TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Määräys 72 työpajat 2020-2021

Määräys 72 A/2018 M sähköisistä tunnistus- ja luottamuspalveluista

Työpajat

16.12.2020-10.6.2021

Työtapa

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

Määräystyöpajojen aikataulu

Aika	Materiaali	Aihe	Lisätyöpaja (tarvittaessa)
KE 16.12.2020 9-11.30	7.12.2020	Tunnistus: rajapinnat ja attribuutit	KE 3.2.2021 9-11
KE 20.1.2021 9-11.30	11.1.2021	**Tunnistus:** **Salaus, osapuolten varmentaminen ja avaintenvaihto**	KE 3.2.2021 9-11
KE 10.2.2021 9-11.30	1.2.2021	Tunnistus: tunnistusjärjestelmän tekniset vaatimukset ja arviointi	KE 17.2.2021 9-11
KE 10.3.2021 9-11.30	1.3.2021	Tunnistus: tunnistusmenetelmä, PSD2-vertailu Blockchain ja SSI	KE 17.3.2021 9-11
KE 15.4.2021 9-11.30	1.4.2021	Luottamuspalvelut: palveluiden ja arvioinnin ETSI-standardit	TO 22.4. ~~KE 21.4~~. 2021 9-11
KE 12.5.2021	3.5.2021	Keskeneräiset aiheet	TO 20.5.2021 9-11
TO 10.6.2021 9-11.30	3.6.2021	Koko määräys ja perustelut	

Jatkoaikataulu – muutokset mahdollisia

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

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Työpaja 2/7

Salaus, osapuolten varmentaminen, avaintenvaihto

Määräys 72 työpajat 2020-2021
Työpaja 2/7 agenda

- Mahdolliset kommentit työpajan 16.12.2020 päätelmiin
- Salaus, osapuolten varmentaminen, avaintenvaihto

  1) Algoritmien ja menetelmien ajantasaisuus ja täydennykset

  2) Salausvaatimusten sääntelytapa ja NCSA-FI/SOGIS MRA täydennykset

  3) TLS 1.2 vähimmäistasoksi, TLS 1.1. kieltäminen

  4) Tietoliikenteen osapuolten tunnistus ja avaintenvaihto

  5) Tietoliikenneyhteyden certificate pinning ja sanomatason salaus suojauksen vaihtoehdoiksi

  6) Muut salausasiat (ei valmisteltu)
- Seuraava työpaja

20.1. työpajan osallistujat

- Työpajassa oli paikalla n. 30 henkilöä seuraavista organisaatioista
  - Aktia, Danske, Handelsbanken, Nordea, OP, POP-pankit, S-Pankki, Säästöpankit, Ålandsbanken
  - DNA, Elisa, Telia
  - Samlink, Ubisecure
  - F-Secure
  - DVV, KKV, Fiva
  - Finanssiala, FiCom

Tunnistus

M72 Luku 2 Tunnistuspalvelun tietoturvavaatimukset

7 § Tunnistusjärjestelmän ja rajapintojen salausvaatimukset

8 § Tietoturvavaatimukset tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa

9 § Tietoturvavaatimukset asiointipalvelurajapinnassa

1) Algoritmien ja menetelmien ajantasaisuus ja täydennykset: alustava muutosehdotus (huom. täydennetty 10.2.2021, ks. kalvot 25-35)

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 [*lisäys sanomatason salauksen takia*: tai epäsymmetrinen salaus]: Käytettäessä RSA:ta ~~sähköiseen allekirjoitukseen~~, avaimen pituuden tulee olla vähintään 2048 bittiä. Käytettäessä elliptisen käyrän menetelmää ECDSA:ta [*lisäys: *tai EdDSA: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, [*mahd. lisäys: *CCM], GCM, XTS tai CTR.*

*d) Tiivistefunktiot: Tiivistefunktion on oltava SHA-2, SHA-3 tai Whirlpool tai Poly1305. [*siirretään perusteluihin säännöksestä ja täydennetään SHA-3*: SHA-2:lla tarkoitetaan funktioita SHA224, SHA256, SHA384 ja SHA512. ...]*

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

1) Algoritmien ja menetelmien ajantasaisuus ja täydennykset: arvio ja vaikutukset

- Turvallisuus:
  - algoritmit, avainpituudet ja funktiot ovat ajan tasalla ja mitään ei tarvitse poistaa
    - CBC-salausmoodi 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
- Toteutettavuus ja soveltaminen:
  - Säännöksessä listatut algoritmit, arvot ja menetelmät koskevat vain säännöksen käyttötarkoitusta *"Salauksessa, avaintenvaihdossa sekä salaukseen liittyvässä allekirjoituksessa…".*
  - TLS 1.2 ja 1.3 ciphersuit-esimerkkejä täydennetään perusteluissa
- Kehitys: muutos mahdollistaa alustapalveluiden uudet vaihtoehdot

