessa OIDC flow:ssa oleellista lisäarvoa tietoturvan kannalta*

48) **Kansallisen solmupisteen rajapinta.** Solmupisteen rajapinnalla luottamusverkostoon voi olla merkitystä, jos jokin luottamusverkoston tunnistusväline notifioidaan komissiolle tai jos solmupisteen ja tunnistusvälityspalvelun kautta voisi välittää ulkomaisen tunnistusvälineen käyttäjän tunnistuksen suomalaiselle yksityiselle asiointipalvelulle. Onko luottamusverkoston ja kansallisen solmupisteen välisen rajapinnan tietoturvallisuudesta määrääminen (10 §) edelleen tarpeellista huomioiden se, että luottamusverkoston ja suomi.fi:n välinen rajapinta kuuluu 9 §:n vaatimusten piiriin?

DVV

- *eIDAS-kontekstissa olisi hyvä olla oma suositus-/määrittelydokumentti, jolloin tekniset määritykset voitaisiin ottaa pois määräyksestä. Erillisen dokumentin teknisten vaatimusten ylläpito olisi tarvittaessa kevyempää.*
- *Kryptografisten vaatimusten osalta vaatimukset ja suositukset voisi täydentää osaksi Traficomin Kyberturvallisuuskeskuksen julkaisemaa kryptografisten vahvuusvaatimuksien ohjetta (190/651/2015). Algoritmien osalta tulee olla riittävä liikkumavara, jotta jonkun algoritmin tietoturvan pettäessä voidaan joustavasti siirtyä toisen algoritmin käyttöön.*

4 2020 muutosvaihtoehdot ja vaikutusarviointi

4.1 Algoritmien ja salausprofiilien ajantasaisuus: oletuslistaus säännöksessä

Arvioitava kysymys:
a) Mitkä säännöksessä listatut algoritmit, avainpituudet jne. ovat vanhentuneet ja poistettava?
b) Tarvitaanko siirtymäaikoja?
c) Mitä uusia oletusalgoritmeja on syytä lisätä?
d) **Miten erotellaan tietoliikenne-, sanomatason- ja säilyttämisen salausvaatimukset?**
e) Miten TLS 1.2 ja 1.3 ciphersuitet päivitetään perustelumuistioon - mikä lähde (viimeksi IANA)?
f) Onko tarpeen selventää perusteluissa sanomatason salausta
g) Onko tarpeen selventää perusteluissa kiintolevysalauksia?

4.1.1 Alustava sääntelyehdotus

7 Kohta Tunnistusjärjestelmän ja rajapintojen salausvaatimukset

7.1. Tietoliikenteen salaus
7.1.1 Tunnistuspalveluntarjoajien välisten ja tunnistuspalveluntarjoajan ja asiointipalvelun välisten rajapintojen liikenne on salattava. Salauksessa, avaintenvaihdossa sekä salaukseen liittyvässä allekirjoituksessa on noudatettava seuraavia menetelmiä:

a) ***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.*
b) ***Allekirjoitus**: Käytettäessä RSA:ta sähköiseen allekirjoitukseen, avaimen pituuden tulee olla vähintään 2048 bittiä. Käytettäessä elliptisen käyrän menetelmää ECDSA:ta alla olevan kunnan koon tulee olla vähintään 224 bittiä.*
c) ***Symmetrinen salaus**: Salausalgoritmin on oltava AES tai Serpent tai ChaCha20. Avaimen pituuden tulee olla vähintään 128 bittiä. Salausmoodin on oltava CBC, GCM, XTS tai CTR.*
d) ***Tiivistefunktiot**: Tiivistefunktion on oltava SHA-2, SHA-3 tai Whirlpool tai Poly1305. SHA-2:lla tarkoitetaan funktioita SHA224, SHA256, SHA384 ja SHA512.*
e) *…..*

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

…

…

7.x Säilytettävien tietojen salaus

Tunnistusjärjestelmässä säilytettävien tietojen eheydestä ja luottamuksellisuudesta on huolehdittava. Jos tiedon suojaaminen perustuu ainoastaan niiden salaukseen, sovelletaan kohdan 7.1 ~~1 momentissa~~ allekirjoittamisen, symmetrisen salaamisen ja tiivistefunktioiden vaatimuksia.

Huomioita perusteluihin:

- 7.1.1 a-d
- Määräyksessä olevat algoritmit, avainpituudet ja funktiot ovat ajan tasalla ja mitään ei tarvitse poistaa
  - CBC-salausmoodi esitetään joissakin arviointityökaluissa vanhentuneena, mutta virasto katsoo, että se on riittävän turvallinen, kunhan käytetään oikeita määrittelyjä ja päivitettyjä kirjastoja.
- Salausalgoritmien luetteloon voidaan lisätä ChaCha20. Tiivistefunktioiden listaan voidaan lisätä Poly1305.
  - NCSA:n alustava arvio on, että ChaCha20+Poly1305 - yhdistelmä voidaan katsoa riittävän turvalliseksi tunnistustoiminnan yhteydessä, vaikka NCSA-FI tai SOGIS MRA ei ole vielä virallisesti hyväksynyt POLY1305:ttä niihin tarkoituksiin, joihin kyseisiä referenssejä käytetään.
- Korkean varmuustason suositus

- Virasto arvioi, että arvot ovat ajan tasalla ja vastaavat NCSA-toiminnon määrittelyjä TL IV
- Virasto arvioi, että korkean varmuustason suosituksen arvojen muuttaminen pakolliseksi ei aiheuttaisi yhteentoimivuusongelmia. Korkean varmuustason tunnistusvälityksen välittäessä sekä korotetun että korkean varmuustason tason tunnistusta on mahdollista valita algoritmit tapahtumakohtaisesti.
- Miten vaatimus vaikuttaisi korkean varmuustason tunnistuspalveluita käyttäviin asiointipalveluihin?
- Kyselyssä tullut ehdotus korotetun ja korkean varmuustason vaatimusten yhtenäistämiseen.