Kommentit työpajassa 20.1.2021/algoritmien ja menetelmien ajantasaisuus

- Viraston arvioon voimassa olevan säännöksen algoritmien ja menetelmien ajantasaisuudesta ei esitetty mitään kommentteja
- Kommentteja ei esitetty myöskään ehdotukseen lisätä ChaCha20 ja Poly1305 säännöksen listalle
- Kysyttiin, ovatko ChaCha20 ja Poly1305 sallittuja ennen kuin muutettu määräys tulee voimaan (arvio 1-2/2022)
- Traficomin päätelmät:
  - Määräysmuutos voidaan valmistella valmistelumuistion säännösluonnoksen pohjalta
  - Virasto ei pidä tarpeellisena kieltää ChaCha20+Poly1305 käyttöä ennen muutetun määräyksen voimaantuloa. Oikeudellisesti virasto voi tehdä
    a) määräyksen osittaismuutoksen tai
    b) kirjallisen valvontalinjauksen, ettei virasto salausvaatimusten valvonnassa puutu ChaCha20-algoritmin ja Poly1305-tiivistefunktion käyttöön määräyksen 72 7 §:n valvonnassa ennen uusitun määräyksen voimaantuloa.
  - Virasto on päätynyt tekemään asiasta valvontalinjauksen (b-kohta).

2) Salausvaatimusten sääntelytapa: alustava muutosehdotus, NCSA-FI/SOGIS MRA täydennykset

7.1. Tietoliikenteen salaus

7.1.1 ...Salauksessa, avaintenvaihdossa sekä salaukseen liittyvässä allekirjoituksessa on noudatettava seuraavia menetelmiä:

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.*

- Turvallisuusvaikutukset:
  - Viitatut lähteet tasoltaan luotettavia
- Tekninen toteutettavuus:
  - Määriteltyjen lähteiden mukaiset menettelyt joustavasti käytössä siinä tapauksessa, että määräystä ei ole ehditty täydentää
- Taloudelliset vaikutukset:
  - Ei velvoita, vaan mahdollistaa
- Virasto ei katso, että koko säännös voidaan korvata viittauksella.
  - Sääntelyn tehokkuus, ennakoitavuus ja kohtuullinen vaatimustaso

Kommentit työpajassa 20.1.2021 /salausvaatimusten sääntelytapa ja NCSA sekä SOGIS MRA -lisäykset

- Hyvin vähän kommentteja
- Ehdotus ok
- Tarkennuspyyntö, miksi tarvitaan a-d –kohdat eli oma lista määräyksessä eikä vain viitata NCSA-FI –toiminnon listaan
- Traficomin päätelmät:
  - Määräysmuutos voidaan valmistella valmistelumuistion säännösluonnoksen pohjalta
  - Traficom ei pidä tarkoituksenmukaisena korvata säännöstä kokonaan NCSA-FI:n listalla, koska määräyksessä on tehty ja on tarpeen tehdä lievennyksiä siihen nähden. Listaa ylläpidetään eri tarkoitusta varten ja myös sen päivittäminen on kiinni muista asioista kuin tunnistussääntelyn tarpeista.

3) TLS 1.2 vähimmäistasoksi, TLS 1.1. kieltäminen

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.~~

- Turvallisuusvaikutukset:
  - TLS 1.1 on vuodelta 2006 ja siinä on tiedossa haavoittuvuuksia.
- Tekninen kehitys ja toteutettavuus:
  - TLS 1.1. poikkeus ollut voimassa 11/2016-> 5 vuotta, (2022 6 vuotta)
  - Viraston arvio: päätelaitekanta tukee hyvin kattavasti vähintään TLS 1.2 -versiota. Käyttöön on jo tulossa TLS 1.3.
  - vaikuttaa siihen, kuinka vanhoja päätelaitteita tai selaimia käyttäjät voivat käyttää
  - Onko tarvetta siirtymäajalle?
  - Muiden yhteyskäytäntöjen kuin TLS määrittelylle ei kyselyn perusteella edelleenkään tarvetta
- Taloudelliset vaikutukset:
  - käyttäjien tiedottaminen

Kommentit työpajassa 20.1.2021 /TLS 1.1 kieltäminen

- Keskusteltiin mobiilipäätelaitteiden kyvystä tukea vähintään TLS 1.2:ta
  - Kysyttiin, onko virastolla tarkempia tietoja päätelaitteiden TLS-tuesta, jotta voisi hahmottaa kuinka suuri käytännön vaikutus on.
  - Kommentoitiin, että suurimmalla osalla mobiilipankeista ja tunnuslukusovelluksista vaikuttaa olevan Androidin versio 5 tai 6 minimivaatimuksena.
  - TLS 1.2 tuki löytyy Androidin versiosta 5 eteenpäin (rajoitetusti 4:ssa).
  - Kokemusta, että on vaadittu TLS 1.2:ta, eikä ole saatu kertaakaan palautetta ongelmista.
  - Tällä perusteella muutos ei aiheuta ongelmia käyttäjien päätelaitteiden takia.
- Edellisestä sääntelymuutoksesta eli TLS 1.0 kieltämisestä saatu kokemus oli, että on tunnistuspalveluiden tarjonnan ja tasapuolisen kilpailun kannalta hyvä, että kaikilla on velvollisuus tehdä muutos samaan aikaan.
- Traficomin päätelmät:
  - Määräysmuutos voidaan valmistella valmistelumuistion säännösluonnoksen pohjalta
  - Alustava arvio palautteen perusteella on, että siirtymäaikaa ei tarvita.
  - Viraston arvio on, että päätelaitteita ilman TLS 1.2 –tukea Suomessa on hyvin vähän.

4) Tietoliikenteen osapuolten tunnistus ja avaintenvaihto, alustava sääntelyehdotus

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

*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~~.

4) Tietoliikenteen osapuolten tunnistus ja avaintenvaihto, vaikutukset

- Turvallisuusvaikutukset:
  - varmistaa, että tunnistustapahtumat välitetään luottamusverkoston sisällä ja luottamusverkostosta ulos vain oikeille tahoille
    - ei perusteita erotella luottamusverkoston ja asiointipalveluiden vaatimuksia
  - varmistaa tietoliikenteen ja sanomien eheys ja luottamuksellisuus
  - luottamussuhteen perustaminen on kriittinen vaihe
    - ei voida tukeutua pelkästään protokollissa määriteltyihin peruskäytäntöihin, vaan edellytetään erityisiä menettelyjä varmistamaan tietoliikenteen varmenteen tai avainten kuuluminen tietoliikenteen osapuolelle
  - Avainten ylläpidossa voidaan nojata perustamisvaiheessa rakennettuun luottamukseen
- Tekninen toteutettavuus ja soveltaminen:
  - Käytännöt ja vaatimukset ovat olleet epäselvät, joten selvennetään yhtenäiset vaatimukset
  - Käytännön toimet mahdollista tehdä sopimusprosessien yhteydessä
  - Luottamussuhde voidaan perustaa TLS-varmenteisiin tai sanomatason salausavaimiin
- Taloudelliset vaikutukset: prosessikustannukset

4) Tietoliikenteen osapuolten tunnistus ja avaintenvaihto, soveltaminen

- *Suora kahdenvälinen menettely*
  - osapuolen varmenne/avaimet on toimitettava siten, että sen haltijasta voidaan nimenomaisesti varmistua
  - Kahdenvälinen: ei voi perustua pelkästään siihen, että toisella osapuolella on luotettu varmenne riippumatta siitä, minkä laatuinen ko. varmenne on (QWAC, QeSeal, EV, muu)
- Uusimismenettelyt
  - 1) Suora kahdenvälinen menettely tai
  - 2) Uusien avainten/metadatan allekirjoitus kahdenvälisesti aikaisemmin toimitetulla avaimella tai
    - *OIDC:ssä ei valmista määrittelyä jwks:n allekirjoittamiselle*
    - SAML-metadata
  - 3) Uusien avainten/metadatan toimittaminen putkessa, jossa certificate pinning kahdenvälisesti toimitettuun varmenteeseen
    - Jwks
- *uusittava säännöllisesti*
  - Ylläpitosykli, ~2 v välein tai tiheämmin
  - Myös häiriötilanteessa/(korruptoituneet) luonnollisesti uusittava

Kommentit työpajassa 20.1.2021/ tietoliikenteen osapuolten tunnistus ja avaintenvaihto

- Säännöksen tarkennusehdotus herätti paljon tarkennuskysymyksiä ja kommentteja toteutustavoista ja vaikutuksista
- Varmenteen/avainten kahdenvälinen toimitusmenettely ja niiden haltijan tunnistaminen luottamussuhdetta perustettaessa
- Säännösehdotus: ”...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.”
  - Vaatimus sinänsä ok
  - soveltamiseen pyydettiin tarkennuksia: Mikä on riittävä tapa tunnistaa toinen osapuoli, mikä täyttää vaatimukset? Pitäisikö olla turvasähköposti tai esim. vahva sähköinen tunnistaminen vastaanottajan edustajalle? Olisiko esimerkkiä tunnistustavasta, joka EI ole määräyksen mukainen?
- Traficomin kommentit ja päätelmät:
  - Ei ole valmisteltu soveltamisohjeita tunnistamisesta tai käytännön menettelystä.
  - Sopimuksen tekemisen yhteydessä varmistuttaneen sopimusosapuolesta.
  - Esimerkkinä käytännön toimitustavoista turvasähköposti olisi varmastikin hyvä, webbilomake ilman tunnistusta taas ei. Jos saamme kysymyksiä/ehdotuksia, esimerkkejä hyvästä soveltamiskäytännöstä voidaan laittaa perustelumuistoon.
  - Määräysmuutosta voidaan valmistella valmistelumuistion säännösluonnoksen pohjalta. Perustelujen laatimisessa yritetään huomioida esitetyt kysymykset.