- Selvennyksiä
  - Säännöksessä listatut algoritmit, arvot ja menetelmät koskevat vain säännöksen käyttötarkoitusta "*Salauksessa, avaintenvaihdossa sekä salaukseen liittyvässä allekirjoituksessa…*".
    - Neuvonnassa on tullut esille esimerkiksi epäselvyys SHA-1:n käyttämisestä satunnaisuuden luomiseen ja joitakin muita kysymyksiä. Perusteluissa pyritään selventämään esille tulleita asioita, jotka liittyvät säännöksen sanamuodon tulkintaan.
  - XTS ei sovellu tietoliikenteen salaukseen, vaan kiintolevysalaukseen
  - Kaikkia mainittuja algoritmeja jne. ei voi käyttää TLS:ssä, mutta luettelosta voidaan poimia yhdistelmät TLS 1.2 ja TLS 1.3 -profiileihin
- Lisätään perustelumuistioon TLS-ciphersuiteja
  - Perustelumuistiossa aikaisemmin mainittujen lisäksi vaatimukset täyttäviä ovat seuraavat ciphersuitet, joita NCSA käyttää arvioidessaan salaustuotteita (tasolla TL IV)
    - DHE-RSA-AES-128-CBC-SHA256
    - DHE-RSA-AES-256-CBC-SHA256
    - DHE-RSA-AES-128-GCM-SHA256
    - DHE-RSA-AES-256-GCM-SHA384
    - ECDHE-RSA-AES-128-CBC-SHA256
    - ECDHE-RSA-AES-256-CBC-SHA384
    - ECDHE-RSA-AES-128-GCM-SHA256
    - ECDHE-RSA-AES-256-GCM-SHA384
    - ECDHE-ECDSA-AES-128-CBC-SHA256
    - ECDHE-ECDSA-AES-256-CBC-SHA384
    - ECDHE-ECDSA-AES-128-GCM-SHA256
    - ECDHE-ECDSA-AES-256-GCM-SHA384
  - RFC 7905:ssä listatut (https://tools.ietf.org/html/rfc7905)
    - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
    - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
    - TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
  - Lisätään TLS 1.3 ciphersuitet [lähde RFC 8446]
    - TLS_AES_256_GCM_SHA384
    - TLS_CHACHA20_POLY1305_SHA256
    - TLS_AES_128_GCM_SHA256
    - [TLS_AES_128_CCM_SHA256]

- 7.1.2
- ei täydennettävää

4.1.2 Tunnistuspalveluiden kehitys

4.1.3 Turvallisuusvaikutukset

4.1.4 Taloudelliset vaikutukset

4.1.5 Muut ohjauskeinot

Ohje
Suositus
Yhteissääntely
Informaatiolla ohjaaminen

4.2 Salausvaatimusten määrittely/tarkkuus ja sääntelytapa

Arvioitava kysymys: Salausvaatimusten määrittely/tarkkuus ja sääntelytapa?
a) Säilytetäänkö määräyksessä tarkka listaus algoritmeista jne.?
b) Miten uudet hyvät algoritmit jne. sisällytetään joustavasti mukaan sallittuihin, jos määräystä ei ehditä päivittää? Mikä tai mitkä ovat luotettavia lähteitä, joiden mukaisia algoritmeja jne. voi käyttää määräyksessä määriteltyjen oletusten lisäksi?
c) Miten määritellään haavoittuneista algoritmeista luopuminen?

13.1.2021

4.2.1 Alustava sääntelyehdotus ja vaihtoehdot

7.1. Tietoliikenteen salaus
7.1.1 Tunnistuspalveluntarjoajien välisten ja tunnistuspalveluntarjoajan ja asiointipalvelun välisten rajapintojen liikenne on salattava. Salauksessa, avaintenvaihdossa sekä salaukseen liittyvässä allekirjoituksessa on noudatettava seuraavia menetelmiä:

*a) **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.*
*b) **Allekirjoitus**: Käytettäessä RSA:ta sähköiseen allekirjoitukseen, avaimen pituuden tulee olla vähintään 2048 bittiä. Käytettäessä elliptisen käyrän menetelmää ECDSA:ta alla olevan kunnan koon tulee olla vähintään 224 bittiä.*
*c) **Symmetrinen salaus**: Salausalgoritmin on oltava AES tai Serpent tai ChaCha20. Avaimen pituuden tulee olla vähintään 128 bittiä. Salausmoodin on oltava CBC, GCM, XTS tai CTR.*
*d) **Tiivistefunktiot**: Tiivistefunktion on oltava SHA-2, SHA-3 tai Whirlpool tai Poly1305. SHA-2:lla tarkoitetaan funktioita SHA224, SHA256, SHA384 ja SHA512.*
e) Edellä kohdissa a-d mainittujen menetelmien ja arvojen lisäksi voidaan noudattaa menetelmiä, jotka Suomen NCSA-toiminto on listannut turvallisuusluokitellun tiedon käsittelyssä [asiakirjaviite] tai SOGIS MRA on hyväksynyt [asiakirjaviite] kohdissa a -d tarkoitettuun käyttöön.

…

Turvallisten uusien algoritmien ja menetelmien salliminen

Nykymuotoisessa sääntelyssä on toimijoiden kokemuksen ja viraston arvion perusteella tarvetta mahdollistaa uusien vahvojen algoritmien käyttö.

Se voidaan tehdä määräystä päivittämällä, mutta koska määräyksen muuttaminen voi olla hidasta, on tarpeen määritellä joustavampi malli määräyksen listan täydentämiselle.

Viraston kyselyn vastauksissa on ehdotettu tarkan määräyksen asemasta viittaamista esimerkiksi Kyberturvallisuuskeskuksen NCSA-toiminnon julkaisemaan hyväksyttyjen algoritmien ja avainpituuksien asiakirjaan.

Virasto pitää NCSA:n listaa soveltuvana lähteenä, ja sitä on käytetty perustana ja vertailukohtana määräystä annettaessa. Toisena ajantasaisena ja relevanttina lähteenä virasto pitää SOGIS MRA:n ylläpitämää listaa. Virasto katsoo kuitenkin, että määräystä ei voi korvata viittauksella näihin lähteisiin. NCSA:n ja SOGIS MRA:n listoja ylläpidetään eri tarkoitukseen ja ne voivat joltain osin olla tarpeettoman tiukkoja korotetun varmuustason tunnistamisen vaatimuksiin nähden.

Virasto arvioi myös valvontakokemuksen perusteella, että vähimmäisvaatimukset on tarpeellista määrätä yksiselitteisesti.

Tarpeellisen joustavuuden lisäämiseksi virasto harkitsee ensisijaisesti mallia, jossa määräykseen listattujen lisäksi voidaan käyttää NCSA:n tai SOGIS MRA:n listoilla olevia algoritmeja ja arvoja.