Kommentit työpajassa 20.1.2021/sertifikaattien käytäntöjä

- Certificate pinningin toteutukseen vaikuttavat käytännöt
  - Maksullisilla varmentajilla tyypillinen vaihtumissykli on vuosi
  - On tavallista, että asiointipalvelu käyttää varmennetta, joka uusitaan 3 kuukauden välein (usein Let’s Encrypt). Liikenne olisi siis pinnattava 3 kk välein uuteen varmenteeseen.
  - Varmenteen vaihtaminen ei tarkoita aina avaimen vaihtamista, myös Let’s Enscryptillä mahdollista
  - Suuntaus on käyttää lyhyempiä avaimia ja päivittää niitä tiheästi, esim. viikon päivityssykli sanomatason salausavainten päivittämiselle jwks:lle luottamusverkoston sisällä
  - Kommentoitiin, miten vaikuttaa se, että 2 tunnistuspalvelua, joilla ei ole käytössä OIDC:tä
- Traficomin kommentit ja päätelmät:
  - Yleisesti Traficom pitää kommenttien perusteella kuitenkin tarpeellisena tarkentaa/yhtenäistää/vahvistaa asiointipalveluiden varmentamista
  - Vallitsevat käytännöt eivät ole olleet aikaisemmin Traficomin tiedossa. Traficom on pohtinut säännösehdotuksen teknisen käytännön toteutuksen vaihtoehtoja. Niitä esitetään jäljempänä ja niitä voi vielä kommentoida.

Kommentit työpajassa 20.1.2021/ certificate pinning

- Certificate pinningin toteutus, tarvittavat toimenpiteet kahdensuuntaisessa certificate pinningissä (mTLS)
- Säännösehdotus: ”sitomalla osapuolten tietoliikenne kohdan 8.1 mukaisesti toimitettuihin varmenteisiin”
  - Pinningia on käytetty pääosin mobiililaitteissa haitallisilta verkoilta suojautumiseen, mutta tässä sen soveltaminen on hankalampaa.
  - Certificate pinning asiointipalvelun suuntaan ei onnistu, eli käytännössä asiointipalvelut eivät saisi muuttaa avaimia (lopulta kuitenkin välttämätöntä) tai sitten kaikissa asiointipalveluissa on rakennettava ketjutusmekanismi. Vaatisi, että kaikki toimijat tekevät teknisen päivityksen ja koodaavat uuden mekanismin.
  - paljon manuaalista työtä, kun sertifikaatteja uusitaan
  - Varmenteen vaihtaminen ei aina tarkoita avainten vaihtamista – mutta eikö pinnaus tehdä sertifikaatin hashiin, joka vaihtuu aina
  - ”staattisiin avaimiin ei pidä mennä”
  - Varmenteita on voitava vaihtaa ja kilpailuttaa
- Traficomin kommentit ja päätelmät:
  - pinnaus ei voi olla pelkästään CA:han, vaan nimenomaiseen varmenteeseen/julkiseen avaimeen
  - Traficom on pohtinut säännösehdotuksen teknisen käytännön toteutuksen vaihtoehtoja. Niitä esitetään jäljempänä ja niitä voi vielä kommentoida.

Kommentit työpajassa 20.1.2021/ avainten päivitys

- Varmenteen/avainten päivitysmenettelyt, Vaihtoehto 3: Uusien avainten/metadatan toimittaminen putkessa, jossa certificate pinning kahdenvälisesti toimitettuun varmenteeseen
- Säännösehdotus: ”toimittamalla uudet avaimet tietoliikenneyhteydellä, jonka eheys [ja luottamuksellisuus] on varmistettu sitomalla osapuolten tietoliikenne kohdan 8.1 mukaisesti toimitettuihin varmenteisiin (certificate pinning)”
  - ongelmallinen, koska jos tunnistuspalvelu vaihtaa sertifikaatin issueria, niin kaikki joutuvat päivittämään certificate pinningin
  - Varmenteita on voitava vaihtaa ja kilpailuttaa
  - Haitallinen sääntelymuutos, jos vaikuttaa niin, että siirrytään käyttämään enemmän staattisia avaimia
- Traficomin päätelmät:
  - Traficom on pohtinut säännösehdotuksen teknisen käytännön toteutuksen vaihtoehtoja. Niitä esitetään jäljempänä ja niitä voi vielä kommentoida.