<u>Haavoittuvat algoritmit</u>

Toinen esille tuotu näkökohta on määräyksessä listattujen algoritmien tai arvojen muuttuminen haavoittuviksi ja siitä aiheutuva tarve luopua niiden käytöstä.

Virasto arvioi, että sääntelyn ennakoitavuuden takia tällaisten ehdoton kieltäminen edellyttää määräyksen muuttamista. Salausmenetelmien haavoittuvuudet eivät ilmene kovin äkillisesti, joten niihin on pääsääntöisesti mahdollista reagoida riittävän nopeasti määräysmuutoksella.

Sen lisäksi tarkoituksenmukainen tapa huomioida haavoittuvuudet on seurata niitä koskevia tiedotuskanavia ja luopua omaehtoisesti haavoittuvien menetelmien käytöstä. Tunnistuspalveluilla on mahdollisuus ja määräyksen 5 §:n mukaan velvollisuus ylläpitää tunnistuspalveluidensa tietoliikenne-, tietojärjestelmä- ja käyttöturvallisuutta. Haavoittuvuuksien seurannan tarkentamista arvioidaan 5 §:n yhteydessä ja soveltamiskäytäntöä voidaan tarkentaa sen perusteluissa. Haavoittuvuuksiin reagoimista voidaan tarvittaessa ohjata viraston suosituksella.

4.2.2 Tunnistuspalveluiden kehitys

Tunnistuspalveluiden tarjonnassa on tarpeellista mahdollistaa ICT-palveluiden käyttö ja niissä tarjolla olevat uusimmat turvalliset salausratkaisut.
Määräyksen vaatimuksissa on tarpeen huomioida tunnistuspalveluiden turvallisuuden vaatimustaso eikä sidota vaatimuksia kansallisen tai kansainvälisen turvaluokitellun tiedon vaatimustasoon.

4.2.3 Turvallisuusvaikutukset

4.2.4 Taloudelliset vaikutukset

Ei erityisiä huomioita.

4.2.5 Muut ohjauskeinot

Ohje
Suositus. Salausmenetelmien haavoittuvuuksiin reagoimista voidaan tarvittaessa ohjata viraston suosituksella.
Yhteissääntely
Informaatiolla ohjaaminen

4.3 TLS-vähimmäistaso

Arvioitava kysymys: Poistetaanko TLS 1.1?

4.3.1 Alustava sääntelyehdotus

7 Kohta Tunnistusjärjestelmän ja rajapintojen salausvaatimukset

7.1 Tietoliikenteen salaus
…
7.1.3 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.~~
~~…~~

4.3.2 Tunnistuspalveluiden kehitys

Tietoliikenneyhteyksien TLS-protokollan versio vaikuttaa siihen, kuinka vanhoja päätelaitteita tai selaimia käyttäjät voivat käyttää.

Tätä harkittiin määräysvalmistelussa jo 2016. Tuolloin arvioitiin kuitenkin toimijoiden palautteen perusteella, että käyttäjillä voi olla vielä mobiilipäätelaitteita, jotka eivät tue TLS 1.2:ta

Virasto arvioi, että tilanne on viiden vuoden aikana muuttunut siten, että päätelaitekanta tukee hyvin kattavasti vähintään TLS 1.2 -versiota. Käyttöön on jo tulossa TLS 1.3.

Vaatimusten tiukentamisessa on arvioitava mahdollinen siirtymäajan tarve.

4.3.3 Referenssit

eIDAS Cryptographic Requirements for the Interoperability Framework, version 1.2

2.1 TLS version …eIDAS nodes MUST use TLS 1.2. Prior TLS versions MUST NOT be accepted.

4.3.4 Turvallisuusvaikutukset

TLS-vähimmäistaso nostetaan versioon TLS 1.2.
TLS 1.1 -poikkeusta ei enää jatkossa sallittaisi
TLS 1.1 on vuodelta 2006 ja siinä on tiedossa haavoittuvuuksia.

4.3.5 Taloudelliset vaikutukset

TLS-version päivittäminen on osa tavanomaista teknistä kehittämistä. Kustannuksia voi aiheutua käyttäjien tiedottaminen.

4.3.6 Muut ohjauskeinot

Ohje. Asia on 2016 määrätty määräyksessä, joten vaatimuksen muuttaminen edellyttää määräyksen muuttamista. Tunnistuspalveluiden tasapuolisen kilpailuaseman takaamiseksi vähimmäistaso ja mahdollinen siirtymäaika on tarpeen määrätä.
Suositus.
Yhteissääntely. Luottamusverkoston yhteistoimintaryhmä tai muut tunnistuspalveluiden yhteisöt voivat tarvittaessa koordinoida viestintää muutoksesta.
Informaatiolla ohjaaminen.

4.4 Tietoliikenteen osapuolten tunnistus ja avaintenvaihdon vaatimukset

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

4.4.1 Alustava sääntelyehdotus ja vaihtoehdot

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

~~Salausmenetelmien tulee täyttää edellä 7 §:n 1 - 4 momentissa määrätyt vaatimukset.~~

8.1 Tunnistuspalveluiden välisillä ja tunnistuspalvelun ja asiointipalvelun välisessä tietoliikenteessä on tunnistettava [uudet] osapuolet ja siten varmistettava liikenteen tai sanomien salaamisessa käytettävien [varmenteen ja] avainten aitous/eheys ja niiden haltijat. Tunnistamisen on perustuttava suoraan kahdenväliseen menettelyyn eikä se voi perustua pelkästään osapuolen yleisesti luotettuun varmenteeseen.