Kommentit työpajassa 20.1.2021/ avainten päivitys

- Varmenteen/avainten päivitysmenettelyt, Vaihtoehto 2: Uusien avainten/metadatan allekirjoitus kahdenvälisesti aikaisemmin toimitetulla avaimella
- Säännösehdotus: ”allekirjoittamalla uudet avaimet 8.1 kohdan mukaisesti aiemmin toimitetulla avaimella”
  - (asiointipalvelun) sertifikaatin uusimiseen ei ole standardoitua menettelyä
  - Traficom: OIDC:ssä uusimisessa voisi käyttää jwks:ää, jos sen allekirjoittaa aikaisemmin varmistetulla avaimella (”ketjutus”). Näin vältytään manuaalisilta avaintenvaihdoilta.
  - ketjuttamisen ajatus on ok, mutta toteutus edellyttää muutoksia asiointipalveluihin.
  - Kaikkien tunnistuspalveluiden olisi tässä tapauksessa tehtävä tekninen päivitys ja olisi hyvä määritellä yhteinen yhdenmukainen mekanismi (jwks:n allekirjoittamiselle).
- Traficomin päätelmät:
  - Palaute vahvisti arvion, että vallitsevaan protokollaan OIDC:iin olisi mahdollista toteuttaa jwks:n sähköinen allekirjoitus, vaikka sitä ei ole standardissa valmiiksi määriteltynä
  - Tekninen määrittely voitaisiin mahdollisesti tehdä luottamusverkoston yhteistoimintaryhmässä ja lisätä rajapintasuosituksiin, mutta tätä ei voida pitää kovin tarkoituksenmukaisena. Pyritään löytämään muita valmiimpia/valmiiksi standardoituja ratkaisuja.

Määräyksen 7-9 kohtien teknisen toteuttavuuden jatkokysymykset

10.2.2021

Jatkokysymykset 10.2.2021/nykytilakuvaus

- Varmistettuja tietoliikenneyhteyksiä (TLS+cert pinning) ja nopeasti vaihtuvia OIDC avaimia (JWKS) käytetään jo luottamusverkoston sisällä ainakin joidenkin toimijoiden kesken
  - Oletus/kysymys: Esitetty uusi toimintatapa ei siis olisi ongelmana luottamusverkoston sisällä
- Aiemmissa teknisen ryhmän työpajoissa on käsitelty asiointipalveluiden kohdalla avainten vaihtoon liittyviä haasteita. Virastolla on käsitys että asiointipalveluiden OIDC –avainten kohdalla toimitaan manuaalisesti ja avaimet ovat suhteellisen pitkäikäisiä
  - Kysymys: Onko oletus oikea? Vai onko käytössä jo muitakin tapoja?
- Määräystyöpajassa tuotiin esille asiointipalveluiden käytäntö hankkia tietoliikenneyhteyden salaamiseen tarkoitetut varmenteet Let’s Encryptin DV-varmenteina
- Huomioitava seikka: SAML ja OIDC luottamusmalli on erilainen

Jatkokysymykset 10.2.2021/ Sääntelyehdotuksen reunaehdot

- Luottosuhde (asiakassuhde) tulee perustaa turvallisesti
  - Teknisessä luottosuhteen toteutuksessa pyritään siis hahmottamaan nyt uusia vaihtoehtoja (seuraavat kalvot)
- Henkilötietoja siirrettäessä ei voida tinkiä luottamuksellisuudesta eikä eheydestä.
- Tunnistussanomia käsiteltäessä ei voida tinkiä eheydestä.
- Ulotuttava asiointipalvelulle asti
- Luottamuksellisuuden ja eheyden takaavat avaimet eivät voi olla voimassa ”ikuisesti”
- Asiointipalveluiden liittymistä luottamusverkoston asiakkaaksi ei tule monimutkaistaa tarpeettomasti – käytetään alustojen, yhteyskäytäntöjen ja ohjelmistojen olemassa olevia toimintoja hyväksi, kunhan ne ovat riittävän turvallisia

Jatkokysymykset 10.2.2021/ Toteutusvaihtoehto 1: turvallinen kanava (TLS+Cert pinning)

- Tietoliikenneyhteyden varmistukseen käytetty eheä julkinen avain toimitetaan ja otetaan käyttöön turvallisesti, kahdenvälisellä menettelyllä
- Toimitettu julkinen avain yksilöi ja toteuttaa tietoliikenneyhteyden luottamuksellisuuden (julkinen avain pinnataan)
- Avain (ja myös varmenne) pitää vaihtaa vähintään kahden vuoden välein

-- Mahdollistetaan esim. Let's Encrypt varmenteiden käyttö ja niiden nopeampi uusimissykli (uusi varmenne samalle avainparille)

-- JWKS:n ja OIDC –avainten protokollan mukainen (automaattinen) päivityssykli

-- Ei pakotettua sanomatason salausvaatimusta

-- Erityinen huolellisuus kohdistuu tämän (pinning key) salausmateriaalin suojaamiseen ja uusimiseen

- ❑ Kysymys: onko toteutuskelpoinen luottamusverkoston sisällä?
- ❑ Kysymys: onko toteutuskelpoinen asiointipalveluille ja onko mahdollista huolehtia konfiguroinnin toimivuudesta asiointipalvelussa siten, ettei automaattisessa uusimisessa vaihdeta avainta, vaan ainoastaan varmenne.