8.2 Edellä kohdassa 8.1 tarkoitetut avaimet on uusittava säännöllisesti
a) 8.1 kohdan mukaisella menettelyllä,
b) allekirjoittamalla uudet avaimet 8.1 kohdan mukaisesti aiemmin toimitetulla avaimella tai
c) toimittamalla uudet avaimet tietoliikenneyhteydellä, jonka eheys [ja luottamuksellisuus] on varmistettu sitomalla osapuolten tietoliikenne kohdan 8.1 mukaisesti toimitettuihin varmenteisiin (certificate pinning)

~~Osapuolten tunnistamisessa ja tunnistamisessa tarvittavan tiedon välityksessä tulee käyttää metadataa tai vastaavia menettelyitä, jotka takaavat vastaavan tietoturvatason.~~

Ks. myös 9 kohta

9 kohta Tunnistussanomien salaaminen/luottamuksellisuus~~Tietoturvavaatimukset asiointipalvelurajapinnassa~~

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

9.1 Sanomien salaus

Tunnistuspalveluiden välisessä ja tunnistuspalvelun ja asiointipalvelun välisessä tietoliikenteessä on suojattava~~H h~~enkilötietoja sisältävien tunnistussanomien eheys ja luottamuksellisuus

a) varmistamalla tietoliikenneyhteyden eheys [ja luottamuksellisuus] sitomalla osapuolten tietoliikenne kohdan 8.1 mukaisesti toimitettuihin varmenteisiin (certificate pinning) [tai muulla vastaavan lopputuloksen takaavalla menettelyllä] tai
b) salaamalla sanomat kohdan 8.1 menettelyllä toimitetulla avaimella.

9.2 Jos tunnistussanomat välitetään käyttäjän päätelaitteen/selaimen/…kautta, sanomat on salattava 9.1.b) mukaisesti.

9.3 Tunnistusanoman salaamisessa on noudatettava [soveltuvin osin] kohdan 7.1 menettelyjä ~~Henkilötietoja sisältävien sanomien eheys ja luottamuksellisuus on suojattava edellä 1 momentissa tarkoitetun liikenteen salauksen lisäksi sanomatasolla 1 momentin mukaisesti.~~

~~on suojattava~~

~~Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tulee huolehtiahenkilötietojen luottamuksellisuudesta ja eheydestä asiointipalvelu- ja käyttäjärajapinnassa.~~

Commented [LA2]: Perusteluihin: molemmissa päissä

Tarkennetaan määräykseen *vaihtoehdot t*ietoliikenteen osapuolen varmentamiselle sekä avaintenvaihdon ja päivittämisen perusvaatimukset.

Vaatimusten tarkoitus on varmistaa, että tunnistustapahtumat välitetään luottamusverkoston sisällä ja luottamusverkostosta ulos vain luotettavasti varmennetuille organisaatioille. Vaatimusten tarkoitus on myös varmistaa tietoliikenteen ja sanomien eheys ja luottamuksellisuus. Siksi tässä yhteydessä on arvioitu myös sanomatason salausvaatimuksia.

Sääntelyn tavoitteista,
- vrt. https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20Cryptographic%20Requirement%20v1.2%20Final.pdf?version=2&modificationDate=1571068651805&api=v2
- …to protect
- confidentiality of the person identification data,
- authenticity/integrity of the person identification data, and
- secure identification of communication end-points.

Seuraavassa on jäsennetty osapuolten varmentamisen ja liikenteen ja sanomatason salauksen toteutusvaihtoehtoja ja perusteluja.

1) 8.1 Uuden luottamussuhteen perustaminen (nyk. 8.2 §)
- saadaan toiselta osapuolelta julkinen avain, *johon voidaan luottaa*
- Mihin luottamus voi perustua:
  - Edellyttää nimenomaisia toimenpiteitä
  - Osapuolen varmenne ("A") on toimitettava siten, että sen haltijasta voidaan nimenomaisesti varmistua
- Ei voi perustua *pelkästään* siihen, että toisella osapuolella on luotettu varmenne
  - riippumatta siitä, minkä laatuinen ko. varmenne on (QWAC, QeSeal, EV, muu)
  - TUPAS-aikana luottamussuhteen perustaminen on perustunut reaalimaailman avaintenvaihtoon. Jos käytäntö nyt tässä kohdin muuttuisi siten, että luotetaan tavanomaisen liikennöintikäytännön mukaisesti muihinkin varmenteisiin kuin säädettyihin, turvallisuus ei olisi enää samalla riittävällä tasolla.
  - varmenne ei sinänsä osoita, että sen varmentama avainpari on oikealla haltijalla
  - lisäksi vaikka CA ja varmenne olisi luotettava, voi konfiguroinnissa helposti käytännössä jäädä varmistamatta, että kelpuutetaan vain ko. varmenne, koska tämä ei ole tyypillinen perustoiminne
  - varmenteen myöntämisessä ei arvioida haltijan avaintenhallinnan käytäntöjä

- Vrt. PSD2-vaatimuksissa luotetaan eIDAS-asetuksen hyväksyttyyn verkkosivujen todentamisen tai sähköisen leiman varmenteeseen. Lisävaatimuksena se, että ko. toimijoita valvovat finanssisektorin viranomaiset ja toimijat löytyvät viranomaisen rekisteristä.

- Toteutettavuus
  OIDC: jwks_uri -osoite ei yksistään riitä luotettavaan osapuolen varmentamiseen, vaan on käytettävä myös muita menettelyjä
  - SAML: …¨
  - Kyselyssä kommentti: *Pitääkö jwks_uri tarjota kiinteästä IP-osoitteesta, jotta kutsuja voi tehdä erikseen palomuuriavauksen kohde-IP perusteisesti.*
    - Liittynee käytännön toteutukseen, varmennetaanko domain vai IP-osoite.
    - Certificate pinning on mahdollinen molemmissa tilanteissa.
    - Kiinteä IP-palomuuriavaus voi kuitenkin olla vain lisäkontrolli.

2) Liikenteen ("putken") salaaminen (7.1 §)
- vaihtoehto 1:
- ankkuroidaan/sidotaan liikenne aina A-varmenteeseen (certificate pinning) molemmissa päissä
  - vaiheen 1 varmennetta A käytetään liikenteen salaamisessa (TLS)
  - ks. certificate pinning vaiheessa 3
- vaihtoehto 2:
- osapuolen tunnistamisen luotettavuus toteutuu sillä perusteella, että sanomatason salausavainten vaihto on tehty vastaavasti kuin A-varmenteen
  - liikennettä ei siis *sidota* varmenteeseen A,
  - liikenne salaus perustuu
    - varmenteeseen A
    - TAI
    - Muuhun luotettavaan varmenteeseen (suositellaan EV, QWAC, QeSeal)
- Toteutettavuus
  - OIDC ja SAML eivät eroa tässä suhteessa

3) Tunnistustapahtumien välittäminen (ja sanomatason salaaminen)
- vaihtoehto 1: sanomien turvallisuus perustuu vaiheen 2 vaihtoehtoon 1 eli A-varmenteen certificate pinningiin, jolloin erillinen sanomien salaaminen ei ole tarpeen niiden luottamuksellisuuden varmistamiseksi
  - OIDC: Sanomatason salaus voidaan korvata tällä menettelyllä
- vaihtoehto 2: Sanomatason salaus perustuu vaiheen 1 mukaisesti saatuihin avaimiin
  - SAML: SAML-toteutuksessa, jossa tietoliikenne/sanomat välitetään käyttäjän selaimen kautta, sanomatason salausta ei voi korvata liikenteen kiinnittämisellä A-varmenteeseen, koska sanomat puretaan selaimessa. SAML mahdollistaisi myös muunlaiset toteutukset, joita ei kuitenkaan tyypillisesti käytettäne.