Jatkokysymykset 10.2.2021/ Toteutusvaihtoehto 2: X5c sanomatason salausavainten uusiminen

- JWKS:ssä olevat avaimet on sidottu varmenteeseen
  - Pohjana turvallinen kahdenkeskeinen tapa tämän luottamussuhteen perustamiseen
  - Uusimisessa: luottamus voisi perustua varmenteeseen/sen myöntäjään
  - **Tässä vaihtoehdossa tulisi säännökseen lisävaatimus varmenteen laadusta**
    - esim. Let's Encrypt DV-varmenteita ei hyväksyttäisi
    - QWAC, eIDAS qualified
    - (mahdollisesti EV-varmenteet – harkittava vielä, onko mahdollista tunnistaa/määritellä määräykseen, mitkä näistä riittävän luotettavia)
- Sanomatason salaus edelleen vaatimuksena

  -- Ei tarvetta TLS pinnaukselle

  -- Mahdollistaisi automaattisen OIDC avainten rotaation

  -- OIDC core speksien mukainen käytäntö

  -- Luottosuhteen määrittävät salaisuudet vaihdettava turvallisesti, vaatinee manuaalista toimenpidettä(??)

  -- CA-vaatimus

- Kysymys: onko toteutuskelpoinen asiointipalveluille huomioiden varmenteen luotettavuusvaatimukset

Jatkokysymykset 10.2.2021/ Toteutusvaihtoehto 3: DNSSEC:n vaatimus yhdessä TLS:n ja JWKS endpointin kanssa

- Työpajassa esitetty vaihtoehto: varmistetaan JWKS endpointin olemassaoloa/oikeellisuutta DNSSECiin perustuen
- Ei poista sanomatason salausvaatimusta
- Virasto arvioi, onko tämä vain hyvä lisäkäytäntö vai voiko korvata esimerkiksi edellisellä kalvolla esitetyn vaihtoehdon.

-- Olemassa olevaa Internet infraa ja muutenkin hyvä käytäntö

-- Mahdollistaisi automaattisen OIDC avainten rotaation

-- Toteutuksen tekeminen oikein pitää varmistaa, ja voi olla haasteellista

  - DANE oltava käytössä, sen ohjelmistotukea ei välttämättä ole sovelluksissa laajalti tarjolla
  - clientin resolver on määriteltävä käyttämään DNSSEC tekniikkaa hard fail tilassa

❑ Kysymys: onko toteutuskelpoinen luottamusverkoston sisällä tai asiointipalveluiden kanssa huomioiden se, että konfiguroinnin on oltava kovimpien määritysten mukainen?

Jatkokysymykset 10.2.2021/ Kooste standardin mahdollistamista vaihtoehdoista

- Mahdollisesti määräysehdotuksen mukaan ok:
- End-to-end TLS with certificate pinning + **JWT encryption** + Rotation of Encryption keys (JWKS, x5c), regular renewal (every year) of pinning keys
- TLS + **JWT Encryption**, Rotation of encryption keys (JWKS, x5c), regular renewal of certificate (and keys) used for x5c
- End-to-end TLS with public key pinning + Rotation of encryption keys (JWKS), regular renewal (every 2 years) of pinning keys used in establishing the secure channel (End-to-end TLS)
- Nykyinen käytäntö: TLS + **JWT Encryption**, Manual rotation of encryption keys (off line, secure method)

- Kovennetuilla määrittelyillä voisi tulla määräyksessä vaihtoehdoksi
- TLS with DNSSEC, **JWT Encryption**, Rotation of encryption keys (JWKS)

- Eivät täytä vaatimuksia
- TLS, **JWT Encryption**, Rotation of encryption keys (JWKS)
- TLS, JWT signing, rotation of signing keys (JWKS)

Jatkokysymykset 10.2.2021/ Sanomien allekirjoitus ja salaus – krypto – ks. myös taulukko seuraavalla kalvolla

- Sanomien salauksen vaatimusten sääntelyyn tarvittava yhteensovittaminen määräyksen 7 kohdan kryptovaatimusten kanssa
- Alustava säännösmuotoilu:
- *9 Tunnistussanomien salaaminen/luottamuksellisuus*
- *9.3 Sanomatason salauksessa on käytettävä soveltuvin osin kohdan 7.1 mukaisia menettelyjä.*
  - *Perustelut: "Soveltuvin osin" = 7.1 kohtaa muutettu siten, että sanomatason salauksen elementit löytyvät sieltä (muutokset, ks. kalvo 34)*
  - *Perustelut: Viraston rajapintasuosituksissa on ennestään ohjeita sanomatason salauksesta. Ko. taulukoihin voidaan viitata perusteluissa tai tuoda taulukot myös perusteluihin. Seuraavalle kalvolle on koottu OIDC-toteutuksen määrittelyjä rajapintasuosituksesta 213*
  - *Perustelut: Vallitseva ja hyvä käytäntö on käyttää RSAES-OAEP:ia*
- Kysymys: onko toteutuskelpoinen?
- Kysymys: Onko sanomatason salaukselle muita toteutusmalleja, jotka eivät sovi yhteen muutetun 7.1 –kohdan kanssa?

Jatkokysymykset 10.2.2021/ Sanomien allekirjoitus ja salaus – krypto (rajapintasuositus 213 taulukko OIDC, vastaava on SAMLista)

Header	Usage	Value	Algorithm	Status in FTN
alg	JWS	RS256	RSASSA-PKCS1-v1_5 using SHA-256	REQUIRED
alg	JWS	PS256	RSASSA-PSS using SHA-256 and MGF1 with SHA-256	OPTIONAL
alg	JWS	ES256	ECDSA using P-256 and SHA-256	OPTIONAL
alg	JWE	RSA-OAEP	RSAES OAEP using default parameters	REQUIRED
alg	JWE	RSA-OAEP-256	RSAES OAEP using SHA-256 and MGF1 with SHA-256	OPTIONAL
alg	JWE	ECDH-ES	Elliptic Curve Diffie-Hellman Ephemeral Static key agreement using Concat KDF	OPTIONAL
enc	JWE	A128GCM	AES GCM using 128-bit key	REQUIRED

1) Algoritmien ja menetelmien ajantasaisuus ja täydennykset: alustava muutosehdotus (huom. täydennetty 10.2.2021, ks. kalvot 25-35)

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 [*lisäys sanomatason salauksen takia*: tai epäsymmetrinen salaus]: Käytettäessä RSA:ta ~~sähköiseen allekirjoitukseen~~, avaimen pituuden tulee olla vähintään 2048 bittiä. Käytettäessä elliptisen käyrän menetelmää ECDSA:ta [*lisäys: *tai EdDSA: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, [*mahd. lisäys: *CCM], GCM, XTS tai CTR.*

*d) Tiivistefunktiot: Tiivistefunktion on oltava SHA-2, SHA-3 tai Whirlpool tai Poly1305. [*siirretään perusteluihin säännöksestä ja täydennetään SHA-3*: SHA-2:lla tarkoitetaan funktioita SHA224, SHA256, SHA384 ja SHA512. ...]*

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

Jatkokysymykset 10.2.2021 päättyvät tähän

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Työpajassa 20.1.2021 esitetty jatkuu

Nykyiset sanomatason salaussäännökset, sääntelyrakenne

- ~~*7 § Tunnistusjärjestelmän ja rajapintojen salausvaatimukset*~~
  - ~~*7 § 4 mom. Henkilötietoja sisältävien sanomien eheys ja luottamuksellisuus on suojattava edellä 1 momentissa tarkoitetun liikenteen salauksen lisäksi sanomatasolla 1 momentin mukaisesti.*~~
  - Yleisvaatimus: sanomat salattava
- ~~*8 § Tietoturvavaatimukset tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa*~~
  - ~~*8 § 3 mom. Kaikki henkilötiedot tulee salata ja allekirjoittaa sanomatasolla.*~~
  - Vaatimuksen korostaminen luottamusverkoston sisällä
- ~~*9 § Tietoturvavaatimukset asiointipalvelurajapinnassa*~~
  - ~~*9 § 2 mom. Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tulee huolehtia henkilötietojen luottamuksellisuudesta ja eheydestä asiointipalvelu- ja käyttäjärajapinnassa.*~~
  - Vaatimuksen korostaminen asiointipalveluiden ja käyttäjän päätelaitteiden suuntaan

5) Sanomatason salaus, alustava sääntelyehdotus

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

9.1 Sanomien salaus

Tunnistuspalveluiden välisessä ja tunnistuspalvelun ja asiointipalvelun välisessä tietoliikenteessä on suojattava henkilötietoja 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 Sanomatason salauksessa on käytettävä [soveltuvin osin] kohdan 7.1 mukaisia menettelyjä.

- **Kaikkien osapuolten suhteet samaan säännökseen**
- **Uusi vaihtoehtoinen menettely mahdollinen, jos sanomia ei välitetä selaimen kautta**