4) 8.2 Osapuolen varmenteen/avainten päivittäminen/uusiminen
- 1) Sama menettely kuin luottamussuhdetta perustettaessa
- 2) Luotetun kanavan kautta, jos on käytetty A-varmenteen certificate pinningiä
  - OIDC: jwks
  - SAML: päivitetty metadata
- 3) luotetaan turvallisesti toimitettuun allekirjoitusavaimeen
  - OIDC: jwks voidaan allekirjoittaa manuaalisesti toimitetulla avaimella. OIDC:ssä ei ole valmiina määrittelyä tälle menettelylle. Tästä voi aiheutua yhteentoimivuusongelmia.
  - SAML: SAML-metadata voidaan allekirjoittaa manuaalisesti toimitetulla avaimella. Ei ole tarkistettu, onko SAMLissa tälle mahdollisesti valmis määrittely.

- 4) Luotetaan turvallisesti toimitettuihin avaimiin, joita käytetään sanomatason salauksessa
  - OIDC: päivitetään manuaalisesti/erillisellä menettelyllä
  - SAML: tarkistetaan SAMLin määrittelyt
-
- Avainten päivityssykli
  - Ylläpitoasia, jossa huomioitava mm. riskit avainten joutumisesta vääriin käsiin tai algoritmien vanhenemisesta
  - Tarkistetaan vallitsevat hyvät käytännöt ja referenssit, esim. NIST (tarkista lähde) oletus 2 vuotta
  - Kommentti kyselyssä: *Kuinka usein tunnistuspalvelun tarjoajan tulee hakea tietojen suojaamisen käytettävää jwks_uri tietosisältöä? (Jokaisen tunnistustapahtuman yhteydessä, kerran tunnissa vai harvemmin?)*
    - toimivuuskysymys, sillä vanhentuneilla avaimilla tunnistussanomat eivät aukea

4.4.2 Referenssit

Vrt. eIDAS Cryptographic Requirements for the Interoperability Framework, version 1.2

> *2.4 certificates*
>
> *Until 2017, eIDAS nodes MUST use extended validation certificates or qualified website certificates1 for TLS. As of 2018, newly issued TLS certificates for eIDAS nodes MUST be qualified.*
>
> Tätä määrittelyä ollaan muuttamassa (EV-varmenne)
> Lisäksi SAML-metadata -käytännöt [täydennetään tarvittaessa]

Vrt. https://openid.net/wg/fapi/

Vrt. Liikenne- ja viestintäviraston suositus 213/2018 (OIDC) S - päivitetään 213/2021

> *The use of extended validation (EV) certificates is RECOMMENDED. eIDAS-notified IdPs may also be subject to additional security requirements based on the eIDAS regulations.*

4.4.3 Tunnistuspalveluiden kehitys ja turvallisuus

Tietoliikenteen osapuolen varmentaminen on perusluonteinen osa luotettavaa sähköistä tunnistuspalvelua. Sähköisessä tunnistamisessa on huolehdittava myös siitä, että tietoliikenne ja sanomat ovat aitoja ja pysyvät luottamuksellisina.

Teknisen kehityksen näkökulmasta on muistettava, että aikaisemmin TUPAS-protokollaa käytettäessä käytäntönä oli antaa toiselle osapuolelle yhteinen jaettu avain jollain manuaalisella reaalimaailman asiointimenettelyllä sopimuksen tekemisen yhteydessä. Tällä käytännöllä pystyttiin identifioimaan tietoliikenteen toinen osapuoli luotettavasti ja varmistumaan transaktioiden eheydestä.

Siirryttäessä OIDC- tai SAML-protokollan käyttöön käytettävissä olisi teknisesti standardoituja menettelyjä tietoliikenteen käynnistämiseen uuden osapuolen kanssa. Siksi on tarpeen arvioida, voidaanko näitä käyttää vahvan sähköisen tunnistamisen tietoliikenneyhteyksien osapuolten varmentamisessa.

OIDC- ja SAML-protokollien perusmenettelyt perustuvat internetin yleisiin käytäntöihin. Ne mahdollistavat automaattisen luottosuhteen perustamisen, mikä edistää yhteentoimivuutta ja

käytettävyyttä, mutta ei turvaa luottosuhteen osapuolen riittävän luotettavaa varmentamista eikä eheyttä ja luottamuksellisuutta.

Rekisteröityjen tunnistuspalveluiden lukumäärä on rajattu, kun taas tunnistusta käyttävien asiointipalveluiden määrä on suuri ja kasvaa toivottavasti jatkuvasti. Siksi on erityisesti tarpeen punnita käytettävyyden ja turvallisuuden suhdetta ja arvioida, voisiko asiointipalveluiden kanssa olla perusteita käyttää erilaisia menettelyjä kuin luottamusverkoston sisällä. Tunnistamisen toimittaminen oikealle asiointipalvelulle on kuitenkin olennainen osa vahvan sähköisen tunnistamisen luotettavuutta. Liikenne- ja viestintävirasto ei ole tunnistanut perusteita sille, että tunnistusvälityspalvelun ja asiointipalvelun tietoliikenneyhteyden luottosuhteen perustaminen ja tunnistustapahtumien toimittaminen ei edellyttäisi yhtä vahvaa luotettavuutta kuin luottamusverkoston sisäinen tietoliikenne. Virasto ei ole tunnistanut myöskään kompensoivia turvatoimia, joilla vastaava vaikutus voitaisiin saavuttaa.

Linjaukset

Osapuolen varmentamisessa ei voida tukeutua pelkästään protokollissa määriteltyihin peruskäytäntöihin, vaan edellytetään erityisiä menettelyjä varmistamaan tietoliikenteen varmenteen tai avainten kuuluminen tietoliikenteen osapuolelle.

Vaatimukset ovat samat luottamusverkoston toimijoiden välillä ja tunnistuspalvelun ja asiointipalvelun välillä.

4.4.4 Toteutettavuus

SAML-protokollaa käytettäessä tietoliikenteen osapuolten varmentaminen perustuu sähköisesti allekirjoitettuun metadataan ja …

OIDC-protokollan mukaisessa perustoteutuksessa luottamus tietoliikenteen osapuoleen perustuu TLS:n perustana käytettyyn varmenteeseen ja on mahdollista perustaa luottosuhde automaattisesti. Siten luotettavuuden taso perustuu varmenteen luotettavuuteen.

Tunnistuspalveluiden tarjoajien kommenteissa on arvioitu, että manuaaliset menettelyt voivat johtaa virheisiin, ennakoimattomiin palvelukatkoksiin tai avainten päivittämisen laiminlyönteihin. Liikenne- ja viestintävirasto arvioi, että pitämällä voimassa useampia avainpareja ja uusimalla näitä eri aikoina voidaan turvata se, että muutokset eivät aiheuta katkoksia.

4.4.5 Taloudelliset vaikutukset

Osapuolten varmentaminen ja salausavainten hallinta aiheuttaa jonkin verran kustannuksia, mutta tätä voitaneen pitää tunnistuspalveluissa perusluonteisena ICT-toteutuksiin liittyvänä kustannuksena.

Automatisoidut tai etänä hoidettavat prosessit olisivat oletettavasti kustannustehokkaampia. Tunnistuspalvelusta tehdään kuitenkin aina sopimus, jossa sovitaan palvelun toimittamiseen liittyvistä asioista, ja tässä prosessissa voidaan toteuttaa myös varmenteiden ja avainten luotettava toimittaminen.

On erotettava uuden luottamussuhteen perustaminen ja varmenteiden uusiminen sopimussuhteen aikana. Certificate pinning mahdollistaa automatisoidun prosessin avainten ylläpidossa.

4.4.6 Muut ohjauskeinot

Ohje. Osapuolten varmentamisen ja avaintenvaihdon käytännöistä on tähän asti puuttunut viranomaisen ohje.
Suositus. Vaatimukset voidaan lisätä rajapintasuosituksiin. Kyselyssä saatiin kommentteja siitä, että suosituksia ei sovelleta yhdenmukaisesti. Siksi virasto ei pidä ohjetta tai suositusta riittävän tehokkaana keinona varmistaa riittävän luotettavia käytäntöjä asiointipalveluiden varmentamisessa.
Yhteissääntely. Avaintenvaihdon käytännöistä on pyritty kokoamaan yhteisiä käytäntöjä luottamusverkoston yhteistoimintaryhmässä. Viraston arvio on, että yhtenäisiä käytäntöjä, joihin kaikki voisivat sitoutua, ei ole löytynyt. Tunnistuspalvelut toivovat viranomaiselta määrittelyä siitä, mikä on hyväksyttävä menettely.
Informaatiolla ohjaaminen. Ei tarkasteltu.

4.5 Sanomatason salaus

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

4.5.1 Lähtötilanne, säännökset ja perustelut

7 § Henkilötietoja sisältävien sanomien eheys ja luottamuksellisuus on suojattava edellä 1 momentissa tarkoitetun liikenteen salauksen lisäksi sanomatasolla 1 momentin mukaisesti.

MPS: Pykälän 4 momentin mukaan sen lisäksi, että tietoliikenneyhteys on salattu 1 momentin mukaisesti, henkilötietoja sisältävät sanomat on salattava. Vastaava määrittely on tehty sanomien salaukselle kansallisten solmupisteiden välisessä liikenteessä. Salausvahvuuden on täytettävä 1 momentin vaatimukset. Sanomatason salausvaatimus koskee liikennettä, säilytettävästä tiedosta säädetään 5 momentissa.

8 § *Kaikki henkilötiedot tulee salata ja allekirjoittaa sanomatasolla.*

MPS: *Kaikki henkilötiedot tulee salata ja allekirjoittaa sanomatasolla. Pelkkä siirtotien salaus ei siis riitä. Asiaa käsitellään vaikutusarvioinnin (ks. A osa) luvussa 3 TUPAS-tarkastelun yhteydessä.*

9 § Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tulee huolehtia henkilötietojen luottamuksellisuudesta ja eheydestä asiointipalvelu- ja käyttäjärajapinnassa.

MPS: Pykälän 2 momentin vaatimus perustuu vaikutusarvioinnin (ks. A osa) luvussa 3 kuvattuun henkilötunnuksen käsittelyn vaatimuksiin. Vaatimukseen liittyvää siirtymäaikaa TUPAS-protokollaa käytettäessä käsitellään 25 §:n kohdalla. Vaatimuksen tarkoitus on estää se, että henkilötunnus tai muut henkilötiedot välitetään päätelaiterajapinnassa siten, että ne voivat tallentua selkokielisinä esimerkiksi päätelaitteen selailuhistoriaan tai tietoliikenneyhteydellä oleville palvelimille.

Commented [LA3]: Voi tallentua myös esim. palvelimille matkan varrella.

EU:n varmuustasoasetus (EU) 2015/1502

2.4.6 Tekniset tarkastukset (LUE: Kontrollit tai toimenpiteet)

MATALA

1. Käytössä on oikeasuhteiset tekniset tarkastukset palvelujen turvallisuuteen kohdistuvien riskien hallitsemiseksi ja käsiteltävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi.

2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät sähköisen viestinnän kanavat on suojattu salakuuntelulta, manipuloinnilta ja toistolta.

5. Kaikki laitteet ja välineet, jotka sisältävät henkilötietoja, salattuja tietoja tai muita arkaluonteisia tietoja, säilytetään, kuljetetaan ja hävitetään turvallisella ja varmalla tavalla.

Soveltamisohje:

On tärkeää pitää erillään luottamuksellisuuden ja eheyden suojaamista koskevien vaatimusten arviointi. Eheyden (tai aitouden) suojaaminen määräytyy periaatteessa varmuustason mukaan, mutta henkilöihin liittyvän tiedon luottamuksellisuuteen vaikuttavat myös tietojen tyyppi sekä mahdolliset suojaamista koskevat lainsäädännölliset vaatimukset.

Henkilötietojen luottamuksellisuus on suojattava ja käytössä on oltava turvatoimenpiteitä, jotka pohjautuvat riskiperusteista lähestymistapaa hyödyntävään arviointiin valitun tietoturvallisuuden hallintajärjestelmän mukaisesti. Turvatoimenpiteiden kattamia osa-alueita ovat esimerkiksi tietomurrot, väärinkäytökset, palvelunestohyökkäykset ja hajautetut palvelunestohyökkäykset.

2.3.1 Todentamismekanismi

MATALA

*2. Jos henkilön tunnistetiedot **tallennetaan** osana todentamismekanismia, nämä tiedot on suojattu niiden menetykseltä ja vaarantamiselta, mukaan lukien analyysi verkkoympäristön ulkopuolella.*

Commented [LA4]: Tämä liittyy sekä tunnistustapahtuman toteuttamiseen että sen tallentamiseen tai tallentumiseen.

Soveltamisohje:

Tallennettuihin henkilötietoihin pääsyä on valvottava huolellisesti. Henkilön tunnistetietojen suojaamisessa käytettäviä menetelmiä ovat esimerkiksi Euroopan unionin verkko- ja tietoturvaviraston ENISAn "Algorithms, Key Sizes and Parameters Report" -asiakirjan, kansallisten salausohjeiden tai muiden hyvien toimintatapojen mukainen salaaminen ja tiivistäminen. Käyttöoikeuksia on aina valvottava.

MPS2016:

Henkilötunnus on tietosuojalain ~~henkilötietolain~~ 29 §:n perusteella katsottavat tunnisteeksi, jota on käsiteltävä erityisen huolellisesti. Edellä poimituista kohdista voidaan ainakin EU:n varmuustasoasetuksen 2.4.6 kohdan 1 alakohdan katsoa soveltuvan suoraan myös asiointipalvelurajapintaan. Vaikka tämän ja muiden poimittujen kohtien vaatimukset kohdistuvat suoranaisesti tunnistuspalveluntarjoajan omiin

järjestelmiin, tukevat ne myös henkilötiedon suojaamista asiointipalvelurajapinnassa. Jos henkilötunnusta on suojattava tiukasti palveluntarjoajan järjestelmässä, ei ole suhteessa näihin vaatimuksiin, jos sen voi luovuttaa asiointipalvelurajapinnassa tavalla, joka altistaa tunnuksen luottamuksellisuuden menettämiselle.

2021 Tietosuojalaki ja GDPR:

Tietosuojalain 29 §:n 4 §:ssä käsitellään henkilötunnuksen esittämistä

Henkilötunnusta ei tule merkitä tarpeettomasti henkilörekisterin perusteella tulostettuihin tai laadittuihin asiakirjoihin.

Henkilötietojen tietoturvaa koskee yleisen tietosuoja-asetuksen 32 artikla.

32 artikla Käsittelyn turvallisuus

1. Ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten

a) henkilötietojen pseudonymisointi ja salaus;
[…]

2. Asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota erityisesti käsittelyn sisältämiin riskeihin, erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi.

[…]

4.5.2 Alustava sääntelyehdotus ja vaihtoehdot

9 kohta Tunnistussanomien salaaminen/luottamuksellisuus~~Tietoturvavaatimukset asiointipalvelurajapinnassa~~

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

9.1 Sanomien salaus

Tunnistuspalveluiden välisessä ja tunnistuspalvelun ja asiointipalvelun välisessä tietoliikenteessä on suojattava~~H~~ henkilötietoja sisältävien tunnistussanomien eheys ja luottamuksellisuus
h) varmistamalla tietoliikenneyhteyden eheys [ja luottamuksellisuus] sitomalla osapuolten tietoliikenne kohdan 8.1 mukaisesti toimitettuihin varmenteisiin (certificate pinning) [tai muulla vastaavan lopputuloksen takaavalla menettelyllä] tai
i) salaamalla sanomat kohdan 8.1 menettelyllä toimitetulla avaimella.

9.2 Jos tunnistussanomat välitetään käyttäjän päätelaitteen/selaimen/…kautta, sanomat on salattava 9.1.b) mukaisesti.

9.3 Sanomatason salauksessa on käytettävä [soveltuvin osin] kohdan 7.1 mukaisia menettelyjä. ~~Henkilötietoja sisältävien sanomien eheys ja luottamuksellisuus on suojattava edellä 1 momentissa tarkoitetun liikenteen salauksen lisäksi sanomatasolla 1 momentin mukaisesti.~~

~~Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tulee huolehtiahenkilötietojen luottamuksellisuudesta ja eheydestä asiointipalvelu- ja käyttäjärajapinnassa.~~

Commented [LA5]: Perusteluihin: molemmissa päissä

Tavoitteet

- Henkilötiedot eivät paljastu oikeudettomasti selaimessa tai palvelimilla tai missään
- Henkilötunnusta koskee erityinen suoja
- Vahvistus autentikoinnista ja henkilötiedot toimitetaan todentamisessa vain oikealle asiointipalvelulle
- Tunnistustapahtumaa ei voi väärentää/toisintaa (tamper/replay) tms. eli todentamismekanismin turvallisuus ei vaarannu

Vaihtoehdot

- Ei muutosta
- Sanomatason salaus ei pakollinen, jos muilla turvakontrolleilla voidaan kompensoida riskit
- Sanomatason salauksen tarpeellisuus arvioidaan protokollakohtaisesti (käytännön toteutettavuutta käsitellään perusteluissa protokollakohtaisesti, mutta vaatimusta ei määritellä niille erikseen)
- Sanomatason salausvaatimuksen tarpeellisuus arvioidaan erikseen luottamusverkoston sisällä ja luottamusverkoston ulkorajapinnoissa

Alustavat linjaukset

Sanomatason salausvaatimusta muutetaan siten, että se ei ole pakollista, jos sanomien luottamuksellisuus voidaan turvata muulla tavalla.

Mahdollisuudet toteuttaa muita suojaustapoja voivat vaihdella eri protokollissa ja toteutuksissa. Relevantteja tarkasteltavia protokollia ovat OIDC, SAML ja ETSI MSS.

Suojaustapojen on estettävä se, että tietoliikenteen mahdollinen purkaminen "matkan varrella" palvelimilla tai tallentuminen salaamattomana käyttäjän päätelaitteelle voi altistaa tunnistussanomat ja henkilötiedot oikeudettomalle paljastumiselle tai väärinkäytölle.

Ei arvioida suojaamistarvetta sen perusteella, millainen henkilötieto tunnistussanomassa välitetään ("*on alaikäinen*" vrt. on "*121212+999Å, Alma Virtanen*"). Rajanveto olisi vaikea perustella ja toteutukset on yksinkertaisinta tehdä kaikille tunnistustapahtumille samalla tavalla.

4.5.3 Referenssit

Vrt. eIDAS Cryptographic Requirements for the Interoperability Framework, version 1.2

https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20Cryptographic%20Requirement%20v.1.2%20Final.pdf?version=2&modificationDate=1571068651805&api=v2

Yleistä

Within the eIDAS Interoperability Framework, communication between eIDAS nodes (i.e. eIDAS-Services and eIDAS-Connectors) is performed via the citizen's browser. Here, the content of the communication between eIDAS nodes is performed using cryptographically protected SAML messages. To secure the transport layer of this communication between these components and the citizen's browser, TLS is used.

This document specifies cryptographic requirements for the protection of the SAML communication as well as on the usage of TLS within this communication.

Sanomien allekirjoitus ja salaus

- Rajat ylittävän tunnistamisen määrittelyssä
- sanomien allekirjoittaminen on määritelty pakolliseksi
- sanoman sisällön allekirjoitus ja salaaminen on valinnaista
- vrt. M72 sanomatason salausvaatimuksessa ei ole eritelty sanoman allekirjoitusta ja sisällön salaamista, mutta edellytetään kokonaisuutena sanomien eheyden ja luottamuksellisuuden varmistamista salauksella

> *3.1. GENERAL REQUIREMENTS*
>
> *The following rules MUST apply to the SAML communication between eIDAS nodes:*
> *• SAML request and SAML response messages MUST be signed by the sending party.*
> *• The signature of a SAML assertion is OPTIONAL.*
> *• The (signed) SAML assertion within the SAML response message MUST be encrypted.*
>
> *Ephemeral keys or random numbers (for nonces or generation of ephemeral keys) SHALL be used only once. It is REQUIRED that random numbers to be used within SAML are generated with cryptographically secure random number generators that provide sufficient entropy (according to the security level of 120 bits).*
>
> *3.2. XML ENCRYPTION WITH SAML*
>
> *To protect the confidentiality of data, a hybrid crypto system is used. The content MUST be encrypted via symmetric cryptography (Content Encryption) and the corresponding symmetric key (Session Key) MUST be randomly generated for each transmission. A static public key of the receiver MUST be used to encrypt the session key (Key Encryption).*
>
> *3.2.1 Content Encryption*
>
> *For content encryption, algorithms of the following list MUST be supported:*
> *• http://www.w3.org/2009/xmlenc11#aes128-gcm*
> *• http://www.w3.org/2009/xmlenc11#aes256-gcm*
> *Additionally, the following algorithms MAY be supported:*
> *• http://www.w3.org/2009/xmlenc11#aes192-gcm*
> *Other algorithms than listed above SHALL NOT be used or accepted for content encryption.*

4.5.4 Tunnistuspalveluiden kehitys,

4.5.5 Turvallisuusvaikutukset

Missä tunnistussanomat voivat tallentua ja paljastua oikeudettomasti……tietoliikennepalvelimilla, käyttäjän päätelaitteessa

Tunnistusvälityspalvelun ja asiointipalvelun välillä sanoman suojaamisen voi toteuttaa joko sanoman salauksella (nyky)vaatimusten mukaisesti) tai alla kuvatulla menettelyllä.

Tilanteet, joissa tunnistussanoma **ei kierrä käyttäjän päätelaitteessa (esim. selaimessa)** (OIDC/ETSI MSS), vaan **tunnistuspalveluntarjoajien tunnistusjärjestelmien (palvelinten välillä)** siten **suojattuna, että sitä ei pureta missään välissä tietoliikenneyhteydellä**.

- Tämä voidaan varmistaa esimerkiksi tietoliikenteen sitomisella ennalta määriteltyihin varmenteisiin (certificate pinning, mTLS) siten, että pystytään varmistamaan päästä-päähän sekä tietoliikenneyhteyden molempien päiden varmenteen luotettavuus ja se, että liikennettä ei pureta muualla kuin osapuolten tunnistuspalvelun tuottamiseen liittyvissä järjestelmissä.
- Tämä edellyttää sitä, että varmenteen luotettavuus on nimenomaisesti erikseen tähän tarkoitukseen varmistettu ja luottamus ei perustu yleisesti luotettuihin CA:hin.
- Pohjaoletuksena on luonnollisesti, että tietoliikenneyhteys ("TLS-putki") on salattu määräyksen vaatimusten mukaisesti.

SAML-toteutuksessa, jossa tietoliikenne/sanomat välitetään käyttäjän selaimen kautta, yllä mainittu menettely ei ole mahdollinen. SAML mahdollistaisi myös muunlaiset toteutukset, joita ei kuitenkaan tyypillisesti käytettäne.

- Onko tarkasteltava tarkemmin?

Viraston arvion mukaan esimerkiksi MPLS-yhteydet eivät tarjoa riittäviä turvakontrolleja tähän tarkoitukseen.

Jos tietoliikenneyhteyden suojauksessa/salaamisessa käytetään TLS-salauksen sijasta IPsec-VPN (virtual private network) -toteutusta, siinä on tehtävä vastaavat sanomien luottamuksellisuutta turvaavat toimenpiteet. Viraston käsityksen ja määräyksen muutostarpeiden kyselyyn saatujen vastausten perusteella vallitseva ja relevantti käytäntö tietoliikenneyhteyksillä on kuitenkin TLS.

Sanomatason salauksessa käytetyt menettelyt

- Onko referenssejä
- Esim. https://tools.ietf.org/html/rfc7519

4.5.6 Taloudelliset vaikutukset

4.5.7 Muut ohjauskeinot

Ohje.
Suositus.
Yhteissääntely.
Informaatiolla ohjaaminen.

4.6 Kansallisen solmupisteen ja tunnistusvälityspalvelun rajapinnan vaatimukset

Ei arvioitu vielä

5 Säädäntö

5.1 Määräyksen antamisen perusta

5.2 Asiaan liittyvät säännökset

5.3 Muu sääntely