5) Sanomatason salaus, sääntelyehdotus: vaikutukset

- Turvallisuusvaikutukset:
  - Henkilötiedot eivät paljastu oikeudettomasti selaimessa tai palvelimilla
    - Sanomien salauksen vaihtoehdoksi tietoliikenneyhteyden luottamuksellisuuden varmistus
  - Henkilötunnusta koskee tietosuojasääntelyssä erityinen suoja, mutta ei perustetta rajata muitakaan henkilötietoja suojan ulkopuolelle.
  - Vahvistus autentikoinnista ja henkilötiedot toimitetaan todentamisessa vain oikealle asiointipalvelulle
  - Tunnistustapahtumaa ei voi väärentää/toisintaa (tamper/replay)
  - ei perustetta erotella luottamusverkoston ja asiointipalveluiden vaatimuksia
- Tekninen toteutettavuus:
  - Mahdollisuudet toteuttaa muita suojaustapoja voivat vaihdella eri protokollissa (OIDC, SAML, ETSI MSS) ja toteutuksissa
  - vaatimus teknisesti neutraali
  - 7 kohdan algoritmien ja menetelmien soveltamisesta ei ole esimerkkejä (ciphersuitet)
- Taloudelliset vaikutukset:
  - yleisiä havaintoja uuden vaihtoehdon mahdollistamisen vaikutuksesta

Kommentit työpajassa 20.1.2021/sanomatason salaus

- Kommentoitiin, että muutosehdotus on kannatettava
- On hyvä, että avataan uusia käytäntöjä eikä suljeta vanhoja pois.
- Certificate pinningistä todettiin sama kuin edellisessä aihepiirissä, että varmenteiden tiheä uusiminen aiheuttaa teknisiä vaikeuksia. Certificate pinning torjuu tietynlaisia hyökkäyksiä ja on sikäli soveltuva.
- Ehdotettiin, että voisi käyttää jwks certificate chainia: JWKS tukee tietyn sertifikaatin jakamista, jolloin ketjussa voitaisiin allekirjoittaa sertifikaatti identity providerin omalla certillä, joka olisi luotettu vastaanottajan puolella.
- Traficomin päätelmät:
  - Määräysmuutosta voidaan valmistella valmistelumuistion säännösluonnoksen pohjalta.
  - Lisäpohdintaa teknisestä toteutettavuudesta, ks. kalvot edellä
    - Sanomatason salauksen vaihtoehtona tietoliikenneyhteyden certificate pinningin toteutettavuutta on vielä selvitettävä.
    - Jwks certificate chain sanomatason salausavainten vaihtamisessa.
- **KS. edellä kalvot 25-35 jatkokysymykset**

6) Muut asiat

- 1) Hybridisalaus, algoritmit- ja menetelmät
  - Pohdittava vielä, miten huomioidaan määräyksessä – 7 kohdassa vai 9 kohdassa sanomatason salausvaatimuksissa (esim. RSAES-OAEP ja avaintenhallinta)
- 2) korkean varmuustason algoritmien ja menetelmien suositus (7 kohdan tiukennukset)
  - Vaihtoehdot säilyttää sellaisenaan perusteluissa tai siirtää määräykseen korkean varmuustason vaatimuksena
- 3) haavoittuvat algoritmit tai menettelyt
  - Huolehditaan haavoittuvuuksien seurannalla, täydennetään 5 §:n perusteluja
- 4)Tietojen säilyttämisen salausvaatimukset
  - Sisällöllisesti tarkoitus säilyttää säännös ja soveltamisohje sellaisenaan
  - Harkitaan siirtämistä 5 §:ään
- 5) salausvaatimukset muissa kuin 7-9 kohdissa erityisesti säädetyissä asioissa
  - 5 §:n yleisvaatimus
  - Tarvittaessa perustelujen täydentämistä ja viitteiden tarkistus
- 6) kansallisen solmupisteen rajapinta
  - Käydään läpi DVV:n kanssa
- 7) Muita?

Kommentit työpajassa 20.1.2021/muut asiat

- Mihinkään aiheeseen ei esitetty yhtään kommenttia
- Traficomin päätelmät:
  - Traficom valmistelee määräystä ja perustelumuistiota edellisellä kalvolla esitetyllä tavalla

Seuraavat työpajat

- KE 10.2.2021 9-11.30
- 3/7 tunnistusjärjestelmän tekniset vaatimukset ja arviointi
  - 4 §, 5 §, 11 §
  - 15 §, 16 §, 17 §, 18 §, 19 §
- Muistio ja kutsu tulevat ~1.2.2021, viimeistään 3.2.

- Jatkotyöpaja 3.2.2021 9-11 aikaisemmista
  - Mahdollisesti ensitunnistamisen attribuutit
  - Salausteemasta:
  - Käytännön toteutusten ja toteutettavuuden tarkempi arvioiminen: certificate pinning, certificate chain?, uusiminen
  - Traficomin arvio, että tarkoituksenmukaisinta käsitellä luottamusverkoston toimijoiden kesken

Kommentit 20.1.2021 seuraavista työpajoista

- Ei kommentteja
- Traficomin päätelmä
  - Jatkotyöpajan aiheet ja osallistujapiiri jää viraston arvioitavaksi
  - Salausasioiden toteutusarviotyöpaja pidettiin 3.2. vain luottamusverkostolle

Kiitos osallistumisesta, olkaa yhteydessä

eidas@traficom.fi

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus