Perustelut määräykselle sähköisistä tunnistus- ja luottamuspalveluista (M72B/2022)

x

Commented [LA1]: **Info:** lisätään lukujako sisällysluetteloon, kun sisältö muutoin valmis.

1 Määräyksen tausta ja säädösperusta

1.1 Määräyshistoria ja päivittämisen syyt

Määräyksellä kumotaan määräys Viestintävirasto 72A/2018 ja annetaan uusi muutettu määräys.

Tekninen kehitys, tietoturvauhkien muuttuminen, ETSI:n standardien edistyminen, markkinoiden kehitys, yritysten soveltamiskokemukset ja Liikenne- ja viestintäviraston kokemus valvonnasta edellyttävät vaatimusten ajantasaisuuden säännöllistä arviointia ja muutoksia.

Nykymuotoinen tunnistus- ja luottamuspalvelumääräys on annettu alun perin 2.11.2016 EU:n eIDAS-asetuksen (EU) 910/2014 voimaantulon yhteydessä sekä kansallisesti säädetyn vahvan sähköisen tunnistamisen luottamusverkoston kilpailu- ja teknisen yhteentoimivuuden edellytysten edistämiseksi. Vuonna 2016 annetun määräyksen siirtymäaikaa jatkettiin muutoksella 14.5.2018. Muutettu määräys on siten nykymuotoisen määräyksen kolmas versio.

Määräys 72/2016 M korvasi aikaisemmat Viestintäviraston määräykset 7 B/2009 M tunnistuspalvelun tarjoajien ja yleisölle laatuvarmenteita tarjoavien varmentajien ilmoitusvelvollisuudesta Viestintävirastolle ja 8 C/2010 M tunnistuspalvelun tarjoajien ja laatuvarmenteita tarjoavien varmentajien toiminnan luotettavuus- ja tietoturvallisuusvaatimuksista. Määräyksessä 7 säädettiin toimijoiden aloitus-, muutos- ja häiriöilmoituksista. Määräyksessä 8 säädettiin tietoturvallisuusvaatimuksista. Laatuvarmenteiden osalta määräykset annettiin ensimmäisen kerran vuonna 2003 ja vuonna 2009 niihin lisättiin vahvan sähköisen tunnistamisen palveluita koskevat vaatimukset.

1.2 Määräystoimivallan säädösperusta

Määräysvaltuutus laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009, tunnistus- ja luottamuspalvelulaki) 42 §

1.3 Asiaan liittyviä muita määräyksiä ja säädöksiä

Valtioneuvoston asetus vahvan sähköisen tunnistuspalveluntarjoajien luottamusverkostosta 169/2016 (muutettu 1212/2018)

Asetuksessa säädetään eräistä hallinnollisista käytännöistä ja rajapinnoista. Asetus liittyy erityisesti määräyksen 3 lukuun, joka koskee tunnistuspalveluiden yhteentoimivuutta.

*EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta (nk. **eIDAS**-asetus)*

Sähköisten luottamuspalveluiden, vaatimustenmukaisuuden akkreditoitujen arviointilaitosten ja sähköisen allekirjoituksen tai leiman luontivälineen nimettyjen sertifiointilaitosten sääntely annetaan valtaosin eIDAS-asetuksessa. Määräyksessä tehdään sääntelyyn vähäiset ja välttämättömät täydennykset.

eIDAS-asetuksen vaatimuksia tarkennetaan komission täytäntöönpanosäädöksillä.

*EU:n komission täytäntöönpanoasetus (EU) 2015/1502 (nk. **EU:n sähköisen tunnistamisen varmuustasoasetus**) teknisten vähimmäiseritelmien ja -menettelyjen vahvistamisesta sähköisen tunnistamisen menetelmien varmuustasoja varten sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 8 artiklan 3 kohdan mukaisesti*

EU:n varmuustasoasetuksessa säädetään tunnistusmenetelmien varmuustasojen vaatimukset. Asetusta sovelletaan niihin tunnistusvälineisiin, jotka notifioidaan EU:n komissiolle. Tunnistus- ja luottamuspalvelulaissa viitataan tunnistuspalvelun vaatimuksia koskevissa säännöksissä asetukseen, joten asetusta sovelletaan lain rinnalla myös tunnistusvälineisiin, joita ei notifioida.

Perustelumuistiossa viitataan varmuustasoasetuksen soveltamisohjeeseen, joka on laadittu jäsenvaltioiden asiantuntijoiden yhteistyönä yhteistyöverkostossa.

*EU:n komission täytäntöönpanoasetus (EU) 2015/1501 (nk. **EU:n yhteentoimivuusasetus**) yhteentoimivuusjärjestelmän vahvistamisesta sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 12 artiklan 8 kohdan mukaisesti.*

EU:n yhteentoimivuusasetus koskee ensisijaisesti Väestörekisterikeskuksen ylläpitämää kansallista solmupistettä. Asetuksen määrittelyt vähimmäis- ja valinnaisattribuuteista on otettu määräyksellä käyttöön myös kansallisessa tunnistuksessa. Asetus koskee myös kansallista solmupistettä.

*EU:n komission täytäntöönpanopäätös (EU) 2015/1984 (nk. **EU:n notifiointimenettelypäätös**) olosuhteiden, muotoseikkojen ja menettelyjen määrittelemisestä sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 9 artiklan 5 kohdan mukaisesti*

EU:n notifiointimenettelypäätöksessä määritellään notifioinnissa ilmoitettavat tiedot ja menettely. Tunnistusmenetelmän (tunnistusvälineen) notifioinnin komissiolle ja muille jäsenvaltioille tekee Viestintävirasto käytännössä yhdessä tunnistusvälineen tarjoajan kanssa.

*EU:n komission täytäntöönpanopäätös (EU) 2015/296 (nk. **EU:n yhteistyöverkostopäätös**) menettelyä koskevien järjestelyjen vahvistamisesta sähköiseen tunnistamiseen liittyvää jäsenvaltioiden välistä yhteistyötä varten sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 12 artiklan 7 kohdan mukaisesti*

EU:n yhteistyöverkostopäätöksessä säädetään jäsenvaltioiden yhteistyöstä tunnistusmenetelmien notifiointiin liittyvässä vertaisarvioinnissa. Liikenne- ja viestintävirasto on yhteistyöverkoston jäsen.

*Komission täytäntöönpanopäätös (EU) 2016/650, annettu 25 päivänä huhtikuuta 2016, **hyväksyttyjen allekirjoituksen ja leiman luontivälineiden tietoturvaarviointia** koskevien standardien vahvistamisesta sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 30 artiklan 3 kohdan ja 39 artiklan 2 kohdan mukaisesti (ETA:n kannalta merkityksellinen teksti)*

Komission täytäntöönpanopäätöksessä säädetään sähköisen allekirjoituksen ja leiman luontivälineen sertifioinnin vaatimuksista. Säädös liittyy määräykseen säännökseen 23.

*EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (**yleinen tietosuoja-asetus**)*

Henkilötiedon määritelmä 4 artikla

> *1) 'henkilötiedoilla' kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä 'rekisteröity', liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella,*

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.*
>
> *[…]*

Tietosuojalain (1050/2018) 29 §:n 4 §:ssä käsitellään henkilötunnuksen esittämistä

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

2 Määräyksen tavoite

2.1 Tavoitteet

Määräyksellä tehtävät tarkennukset lainsäädännön vaatimuksiin tekevät sääntelystä ennakoitavaa toimijoille ja edistävät toimijoiden tasapuolista kilpailua. Määräyksellä varmistetaan palveluiden tietoturva ja yhteentoimivuus.

Määräyksen valmistelu yhdessä toimialan kanssa tukee toteutuskelpoisten vaatimusten määrittelyä.

Tunnistus- ja luottamuspalveluiden asiakkaiden kannalta sääntelyllä huolehditaan tietoturvasta ja yksityisyyden suojaamisesta oletusarvoisesti (by design). Luottamuksen rakentaminen alaa kohtaan edellyttää, että toimijat rakentavat palvelunsa alusta pitäen asianmukaisesti.

2.2 Pääasialliset muutokset ja arvio määräyksen vaikutuksista

Määräykseen on tehty sanamuotojen selvennyksiä. Määräyksen ulkoasu on muutettu Liikenne- ja viestintäviraston yhtenäisen määrittelyn mukaiseksi, mistä syystä on muun ohessa korvattu pykälät ja momentit kohdilla ja alakohdilla. Niistä käytetään tässä perustelumuistiossa selvyyden vuoksi termiä säännös erotuksena perustelumuistion kohtiin.

Perustelumuistio on laadittu Liikenne- ja viestintäviraston uuden käytännön mukaisesti. Muistiosta on karsittu selittäviä aihepiiriä sivuavia osia.

Seuraavissa kohdissa kuvataan pääasialliset muutokset ja muutosten tarkoitus. Vaikutuksia käsitellään tarkemmin säännöskohtaisissa perusteluissa.

Säännös 4 Tietoturvallisuuden hallintajärjestelmä

Säännöksen 4.1 sanamuotoa muutetaan siten, että valittua tai valittuja **tietoturvallisuuden hallinnan standardeja on noudatettava, ei ainoastaan käytettävä.** Tämä tiukentaa vaatimusta hienoisesti. Tarkoitus on korostaa tunnistuspalvelun tarjoajan johdon sitoutumisen merkitystä ja tietoturvallisuuden hallintajärjestelmän ja prosessien ylläpidon merkitystä.

Sertifiointi on hyvä tapa osoittaa tietoturvallisuuden hallinnan vaatimustenmukaisuus, mutta sertifiointia ei edelleenkään edellytetä edes korkealla varmuustasolla.

Säännöksen 4 muutos ei edellytä siirtymäaikaa.

Säännös 5 Tunnistusjärjestelmän tietoturvavaatimukset

Säännös 5.1 tunnistusjärjestelmän suojautumiskyky on uusi.

Määräykseen lisätään tarkennus tunnistusjärjestelmän suojautumiskyvyn vaatimustasosta. Säännöksellä 5.1 tarkennetaan tunnistusjärjestelmän turvatoimenpiteiden ja teknisten määrittelyjen kokonaisuuden vaatimustaso. Tulkinnallisesti vaatimus olisi johdettavissa myös laista, mutta asiaa halutaan selkeyttää määräyksessä.

Sähköisen tunnistamisen varmuustasoasetuksen kohdan 2.4.6 mukaan edellytettyjen turvatoimenpiteiden eli teknisten kontrollien vaatimustaso määritellään varmuustasoasetuksen 2.3.1 kohdan hyökkäyspotentiaalilta suojautumiskyvyn perusteella. Riskiarvioon ei määrätä tarkempaa kriteeristöä tai noudatettavaa standardia. Arvion on perustuttava hyvään toimialaosaamiseen ja uhkien, haavoittuvuuksien ja teknisen kehityksen seurantaan.

Säännöksiin 5.2-5.4 tietoliikenne-, tietojärjestelmä- ja käyttöturvallisuudesta tehdään vakiintunutta soveltamista vastaavia tarkennuksia. Tiedon säilyttämisen turvallisuusvaatimus 7 §:stä on siirretty säännökseen 5.4.

Säännöksen 5 muutokset eivät edellytä siirtymäaikaa.

Säännökseen 5 liittyvän suosituksen muutos: Suositus tunnistusjärjestelmän kellonajan luotettavuudesta

Määräyksen perustelumuistiossa 2016 C-osa kohdassa 1 ollut *Suositus tunnistusjärjestelmän kellonajan luotettavuudesta* siirretään muutettuna säännöksen 5.3 e) perusteluihin. Järjestelmän luotettava aika on tärkeä osatekijä lokituksessa ja niiden aikaleimoissa ja muutoinkin keskeinen perusvaatimus. Aikalähteisiin ja synkronointiin ei oteta kantaa.

Säännös 6 Tunnistusmenetelmän tietoturvavaatimukset

Säännös 6.1 tunnistusmenetelmän ominaispiirteet ja suojautumiskyky on uusi.

Tarkoitus on yhdenmukaistaa ja parantaa tunnistusmenetelmien turvallisuuden vähimmäistasoa ja niihin tehtävien muutosten arviointia. Tunnistusmenetelmät kehittyvät jatkuvasti ja myös tietoturvauhkat muuttuvat.

Määräykseen lisätään vaatimus tehdä tunnistusmenetelmästä erityinen riskiarvio, jossa arvioidaan erikseen eri todentamistekijöihin ja todentamismekanismiin liittyvät uhkat ja niiltä suojaavat turvatoimenpiteet. Turvatoimenpiteistä säännöksessä huomioidaan nimenomaisesti salausratkaisut sekä todentamistekijöiden eriyttäminen, kun niitä käytetään samalla päätelaitteella (esimerkiksi mobiilitunnistussovellus ja sormenjälki tai PIN-koodi).

Erityisen riskiarviovaatimuksen tarkoitus on korostaa tunnistusmenetelmän turvallisuuden suunnittelun tärkeyttä. Arviot antavat myös Liikenne- ja viestintävirastolle perustellut tiedot, joiden nojalla virasto voi tarvittaessa kohdistaa tunnistuspalveluihin korjausvelvoitteita ennakollisesti.

Määräykseen lisätään tarkennus tunnistusmenetelmän suojautumiskyvyn vaatimustasosta. Tulkinnallisesti vaatimus olisi johdettavissa myös laista, mutta asiaa halutaan selkeyttää määräyksessä. (Vrt. säännöksen 5 vastaava muutos)

Virasto arvioi, että tällainen malli on tarpeeksi joustava eri tunnistusmenetelmien ja todentamistekijöiden suhteen ja huomioi tunnistusmenetelmän turvakontrollit kokonaisuutena.

Virasto arvioi sidosryhmäpalautteen perusteella, että tunnistusmenetelmän riskiarviovaatimukselle ei tarvita siirtymäaikaa.

Vaihtoehtoina säännökselle 6.1 virasto on arvioinut sääntelymalleja, joissa määräyksessä tarkennettaisiin todentamistekijäkohtaiset vaatimukset tai tarkennettaisiin tunnistusmenetelmän suojautumiskyvyn vaatimukset. Todentamistekijäkohtaiseen sääntelytapaan liittyisi todentamistekijöiden moninaisuuden ja kehittymisen takia paljon yksityiskohtia, joita ei ole viraston arvion mukaan mahdollista eikä tarkoituksenmukaista pyrkiä kattamaan säännöstasolla. Myöskään uhkat tunnistusmenetelmän turvallisuudelle ja turvakeinot uhkilta suojaamiselle eivät ole puhtaasti todentamistekijätyyppikohtaisia. Suojautumiskyvyn mittareita tai muunlaisia tarkennuksia määräyksessä voisi ajatella standardien perusteella, mutta tiedossa ei kuitenkaan ole sellaista yleispätevää standardia, jonka perusteella voisi yleispätevästi määrätä pakottavat vaatimukset. Suojautumiskyvyn vaatimusta tarkennetaan kuitenkin määräyksessä listaamalla osatekijöitä, joita riski- ja uhka-arvioinnissa on huomioitava.

Säännös 6.2 erityiset turvatoimenpiteet on uusi.

Tarkoitus on ottaa yhdenmukaisesti käyttöön joitakin hyviä turvakäytäntöjä niissä tunnistusmenetelmissä, joissa ne ovat teknisesti toteutettavissa.

Määräykseen lisätään vaatimus (6.2.1), että käyttäjälle on näytettävä tunnistuspyynnön yksilöintitieto (***nk. session binding***), jonka perusteella käyttäjä voi yhdistää asiointitapahtuman ja tunnistuspyynnön ja välttää vahvistamatta oikeudettomat tunnistuspyynnöt.

Määräykseen lisätään vaatimus (6.2.2), että käyttäjälle on näytettävä **luottavan osapuolen eli asiointipalvelun nimi**. Näytettävän tiedon varmentaa tunnistusvälityspalvelu, mutta jää eri toimintamalleissa sovittavaksi, kenen vastuulla on näyttää se käyttäjälle.

Määräykseen lisätään säännös (6.2.3) **kertakirjautumisen turvallisuusvaatimuksista**: velvollisuus huolehtia kertakirjautumiseen liittyvien istuntojen keston, siirtämisen ja lopettamisen hallinnasta. Määräyksen tarkoitus on tältä osin määrätä yleisellä tasolla aikaisemmassa sidosryhmäyhteistyössä todetut periaatteet. Myös kertakirjautumisessa on näytettävä käyttäjälle luottavien osapuolten eli asiointipalveluiden nimet.

Virasto arvioi, että vaatimus 6.2.2 edellyttää siirtymäaikaa.

Säännös 7 Tunnistusjärjestelmän ja rajapintojen salausvaatimukset

Säännös 7.1 Tietoliikenteen salausmenetelmät

Määräyksen luetteloa tietoliikenteen salauksessa kelpaavista salausmenetelmistä ja algoritmeista (7.1.1) täydennetään teknisen kehityksen takia. Kohtaa tarkennetaan siten, että se soveltuu myös 9 kohdassa määrättävään sanomien salaamiseen. Kohdasta jätetään pois salausmoodi XTS, joka ei sovellu teknisesti tietoliikenteen tai sanomien salaamiseen, vaan säilytettävän tiedon levysalaukseen. Virasto katsoo edelleen valvontakokemuksen perusteella, että vähimmäisvaatimukset on tarpeellista määrätä yksiselitteisesti.

Määräykseen lisätään mahdollisuus (7.1.2) käyttää lueteltujen algoritmien ja menettelyjen lisäksi Liikenne- ja viestintäviraston NCSA:n salaustuotteiden hyväksyntäviranomaisen (CAA) tai SOGIS MRA:n listoilla olevia algoritmeja ja arvoja. Tarkoitus on joustavoittaa vaatimuksia siltä varalta, että määräystä ei ehditä muuttaa teknisen kehityksen myötä. Virasto katsoo, että määräystä ei voi korvata pelkällä viittauksella näihin lähteisiin, sillä niitä ylläpidetään eri tarkoitukseen ja ne voivat joltain osin olla tarpeettoman tiukkoja korotetun varmuustason tunnistamisen vaatimuksiin nähden.

Säännös 7.2 Tietoliikenteen salausprotokolla

Määräyksestä poistetaan mahdollisuus käyttää poikkeuksellisesti versiota TLS 1.1. Vaadittu vähimmäistaso on siten poikkeuksetta TLS 1.2.

Vuoden 2016 määräyksellä tehdyn TLS 1.0 version käytön kieltämisestä saadun kokemuksen perusteella on tasapuolisen kilpailun kannalta hyvä, että kaikilla tunnistuspalveluilla on velvollisuus tehdä muutos samaan aikaan. Viraston arvio sidosryhmäpalautteen perusteella on, että siirtymäaikaa vaatimukselle ei tarvita. TLS 1.2 -versioon on laajalti siirrytty jo edelliseen siirtymän yhteydessä ja päätelaitekanta tukee sitä.

Säännöksen 7 muutokset eivät edellytä siirtymäaikaa.

Suositus säännöksen 7.1 soveltamisesta korkealla varmuustasolla

Vuoden 2016 määräyksen perustelumuistion suositus salausmenetelmistä ja algoritmeista korkealla varmuustasolla säilytetään suosituksena ja päivitetään.

Suositus vastaa salaustuotteiden hyväksyntäviranomaisen (CAA) arviointiohjeen määrittelyä turvaluokalle TL IV. Virasto arvioi, että korkean varmuustason suosituksen arvojen muuttaminen pakolliseksi ei aiheuttaisi yhteentoimivuusongelmia, koska tunnistusvälityksessä on teknisesti mahdollista valita algoritmit tapahtumakohtaisesti. Virasto katsoo kuitenkin, että vaikutus korkean varmuustason tunnistusta käyttäviin luottaviin osapuoliin on vaikeampi arvioida.

Säännös 8 Tietoliikenteen osapuolten varmentaminen

Voimassa olevan määräyksen 8.2 §:n vaatimusta tietoliikenteen osapuolen varmentamisesta tarkennetaan erottamalla luottamussuhteen perustaminen ja ylläpito. Määräyksen säännöksessä 8 tarkennetaan vaatimukset tunnistuspalveluiden välisillä ja tunnistuspalveluiden ja luottavien osapuolten eli asiointipalveluiden välisillä tietoliikenneyhteyksillä.

Säännöksellä 8.1 määrätään tietoliikenneyhteyden osapuolen tunnistamisen vaatimukset luottamussuhteen perustamisessa.

Säännöksellä 8.2 tarkennetaan vaihtoehtoiset menettelyt varmenteiden ja avainten päivittämiselle luottamussuhteen ylläpidossa.

Tarkoitus on selkeyttää vaatimukset ja varmistaa turvallisten menettelyjen yhtenäinen käyttö tunnistuspalvelusta riippumatta. Vaatimukset ovat olleet käytännössä epäselviä ja aiheuttaneet paljon tulkintakysymyksiä sekä turvallisuudeltaan vaihtelevia menettelyjä etenkin luottavien osapuolten eli asiointipalveluiden varmentamisessa.

Vaatimusten tarkoitus on varmistaa, että tunnistustapahtumat välitetään vain luotettavasti varmennetuille organisaatioille. Luottavan osapuolen todentaminen on yksi olennainen keino suojata tunnistusvälineen käyttäjää petollisten tunnistuspyyntöjen vahvistamiselta. Tarkoitus on myös varmistaa tietoliikenteen ja sanomien eheys ja luottamuksellisuus.

Vaatimuksilla saavutetaan parempi turvallisuus kuin protokollien peruskäytännöissä, joissa luotetaan mihin tahansa internetissä yleisesti luotettuihin varmenteisiin. Vaatimusten toteuttaminen edellyttää prosessien määrittelyä avainten ja varmenteiden toimittamisessa ja erilaisia asetusten määrittelyjä palvelinohjelmistoissa sekä tunnistuspalveluissa että asiointipalveluissa. Siksi vaikutuksia ja teknistä toteutettavuutta on arvioitu ja punnittu erityisen tarkasti ja vaatimusten teknistä toteutettavuutta OpenID Connect- ja SAML -protokollien kannalta on arvioitu valmistelussa sidosryhmäyhteistyössä. Viraston arvio on, että muutokset ovat teknisesti toteutettavissa ja tarpeellisia vahvan sähköisen tunnistuksen turvallisuuden jatkuvassa kehittämisessä. Vaatimuksille on kuitenkin tarpeen varta siirtymäaikaa etenkin suhteessa asiointipalveluihin ja muutosten läpivieminen edellyttää yhteistyötä neuvonnassa ja viestinnässä.

Virasto arvioi, että säännöksen 8 muutokset edellyttävät siirtymäaikaa, sillä ne vaikuttavat olennaisesti luottaviin osapuoliin eli tunnistuspalveluita käyttäviin asiointipalveluihin.

Säännös 9 Tunnistussanomien eheys ja luottamuksellisuus

Tunnistussanomien kategorinen sanomatason salausvaatimus muutetaan siten, että tunnistussanomien luottamuksellisuuden ja eheyden turvaamiselle määritellään **sanomien salaamisen rinnalle vaihtoehtoinen menettely** tietoliikenneyhteyden luottamuksellisuuden ja eheyden erityisellä varmistamisella. Vaihtoehtoinen menettely on mahdollinen, jos sanomia ei välitetä käyttäjän selaimen tai päätelaitteen kautta.

Muutoksen tarkoitus on huomioida voimassa olevaa määräystä paremmin eri protokollien ja standardien ominaisuudet ja sääntelyn tarkoitus. Muutos mahdollistaa esim. nykyisen ETSI MSS-standardia käyttävän mobiilivarmenneratkaisun ja lisää joustavuutta OpenID Connect -protokollaa käytettäessä. SAML -protokollan käytettäessä käytetään yleensä käyttäjän selainta, joten niissä on toteutettava aina sanomien salaus.

Vaatimuksen tarkoitus on, että henkilötiedot eivät paljastu oikeudettomasti käyttäjän päätelaitteen selaimessa tai palvelimilla. Yhdessä säännöksen 8 vaatimusten kanssa tunnistussanomien salaus ja allekirjoitus suojaavat myös tunnistustapahtuman väärentämiseltä ja toisintamiselta. Edelleen menettelyllä turvataan osaltaan sitä, että vahvistus käyttäjän todentamisesta ja henkilötiedot toimitetaan todentamisessa vain oikealle luottavalle osapuolelle eli asiointipalvelulle. Suojausvaatimus koskee yhtäläisesti tunnistuspalveluiden välisiä ja tunnistuspalveluiden ja luottavien osapuolten välisiä yhteyksiä.

Salauksen ja allekirjoituksen teknisessä toteuttamisessa viitataan säännöksen 7, jota on muutettu siten, että se soveltuu teknisesti myös sanomatason salaukseen.

Säännöksen 9 muutokset eivät pääosin edellytä siirtymäaikaa. 9.1.2 teknisluonteinen tarkennus tunnistussanomien allekirjoittamisesta saattaa edellyttää lyhyttä siirtymäaikaa.

Säännös 11 Tunnistuspalveluntarjoajan häiriöilmoitukset Liikenne- ja viestintävirastolle.

Säännökseen lisätään vaatimukset ilmoitusmenettelystä (11.3). Säännös kuvaa vakiintuneesti noudatettua käytäntöä. Tarkoitus on selkeyttää ilmoitusvelvollisuutta kaikille tunnistuspalveluille.

Muutoin säännöksessä selkeytetään merkittävän uhkan tai häiriön ilmoituskynnystä ja ilmoitettavia tietoja. Muutokset vastaavat valvontakäytäntöä eivätkä muuta vaatimustasoa.

Virasto ei pidä tarkoituksenmukaisena tai tarpeellisena laatia määräykseen toimivuushäiriöille uusia ilmoituskynnyksiä. Arviota ei muuteta vuonna 2016 tehdystä arviosta. On myös huomattava, että tunnistuslaissa ei ole nimenomaisia vaatimuksia tunnistuspalveluiden toimintavarmuudesta, varmistamisesta tai varautumisesta eikä siten toimivaltuutta määrätä niistä.

Viraston kyselyyn määräyksen muutostarpeista annetuissa vastauksissa esitettiin huoli, että kaikki eivät ilmoita häiriöistä virastolle riittävän alhaisella kynnyksellä ja että kaikki tunnistuspalvelut eivät informoi toisiaan häiriötilanteista. Virasto arvioi, että näihin havaintoihin on vaikutettava ensisijaisesti valvonnalla ja tehostamalla edelleen luottamusverkoston keskinäistä informointia. Toimijoiden keskinäinen tiedotusvelvollisuus ei kuulu määräystoimivallan piiriin vaan on valvonta-asia.

Säännöksen 11 muutokset eivät edellytä siirtymäaikaa.

Säännös 12

Säännös 12.1 Luottamusverkostossa välitettävät pakolliset tiedot (attribuutit).

Säännökseen 12.1. 4) lisätään pakollisiin tietoihin tunnistusvälityspalvelun varmistama tieto luottavasta osapuolesta eli asiointipalvelun nimi. Tarkoitus on mahdollistaa säännöksessä 6.2. määrättävä turvallisuutta lisäävä käytäntö näyttää käyttäjälle sen asiointipalvelun nimi, johon hän on tunnistautumassa.

Säännös 12.3 Tunnistuksen pseudonymisointi on uusi.

Sen tarkoitus on selventää attribuuttivaatimuksia tunnistusvälineen tarjoajan ja tunnistusvälityksen tarjoajan välisessä rajapinnassa luottamusverkoston sisällä siinä tapauksessa, että asiointipalvelulle toimitetaan vain ns. köyhdytetty vahvistus käyttäjän todentamisesta.

Tunnistus- ja luottamuspalvelulain 8 §:n 2 momentin mukaan *Mitä 1 momentissa säädetään, ei estä palvelun tarjoamista palvelukohtaisesti siten, että tunnistuspalvelun tarjoaja ilmoittaa tunnistuspalvelua käytävälle palveluntarjoajalle tunnistusvälineen haltijan salanimen tai ainoastaan rajoitetun määrän henkilötietoja.*

Laissa tai tässä määräyksessä ei säädetä siitä, mitä henkilötietoja luottavalle osapuolelle toimitetaan tai todennetaan vahvalla sähköisellä tunnistamisella. Määräyksessä määrätään attribuuteista, joita todentamisessa käsitellään luottamusverkoston sisällä. Luottavalle osapuolelle toimitetaan tyypillisesti esimerkiksi nimi ja henkilötun-

nus, mutta laissa todetulla tavalla luottavalle osapuolelle voidaan toimittaa myös salanimi tai rajoitettu määrä henkilötietoja. Tällöinkin käyttäjä on todennettava vahvasti ja tunnistustapahtuman tiedot on tallennettava lain 24 §:n mukaisesti.

Määräyksessä käytetään salanimen sijaan termiä pseudonyymi, koska henkilötietojen sääntelyn kannalta kysymys on viraston arvion mukaan pseudonyymistä henkilötiedosta. Vaikka tieto olisi luottavan osapuolen näkökulmasta sikäli anonyymiä, että luottava osapuoli ei välttämättä voi yhdistää sitä tiettyyn henkilöön, tieto on yhdistettävissä henkilöön tunnistuspalveluiden tallentamien tietojen perusteella.

Säännöksen 12 muutokset eivät edellytä siirtymäaikaa.

12.1 mukaisen luottavan osapuolen nimen käsittelyä välitettävän tietona on valmisteltu sidosryhmien kanssa jo aikaisemmin ja tieto on määritelty rajapintasuosituksiin.

12.3. mukaista pseudonymisointia ei viraston käsityksen mukaan ole tarjolla ja tällaisen palvelun mahdollisen kehittämisen tulee viraston arvion mukaan perustua määräyksen lähtökohtiin.

Säännös 14 Tiedonsiirrossa käytettävä protokolla ja muut vaatimukset

Säännöstä 14.1 tiedonsiirrossa käytettävä protokolla on tarkennettu nimeämällä Open ID Connect ja SAML standardeiksi, joista jommankumman mukaista rajapintaa tunnistuspalvelun on vähintään tarjottava 17 §:n mukaisen ensitunnistamisen ketjuttamiseen tunnistusvälineen tarjoajien välillä ja tunnistuslain 12 a §:n mukaiseen tunnistusvälitykseentunnistusvälineen tarjoajan ja tunnistusvälityspalvelun välillä.

Säännöksen tarkoitus on rajoittaa niiden standardien lukumäärää, joiden mukaiset rajapinnat tunnistuspalvelun on oltava valmis ylläpitämään voidakseen osaltaan välittää tai vastaanottaa tunnistetiedot ensitunnistamisessa tai tunnistusvälityksessä.

Mahdollistaminen tarkoittaa säännöksessä sitä, että vaatimusta tarkastellaan ensitunnistamisen tai luottavalle osapuolelle välitettävän tunnistustapahtuman vastaanottajan oikeuden näkökulmasta. Tunnistuspalvelu voi täyttää velvoitteensa tarjoamalla toiminnon toisen luottamusverkoston tunnistuspalvelun kautta, kunhan säädetyt ja määrätyt vaatimukset tällöinkin täyttyvät.

Säännöksen 14 muutokset eivät edellytä siirtymäaikaa.

Säännös 15 Vaatimuksenmukaisuuden arviointikriteerit

Säännökseen 15.1 on lisätty arvioitavaksi toiminnoksi yhteentoimivuus luottamusverkostossa. Yhteentoimivuus kuuluu tunnistus- ja luottamuspalvelulain 29 §:n mukaan vaatimuksenmukaisuuden arvioinnin piiriin, vaatimuksia tarkennetaan määräyksessä ja ne on huomioitu Liikenne- ja viestintäviraston arviointiohjeessa.

Säännökseen on lisätty viittaus Liikenne ja viestintäviraston arviointiohjeeseen mahdollisena arviointikriteeristönä. Sanamuotoja on selkeytetty.

Säännöksen 15 muutokset eivät edellytä siirtymäaikaa.

Säännös 16 Selvitys tunnistuspalvelun tarjoajan ja julkaistujen tietojen luotettavuudesta

Säännös liittyy vahva sähköisen tunnistuspalvelun ilmoitusvelvollisuuteen toiminnan aloittamisesta ja muutoksista tunnistuslian 10 §:ssä. Säännöksen tarkoitus on myös

selkeyttää niitä tietoja, joita ei koske säännöksen 15 riippumaton ja pätevä säännöllinen vaatimusten mukaisuuden arviointi. Säännöstä on täydennetty ja muokattu valvonta- ja neuvontakäytännön mukaisesti.

Säännöksen 16 muutokset eivät edellytä siirtymäaikaa.

Säännös 21 Hyväksytyn luottamuspalvelun arviointikriteerit

Säännöksellä määrätään hyväksyttyjen luottamuspalvelujen vaatimuksenmukaisuuden arviointikriteereistä viittaamalla valmiisiin ETSI:n standardeihin. Säännökseen lisätään edellisen määräyksen jälkeen valmistuneet viittaukset hyväksytyn sähköisen allekirjoituksen tai leiman hyväksytyn validointipalvelun standardiin ja hyväksytyn sähköisessä rekisteröidyn jakelupalvelun standardeihin.

Tarkoitus on tarkentaa arviointikriteerit siltä osin, kun komissio ei ole käyttänyt täytäntöönpanosäädösvaltuuttaan. Jos komissio antaa täytäntöönpanosäädökset, määräyksen vaatimukset kumotaan.

Säännöksen 21 muutokset eivät edellytä siirtymäaikaa.

2.3 Muut toteuttamisvaihtoehdot

Säännösten valmistelussa harkittuja vaihtoehtoja kuvataan säännöskohtaisissa perusteluissa.

Määräysvalmistelussa ja vaikutusarvioinnissa on tarkasteltu, voiko ohjaustarpeet ratkaista tehokkaasti ja tasapuolisesti määräyksen sijaan ohjeilla ja suosituksilla tai yhteissääntelyllä. Arviot ovat säännöskohtaisissa perusteluissa.

3 Määräyksen valmistelu

3.1 Sidosryhmävalmistelu

Liikenne- ja viestintävirasto teki 4.8.2020 toimialalle laajan ennakkokyselyn määräyksen mahdollisista muutostarpeista (dnro TRAFICOM/245890/03.04.05.00/2020). Kyselyssä oli 74 kysymystä. Kyselyyn saatiin 8 vastausta. Vastaukset on huomioitu määräyksen valmistelun aikana julkaistuissa valmistelumuistioissa.

Määräyksen muutosvalmistelusta julkaistiin 7.12.2020 työsuunnitelma, josta ilmenevät tarkasteltavat kysymykset, aiheiden ryhmittely sidosryhmätyöpajoihin ja hankkeen koko aikataulu. Työsuunnitelmasta julkaistiin 26.3.2021 päivitetty versio, jossa kerrottiin valmistelun aikana tehdyistä linjauksista.

Sidosryhmille on järjestetty työsuunnitelman mukaisesti 7 työpajaa ja 2 ylimääräistä työpajaa ajalla 10.12.2020 - 16.6.2021. Lisäksi virasto on pyynnöstä tavannut muutamia toimijoita kahdenvälisesti. Jokaisesta määräysmuutosaiheesta on ennen työpajaa julkaistu valmistelumuistio, johon on koottu voimassa oleva säännös ja sen perustelut ja aikaisemmat vaikutusarviot, lähteet, ennakkokyselyssä saadut vastaukset ja säännösten muutosehdotukset sekä näkökohtia muutosten tietoturvallisuus-, toteutettavuus- ja taloudellisista vaikutuksista. Sidosryhmätyöpajoissa saatu palaute ja viraston päätelmät siitä on koottu ja julkaistu työpajojen esittelykalvoilla.

Määräysvalmistelusta on tiedotettu sähköpostijakeluilla tunnistuspalveluiden luottamusverkoston rajattua yhteistoimintaryhmää, kaikille avointa tunnistus- ja luottamuspalveluiden eIDAS-ryhmää ja kaikille avointa tunnistus- ja luottamuspalveluiden teknistä eIDAS-ryhmää. Jakeluissa on mukana laajasti tunnistus- ja luottamuspalve-

lun tarjoajia, ICT-toimijoita, viranomaisia ja jonkin verran sähköisten asiointipalveluiden tarjoajia, jotka käyttävät tunnistus- ja luottamuspalveluita. Kaikki valmisteluma-teriaalit on julkaistu viraston verkkosivulla.

Lausuntopyyntö on toimitettu x.x.2021 samoilla jakeluilla ja julkaistu valtionhallinnon lausuntopalvelussa.

Määräys koskee tietoyhteiskunnan palveluja ja se on notifioitu EU:n transparenssidirektiivin (EU) xxx/xxx mukaisesti x.x.2021.

3.2 Lausuntopalaute

Lyhyen lausuntoyhteenvedon (sidosryhmien lausunnot) voi sisällyttää muistioon, pidemmän erillisenä liitteenä.

Kuvataan, miten saadut lausunnot ja kommentit on huomioitu ja miksi. Tuodaan esiin muutosta tukevat sekä siitä poikkeavat kannat. Kommenttikooste mahdollisesti liitteenä.

Muista myös notifiointipalaute.

4 Yksityiskohtaiset perustelut

Määräyksen luku 1 Yleiset säännökset

4.1 Säännös 1 Soveltamisala

Määräystä sovelletaan, kuten aikaisempiakin määräyksiä, vahvan sähköisen *tunnistusvälineen* tarjoamiseen. Vahvoja sähköisiä tunnistusvälineitä ovat sellaiset, joista on tehty ilmoitus liikenne- ja viestintävirastolle ja jotka täyttävät säädetyt vaatimukset.

Määräystä sovelletaan myös *tunnistusvälityspalveluihin*, joista on tehty ilmoitus Liikenne- ja viestintävirastolle. Tunnistusvälityspalveluilla tarkoitetaan tunnistustapahtumien välittämistä luottaville osapuolille eli asiointipalveluille.

Sama oikeushenkilö voi toimia halutessaan sekä tunnistusvälineen tarjoajana että tunnistusvälityspalveluna.

Määräystä sovelletaan myös eIDAS-asetuksen mukaisiin hyväksyttyihin luottamuspalveluihin, joilla tarkoitetaan asetuksen vaatimukset täyttäviä luottamuspalveluja.

Määräystä ei sovelleta luottamuspalveluihin, joille ei ole haettu hyväksyntää. Liikenne- ja viestintäviraston tehtävänä on tunnistus- ja luottamuspalvelulain 42 a §:n ja eIDAS-asetuksen 17 artiklan mukaan valvoa tietyillä edellytyksillä ei-hyväksyttyjä luottamuspalveluita, jos virastolle ilmoitetaan, että ei-hyväksytyt luottamuspalvelun tarjoajat tai niiden tarjoamat luottamuspalvelut eivät väitetysti täytä asetuksessa säädettyjä vaatimuksia. Virasto arvioi, että valvontatilanteessa toimintaa voitaisiin verrata lähinnä eIDAS-asetuksen täytäntöönpanon tueksi laadittuihin standardeihin.

Täsmälliset viittaukset EU-säädäntöön ovat tarpeen selkeyttävänä informaationa määräyksessä mm. siksi, että EU-oikeuden ensisijaisuus ilmenee selvästi.

Säännökseen ei tehdä muutoksia määräyksessä 2022 lukuun ottamatta viraston nimen päivittämistä.

4.2 Säännös 2 Tarkoitus

Säännöksessä kuvataan lyhyesti määräykseen pääasialliset tavoitteet. Säännös on informatiivinen eikä esimerkiksi määrittele tarkemmin vaatimusten soveltamisalaa.

Säännökseen ei tehdä muutoksia määräyksessä 2022.

Tunnistuspalvelut

Tunnistus- ja luottamuspalvelulain mukaan myös kansallisesti edellytetään, että tunnistuspalvelujen tarjonnassa täytetään vähintään EU:n varmuustasoasetuksen liitteen mukaiset korotetun varmuustason vaatimukset. Tavoitteena on, että toimijoiden on helppo hakea halutessaan EU-notifiointia missä tahansa vaiheessa, kun ne täyttävät kansallisesti asetetut vaatimukset. Tunnistuspalvelun tarjoajien ei tarvitse laatia erillistä tunnistusratkaisua rajat ylittäviä tilanteita ja kansallista tunnistamista varten.

Sama tavoite on otettu määräysvalmistelun lähtökohdaksi. Määräyksen valmistelussa on pyritty hyödyntämään mahdollisimman laajasti kansainvälisiä standardeja, vaatimusmäärittelyjä ja ilmoittamistapoja. Ratkaisulla pyritään helpottamaan myös rajat ylittävää palveluntarjontaa ja välttämään kansallisesti räätälöityjä vaatimuksia.

Luottamuspalvelut

Yleisesti luottamuspalveluiden sääntelyn tavoitteena on tietoyhteiskuntakehitys ja luottamuksen lisääminen sähköiseen asiointiin. Luottamuspalveluiden sääntelyllä autetaan sähköisten palveluiden toteuttajia ja käyttäjiä tunnistamaan ne palvelut, joiden avulla on mahdollista toteuttaa sähköisten asiointipalveluiden eri toiminnot mahdollisimman tietoturvallisesti.

Määräyksen tavoitteena on selkeyttää hyväksyttyjen luottamuspalvelujen eIDAS-asetuksessa säädettyjä vaatimuksia viittaamalla EU:n valmistelutyössä viitoittamiin kansainvälisiin standardeihin siltä osin, kun niihin ei ole ainakaan toistaiseksi tehty viittauksia komission täytäntöönpanosäädöksillä, vaikka siihen olisi eIDAS-asetuksessa toimivalta.

Standardiviittaukset määräyksessä tukevat myös sitä, mitä ainakin tulee huomioida mahdollisten vaatimustenmukaisuuden arviointilaitosten pätevyysvaatimuksena, kun niitä akkreditoidaan.

Arviointitoiminta

Määräyksen tavoitteena on selkeyttää toimijoille ja vaatimustenmukaisuuden arviointilaitoksille luottamuspalveluiden vaatimuksia siltä osin, kun komissio ei ole käyttänyt luottamuspalveluihin liittyvää säädäntötoimivaltaansa ja antanut täytäntöönpanosäädöksiä, joissa viitattaisiin tarpeellisiin standardeihin.

Tunnistuspalveluiden arvioinnin osalta määräyksen tavoitteena on selkeyttää toimijoille, millä perusteella niiden käyttämät auditoijat ovat päteviä tekemään tunnistusjärjestelmän arviointeja. Tunnistuspalveluntarjoajan arviointielimen ei tarvitse hakea erikseen hyväksyntää, ellei se ole vaatimustenmukaisuuden arviointilaitos. Määräyksen tavoitteena on, että toimijat voisivat mahdollisimman paljon hyödyntää auditointeja, joita ne tekevät tai teettävät jo ennestään.

4.3 Säännös 3 Määritelmät

4.3.1 Säännös 3.1 määräyksen määritelmät

Rajapinnan määritelmä kattaa tiedonsiirtoon käytetyn protokollan mukaisten tekijöiden tarkemman määrittelyn ja valinnaiset tekijät. Se kattaa myös käytännön toteutuksen eli siirrettävien tietosisältöjen valikoiman ja muodon.

Varmenteen määritelmä lisätään määräykseen. Tunnistus- ja luottamuspalvelulain määritelmä on sidottu vahvan sähköisen tunnistamisen varmenteisiin tai luottamuspalveluina tarjottaviin varmenteisiin.

Määräyksessä termiä varmenne käytetään säännöksessä 8 sen yleisemmässä merkityksessä. Varmenteilla on yleisesti ottaen erilaisia myöntämismenettelyjä ja niiden luotettavuuden taso vaihtelee siksi paljon. Varmenteen haltijaa ei aina tunnisteta vaan tieto haltijasta voi olla haltijan itse ilmoittama. Todentamistiedoilla tarkoitetaan haltijan julkista avainta, joka on osa julkisen avaimen eli PKI-menetelmää. Julkiseen avaimeen liittyvän yksityisen avaimen kuuluisi olla vain varmenteen osoittaman haltijan hallinnassa.

Vertaa tunnistus- ja luottamuspalvelulain 2.1 § 8) *varmenteella sähköistä todistusta, joka todentaa henkilöllisyyden tai todentaa henkilöllisyyden ja liittää luottamuspalvelun todentamistiedot luottamuspalvelun käyttäjään ja jota voidaan käyttää vahvassa sähköisessä tunnistamisessa ja luottamuspalveluissa*

Kansallinen solmupiste. Määräyksestä poistetaan tarpeettomana *eIDAS-rajapinnan* määritelmä. Määritelmä on koskenut kansallisten solmupisteiden välisiä rajapintoja ja soveltamiskokemus on osoittanut, ettei kyseinen Digi- ja väestötietoviraston ja muiden jäsenvaltioiden julkishallinnon solmupisteiden välinen rajapinta vaikuta kansallisiin rajapintoihin siten, että määritelmälle olisi tarvetta. Sen sijaan käytetään termiä *kansallinen solmupiste*. Tunnistus- ja luottamuspalvelulain 30 §:ssä kansallisella solmupisteellä tarkoitetaan *tiettyä sähköisen tunnistamisen yhteentoimivuusjärjestelmään liittyvää kansallista rajapintaa.* Komission täytäntöönpanoasetuksessa (EU) 2015/1501 2 artiklassa tarkoitetaan *solmupisteellä yhteyspistettä, joka on osa sähköisen tunnistamisen yhteentoimivuusarkkitehtuuria ja joka osallistuu henkilöiden todentamiseen rajojen yli ja joka pystyy tunnistamaan sekä käsittelemään tai siirtämään tietoja muille solmupisteisiin tarjoamalla yhden jäsenvaltion kansalliselle sähköisen tunnistamisen infrastruktuurille rajapinnan muiden jäsenvaltioiden sähköisen tunnistamisen infrastruktuureihin.*

Termiä käytetään säännöksissä 10, 13 ja 17.

4.3.2 Säännös 3.2 Määräyksessä käytetyt tunnistuslain ja eIDAS-asetusten määritelmät

Viittausta säädöshierakkisesti ylemmän asteisiin säädöksiin täydennetään.

Määräyksen kannalta keskeisiä ovat seuraavat tunnistus- ja luottamuspalvelulain 2 §:ssä ja eIDAS-asetuksen 3 artiklassa säädetyt määritelmät

Tunnistus- ja luottamuspalvelulain 2 §

> *1) **vahvalla sähköisellä tunnistamisella** sellaista henkilön, oikeushenkilön tai oikeushenkilöä edustavan luonnollisen henkilön yksilöimistä ja tunnisteen aitouden ja oikeellisuuden todentamista sähköistä menetelmää käyttäen, joka täyttää sähköisestä tunnistamisesta ja luottamuspalveluista annetun EU:n asetuksen 8 artiklan 2 kohdan b alakohdassa tarkoitetun korotetun varmuustason tai mainitun kohdan c alakohdassa tarkoitetun korkean varmuustason vaatimukset;*

*2) **tunnistusvälineellä** sähköisestä tunnistamisesta ja luottamuspalveluista annetun EU:n asetuksen 3 artiklan 2 kohdassa tarkoitettua **sähköisen tunnistamisen menetelmää**;*

*3) **tunnistuspalvelun tarjoajalla** tunnistusvälityspalvelun tarjoajaa tai tunnistusvälineen tarjoajaa;*

*4) **tunnistusvälineen tarjoajalla** palveluntarjoajaa, joka tarjoaa tai laskee liikkeelle vahvan sähköisen tunnistamisen tunnistusvälineitä yleisölle sekä tarjoaa tunnistusvälinettään tunnistusvälityspalvelun tarjoajalle välitettäväksi luottamusverkostossa;*

*5) **tunnistusvälityspalvelun tarjoajalla** palveluntarjoajaa, joka välittää vahvan sähköisen tunnistamisen tunnistustapahtumia sähköiseen tunnistukseen luottavalle osapuolelle;*

*10) **luottamusverkostolla** Liikenne- ja viestintäviraston ilmoituksen tehneiden tunnistuspalvelun tarjoajien verkostoa;*

*11) **vaatimustenmukaisuuden arviointilaitoksella** Viestintäviraston hyväksymää tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista ja neuvoston asetuksen (ETY) N:o 339/93 kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 765/2008 2 artiklan 13 kohdassa tarkoitettua elintä, joka on akkreditoitu mainitun asetuksen mukaisesti*

eIDAS-asetuksen 3 artikla

*2) '**sähköisen tunnistamisen menetelmällä**' aineellista ja/tai aineetonta kokonaisuutta, joka sisältää henkilön tunnistetietoja ja jota käytetään verkkopalveluun liittyvään todentamiseen;*

*4) '**sähköisen tunnistamisen järjestelmällä**' sähköiseen tunnistamiseen liittyvää järjestelmää, jonka puitteissa sähköisen tunnistamisen menetelmiä myönnetään luonnollisille henkilöille, oikeushenkilöille tai oikeushenkilöä edustaville luonnollisille henkilöille;*

*6) '**luottavalla osapuolella**' luonnollista henkilöä tai oikeushenkilöä, joka luottaa sähköiseen tunnistamiseen tai luottamuspalveluun;*

*16) '**luottamuspalvelulla**' sähköistä palvelua, jota yleensä tarjotaan vastiketta vastaan ja joka koostuu seuraavista:*

a) sähköisten allekirjoitusten, sähköisten leimojen tai sähköisten aikaleimojen, sähköisten rekisteröityjen jakelupalvelujen ja kyseisiin palveluihin liittyvien varmenteiden luomisesta, tarkastamisesta ja validoinnista; tai

b) verkkosivustojen todentamisen varmenteiden luomisesta, tarkastamisesta ja validoinnista; tai

c) sähköisten allekirjoitusten, leimojen tai kyseisiin palveluihin liittyvien varmenteiden säilyttämisestä;

*17) '**hyväksytyllä luottamuspalvelulla**' luottamuspalvelua, joka täyttää tässä asetuksessa säädetyt sovellettavat vaatimukset;*

*20) '**hyväksytyllä luottamuspalvelun tarjoajalla**' luottamuspalvelun tarjoajaa, joka tarjoaa yhtä tai useampaa hyväksyttyä luottamuspalvelua ja jolle valvontaelin on myöntänyt hyväksytyn aseman;*

EU:n sähköisen tunnistamisen varmuustasoasetuksen Liite kohta 1.

*2) '**todentamistekijällä**' tarkoitetaan tekijää, joka on vahvistettu henkilöön kytkeytyväksi ja joka kuuluu johonkin seuraavista luokista:*

a) 'hallussapitoon perustavalla todentamistekijällä' tarkoitetaan todentamistekijää, jonka henkilön on osoitettava olevan hallussaan;

b) 'tiedossaoloon perustavalla todentamistekijällä' tarkoitetaan todentamistekijää, jonka henkilön on osoitettava olevan tiedossaan;

c) 'luontaisella todentamistekijällä' tarkoitetaan todentamistekijää, joka perustuu johonkin luonnollisen henkilön fyysiseen ominaisuuteen, jonka henkilön on osoitettava fyysiseksi ominaisuudekseen;

*3) '**dynaamisella todentamisella**' tarkoitetaan sähköistä prosessia, jossa käytetään salausta tai muita tekniikoita, joiden avulla voidaan pyynnöstä luoda sähköinen todiste siitä, että henkilöllä on hallinnassaan tai hallussaan tunnistetiedot, sekä muuttaa sitä jokaisessa uudessa henkilön ja hänen henkilöllisyytensä varmentavan järjestelmän välillä tapahtuvassa todentamisessa;*

*4) '**tietoturvallisuuden hallintajärjestelmällä**' tarkoitetaan prosesseja ja menettelyjä, joiden tarkoituksena on pitää tietoturvallisuuteen liittyvät riskit hyväksyttävällä tasolla.*

Määräyksen luku 2 Tunnistuspalvelun tietoturvavaatimukset

4.4 Säännös 4 Tunnistuspalvelun tarjoajan tietoturvallisuuden hallintajärjestelmä

4.4.1 Säännös 4.1 Tietoturvallisuuden hallinnan standardi

Säännöksessä määrätään yleisellä tasolla siitä, mitä tunnistusjärjestelmän tietoturvallisuuden hallinnassa täytyy ottaa huomioon. Tunnistuspalvelun tarjonnalla tarkoitetaan koko tunnistusjärjestelmää, joka kattaa koko tunnistuspalvelun kokonaisuuden.

Tunnistuslain 8.1 §:n 5 alakohdassa säädetään tietoturvallisuuden hallinnasta ja viitataan mm. EU:n sähköisen tunnistamisen varmuustasoasetuksen kohtaan 2.4.3. EU:n sähköisen tunnistamisen varmuustasoasetuksen liitteen 1 kohdassa 2.4.3 edellytetään, että *tietoturvallisuuden hallintajärjestelmässä noudatetaan vakiintuneita standardeja tietoturvaan liittyviä riskien hallintaa ja valvontaa varten.*

Säännöksessä 4.1 tarkennetaan tunnistus- ja luottamuspalvelulain ja EU:n sähköisen tunnistamisen varmuustasoasetuksen vaatimusta. Ainakin ISO/IEC 27001 -standardi [viite] on yleisesti tunnettu ja pätevä tietoturvallisuuden hallinnan standardi. Myös muuta standardia tai standardien yhdistelmää voi käyttää, edellyttäen, että standardi todella kohdistuu tietoturvallisuuden hallintaan. Standardi voi olla kansainvälinen, kuten ISO, mutta myös kansallinen kuten KATAKRI [VIITE].

Säännöksen sanamuotoa muutetaan siten, että valittua tai valittuja tietoturvallisuuden hallinnan standardeja on noudatettava, ei ainoastaan käytettävä. Tämä tiukentaa vaatimusta hienoisesti. Tarkoitus on korostaa tunnistuspalvelun tarjoajan johdon sitoutumisen merkitystä ja tietoturvallisuuden hallintajärjestelmän ja prosessien ylläpidon merkitystä.

Korkeallakaan tasolla ei määrätä pakolliseksi sertifiointia, mutta tietoturvallisuuden hallinnan toteutusta ja tehokkuutta arvioidaan korkealla varmuustasolla kautta linjan

tiukasti. Tietoturvallisuuden hallinnan on oltava poikkeuksetta kattavaa, johdonmukaista ja aktiivista.

4.4.2 Säännös 4.2 Tietoturvallisuuden hallinnan kattavuus

Säännöksessä 4.2 luetellaan toiminnan osa-alueet, jotka tietoturvallisuuden hallinnan täytyy kattaa. Vaatimusten tarkentamisessa on hyödynnetty ISO/IEC 27001 vaatimusten ylätason ryhmittelyä.

Säännöstä ei ole muutettu. Vaatimukset vastaavat pitkälti jo ennen vuotta 2016 voimassa olleen silloisen määräyksen 8 2 §:ää tietoturvallisuuden hallinnasta.

Tietoturvallisuuden hallinnan on oltava kattavaa, johdonmukaista, organisoitua, suunnitelmallista ja jatkuvasti seurattua. Säännöksessä tarkennetaan, mitä seikkoja tietoturvallisuuden hallintajärjestelmässä täytyy vähintään huomioida.

Myös alihankkijoiden tietoturvallisuuden hallinnan tulee täyttää vaatimukset. Ne voidaan suhteuttaa alihankitun toiminnon kriittisyyteen tunnistusjärjestelmässä.

Tietoturvallisuuden hallinnan vaatimustenmukaisuuden arvioinnista ks. määräyksen 15 kohta ja sen perustelut.

Seuraavassa kuvaillaan alakohtien sisältöä ja arvioidaan niiden liityntä ISO/IEC 27001 -standardin kohtiin. Taulukkoon on tehty täydennyksiä 2016 perusteluihin nähden.

Määräys 4.2 kohta ja soveltaminen	**ISO/IEC 27001**
1) *tunnistuspalveluntarjoajan toimintaympäristö kokonaisuutena* - Tietoturvallisuuden hallintajärjestelmä kattaa tunnistusjärjestelmään vaikuttavat olennaiset sisäiset ja ulkoiset tekniset, oikeudelliset ja hallinnolliset vaatimukset ja tarpeet. - Tunnistuspalvelussa tulee mm. noudattaa ajantasaisia lainsäädäntöä ja määräyksiä, kuten tunnistus- ja luottamuspalveluakia, määräystä 72 ja yleistä tietosuoja-asetusta.	4 organisaation toimintaympäristö
2) *tietoturvallisuuden hallinnan johtaminen, organisointi ja ylläpito* - Tietoturvallisuuden hallintajärjestelmä kattaa hallinnan johtamisen, organisoinnin ja ylläpidon, joka dokumentoidaan tietoturvapolitiikassa tai vastaavissa ohjausasiakirjoissa. - Käytössä on ajantasainen ja johdon hyväksymä tietoturvapolitiikka tai vastaavat ohjausasiakirjat.	5 johtajuus 9.2 sisäinen auditointi 9.3 johdon katselmus 10 hallintajärjestelmän parantaminen A.5.1.1 Tietoturvapolitiikat

Turvallisuusperiaatteet ja politiikat ovat organisaation ja suojattavien kohteiden kannalta kattavat ja tarkoituksenmukaiset. - Henkilökunnan ja alihankkijoiden tietoturvallisuuteen liittyvät vastuut on kuvattu.	A.6.1.1 Tietoturvaroolit ja -vastuut A.15.1.1 toimittajasuhteiden tietoturvapolitiikka
3) *tunnistuspalvelun tarjontaan liittyvien tietoturvallisuusriskien hallinta* - Tietoturvallisuuden hallintajärjestelmä kattaa tunnistuspalvelun tarjontaan liittyvien tietoturvallisuusriskien hallinnan. - Riskienhallinta on säännöllinen ja jatkuva, dokumentoitu prosessi. - Tunnistetut riskit luokitellaan ja priorisoidaan. - Riskienhallintaprosessi tunnistaa tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen kohdistuvat riskit. - Riskienhallintaprosessia ja sen tuloksia hyödynnetään tunnistuspalvelun/tunnistusjärjestelmän turvatoimien suunnittelussa. - Vrt. eIDAS varmuustasoasetuksen soveltamisohje: *Riskienhallinnassa yleisenä periaatteena on, että organisaation on itsensä valittava, minkä tasoista riskiä se pitää hyväksyttävänä. Kohdan 2.4 vaatimuksella muutetaan tätä yleistä periaatetta, sillä sen mukaan organisaation turvatoimenpiteiden on oltava suhteutettuja riskeihin nyllois-tasolla.* - Määräyksen säännöksessä on määrätään tarkemmat vaatimukset tunnistusmenetelmän riskien arvioimiselle	6 suunnittelu
4) *tietoturvallisuuden resursointi, pätevyys, henkilöstön tietoisuus tietoturvallisuudesta, viestintä ja dokumentointi sekä dokumentoidun tiedon hallinta* - Tietoturvallisuuden hallintajärjestelmä kattaa tietoturvallisuuden resursoinnin, pätevyysvaatimukset, henkilöstön tietoisuuden tietoturvallisuudesta, viestinnän ja dokumentoinnin sekä dokumentoidun tiedon hallinnan. - Ajantasaiset tietoturvaohjeet ja käytännöt ovat kaikkien sähköisen tunnistamisen tehtäviin osallistuvien saatavilla ja tiedossa.	7 tukitoiminnot

- Henkilöstön turvallisuuskoulutus on säännöllistä ja dokumentoitua. Koulutuksen tehokkuutta seurataan. - Tyypillisenä esimerkkinä tunnistusvälineen tarjoajan henkilöstön pätevyysvaatimusten hallinnasta voidaan mainita perehdytys passien ja henkilökorttien aitouden tarkistamiseen tunnistusvälineen hakijoiden ensitunnistamisessa tai tunnistusjärjestelmän etähallinnan tietoturvallisuuskäytäntöihin.	
5) *tunnistuspalvelun tarjonnan suunnittelu ja ohjaus tietoturvavaatimusten täyttämiseksi* - Tietoturvallisuuden hallintajärjestelmässä huolehditaan tunnistuspalvelun tarjonnan suunnittelusta ja ohjauksesta siten, että tunnistuspalvelulle säädetyt tietoturvavaatimukset täyttyvät. - Tunnistuspalvelun vaatimukset (TunnL, EU:n sähköisen tunnistamisen varmuustasoasetus ja viraston määräys 72) on huomioitu hallintajärjestelmässä	8 toiminta A.18.1.1 vaatimustenmukaisuus/lainsäädäntöön ja sopimuksiin sisältyvien vaatimusten noudattaminen: sovellettavien lakisääteisten ja sopimuksellisten vaatimusten tunnistaminen
6) *tietoturvallisuuden hallinnan tehokkuuden ja toimivuuden arviointi* - Tietoturvallisuuden hallintajärjestelmä kattaa tietoturvallisuuden hallinnan tehokkuuden ja toimivuuden säännöllisen arvioinnin. - Ts. miten hyvin tietoturvallisuuden hallinta tehoaa ja vaikuttaa niihin tekijöihin, prosesseihin ja ongelmiin, jotka vaikuttavat tunnistusjärjestelmän tietoturvallisuuteen.	9.1 seuranta, mittaus, analysointi, arviointi

4.4.3 Riskinhallintamalli ja -prosessi

Säännöksen 4.2 3) edellyttämän riskinhallinnan täytyy kattaa koko tunnistusjärjestelmän riskit. Velvollisuus kattaa myös järjestelmän puitteissa myönnettyjen tunnistusvälineiden eli tunnistusmenetelmän riskit. Säännöksessä 6.1 määrätään tunnistusmenetelmän uhka- ja riskiarvion erityiset vaatimukset ja asiat, jotka arviossa on välttämättä otettava huomioon.

Määräyksessä ei oteta kantaa riskinhallinnassa käytettävään malliin tai siinä noudatettavaan standardiin. Sekä koko tunnistusjärjestelmää koskevassa että erityisesti säännöksen 6 tunnistusmenetelmää koskevassa uhka- ja riskiarviossa voidaan käyttää samaa tunnistuspalvelun tarjoajan valitsemaa standardia tai toimintamallia.

Riskiarviossa voi hyödyntää relevantteja standardeja. Määräyksessä ei määrätä pakolliseksi tai vertailukohdaksi tiettyä standardia. Riskinhallinnassa voi hyödyntää esimerkiksi seuraavia standardeja tai ohjeita:

- SFS-ISO 31000:2018 [VIITE]

- ISO/TR 31004, Risk management – Guidance for the implementation of ISO 31000, and International Standard/ISO/TR 31004:fi [VIITE]
- ISO/IEC 31010, Risk management – Risk assessment techniques, developed jointly with the International Electrotechnical Commission/SFS-EN IEC 31010:2019 [VIITE]
- ISO 27005 [VIITE] https://en.wikipedia.org/wiki/ISO/IEC_27005
- VAHTI Ohje riskienhallintaan, Valtiovarainministeriön julkaisuja 22/2017 [VIITE] https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/VM_22_2017.pdf?sequence=1&isAllowed=y
- NIST Risk Management Framework (RMF) [VIITE] https://csrc.nist.gov/projects/risk-management/about-rmf
- Erityisesti tunnistusmenetelmien tai salauskäytäntöjen toteutuksen arvioinnissa voi käyttää myös standardeja, kuten FIPS 140-3 [VIITE] https://csrc.nist.gov/publications/detail/fips/140/3/final

Riskinhallintamallin tarkistuslistana voidaan pitää myös seuraavaa, lähteenä KATAKRI 2020 [VIITE] , T-03:

1) *Tietoturvallisuusriskien hallinta on osa organisaation toimintaa ja muuta riskienhallintaa.*
2) *Tietoturvallisuusriskien hallinnan avulla varmistetaan riittävien tietoturvallisuustoimenpiteiden toteuttaminen turvallisuusluokiteltujen tietojen suojaamiseksi.*
3) *Tietoturvallisuusriskien arvioinnissa ja analysoinnissa käytetään toiminnon näkökulmasta asianmukaista ja päätöstentekoon ymmärrettävää informaatiota tuottavaa menetelmää.*
4) *Tietoturvallisuusriskien hallintaan osallistuu riittävästi asiantuntijoita.*
5) *Tietoturvallisuusriskien hallinnassa on otettu huomioon sidosryhmistä ja toimitusketjuista aiheutuvat riskit. Vrt. turvallisuuskriittisten laitteistojen ja ohjelmistojen (vrt. I-01, I-12 ja I-13) toimitusketjuihin liittyvät riskit.*
6) *Tietoturvallisuusriskien arvioinnista ja analysoinnista saatuja tuloksia hyödynnetään turvallisuusluokiteltujen tietojen tietoturvallisuustoimenpiteiden suunnittelussa ja toteuttamisessa, turvallisuuspoikkeamien vaikutusten arvioinnissa sekä muutoksenhallinnassa ja soveltuvilta osin hankintamenettelyissä.*
7) *Tietoturvallisuustoimenpiteet on mitoitettu riskiperusteisesti ottaen huomioon muun muassa tiedon turvallisuusluokka, määrä, muoto, luokitteluperuste ja sijoitustilat suhteessa arvioituihin riskeihin.*
8) *Organisaatio on dokumentoinut keskeisiltä osin sovellettavat valvonta- ja turvatoimet ja niiden perusteena olevan riskienarvioinnin.*

Riskienhallinnan prosessin tulisi kattaa ISO31000 standardin kuvaamat prosessit, jossa huomioidaan (esim. SFS-ISO 31000:2018, sivu 14) [VIITE]

1) *Kattavuus, toimintaympäristö ja kriteerit*
2) *Riskien arviointi*
   - *Riskien tunnistaminen*
   - *Riskianalyysi*
   - *Riskien merkityksen arviointi*
3) *Riskien käsittely*

4) Viestintä ja tiedonvaihto
5) Tallenteet ja raportointi
6) Seuranta ja katselmointi

4.4.4 Säännös 4.1, harkitut sääntelyvaihtoehdot

2016 pohdittiin, mitä standardeja määräyksessä voidaan asettaa referenssiksi. Tuolloin päädyttiin siihen, että ISO 27001 on ainoa riittävän kattava standardi. Arvioinneissa on käytännössä tullut esille ainakin finanssialan standardeihin (kuten PCI DSS) tukeutuminen osana tietoturvallisuuden hallintaa.

Virasto arvioi, että edelleenkään ei ole esitetty relevantteja kokonaisvaltaisia vaihtoehtoja ISO 27001:lle. Se ei ole ainoa vaihtoehto, mutta vaikuttaa olevan ainoa toimialariippumattomasti laajalti käytetty nimenomaan tietoturvallisuuden hallintaan liittyvä standardi.

Määräysmuutostarvekyselyssä annetussa palautteessa ehdotettiin, että säännöksen sanamuotoa tiukennettaisiin tai tarkennettaisiin siten, että edellytetään standardin noudattamista tai sertifiointia. Liikenne- ja viestintävirasto arvioi, että ehdoton sertifiointivaatimus olisi taloudellisesti raskas ja soveltuisi huonosti siihen tilanteeseen, että tietoturvallisuuden hallinnasta huolehditaan usean standardin yhdistelmällä.

4.5 Säännös 5 Tunnistusjärjestelmän tietoturvavaatimukset

4.5.1 Yleistä

Säännöksessä 5 tarkennetaan koko tunnistusjärjestelmän tietoturvallisuuden toteuttamisessa tarvittavia toimenpiteitä.

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

Erikokoiset tunnistuspalvelut ja uudet tulokkaat. Tunnistusjärjestelmän ja tunnistusmenetelmän vaatimukset koskevat kaikenkokoisia resursseiltaan erilaisia tunnistuspalveluntarjoajia eli tunnistusvälineen tarjoajia ja soveltuvin osin tunnistusvälityspalveluita. Määräyksen vaatimusten tarkoitus on parantaa turvallisuutta, mutta myös parantaa sääntelyn ennakoitavuutta tunnistuspalveluiden toiminnan helpottamiseksi. Selkeät vaatimukset luovat viraston arvion mukaan myös keskinäistä luottamusta luottamusverkoston nykyisten ja tulevien tunnistuspalveluiden tietoturvallisuuteen.

Suojautumiskyky tietoturvauhkilta. Sähköisen tunnistamisen varmuustasoasetuksen kohdan 2.3.1 mukaan

> *Todentamismekanismissa toteutetaan turvatoimenpiteitä sähköisen tunnistamisen menetelmän varmentamiseksi siten, että on erittäin epätodennäköistä, että viestin arvaaminen, salakuuntelu, toisto tai manipulointi hyökkäyksessä, jonka vakavuusaste on kohtuullinen (”moderate attack potential)”), voi heikentää todentamismekanismeja.*

Korkealla varmuustasolla turvatoimenpiteet on mitoitettava korkean ("high") vakavuusasteen hyökkäykseltä suojautumiseksi.

Sähköisen tunnistamisen varmuustasoasetuksen kohdan 2.4.6 mukaan

> *1. Käytössä on oikeasuhteiset tekniset tarkastukset ("technical controls") palvelujen turvallisuuteen kohdistuvien riskien hallitsemiseksi ja käsiteltävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi.*

Sähköisen tunnistamisen varmuustasoasetuksen kohdassa 2.4.6 säädetään myös sähköisen viestinnän kanavien suojaamisesta salakuuntelua, manipulointia ja toistoa vastaan, salausteknisen aineiston suojaamisesta, valmiudesta reagoida riskin muutoksiin, poikkeamiin ja tietoturvaloukkauksiin sekä laitteiden ja välineiden tietoturvallisuudesta.

Tietojärjestelmä-, tietoliikenne- ja käyttöturvallisuus. Säännöksissä 5.2-5.4 kohdissa tarkennetaan tietoliikenne-, tietojärjestelmä- ja käyttöturvallisuutta, jotta säädännössä vaadittu tietoturvallisuus toteutuisi. Tarkennukset perustuvat tietojärjestelmien turvallisuuden yleisesti käytettyyn jaotteluun tietojärjestelmä- tietoliikenne- ja käyttöturvallisuuteen. Alueet eivät sulje toisiaan pois, vaan ovat pikemminkin eri näkökulmia samaan tunnistusjärjestelmän kokonaisuuteen.

Eriyttäminen tietoturvatoimenpiteenä. Henkilöstön työtehtävien eriyttäminen, fyysisten työtilojen ja -välineiden eriyttäminen tai teknisen palveluympäristön ja palvelinympäristöjen mahdollinen eriyttäminen muusta tuotannosta ovat osa normaaleja hyviä käytäntöjä. Riittävän eriyttämisen oletetaan toteutuvan normaalin tietoturvallisuuden hallinnan, suunnittelun ja auditoinnin kautta, eikä asiasta määrätä erikseen lukuun ottamatta säännöksen 5.5 vaatimusta.

Vaikutukset. Säännöksen 5 vaatimukset eivät muutu, mutta niitä selvennetään. Säännöstä on tarkennettu ja perusteluihin on lisätty esimerkkejä soveltamisesta tunnistuspalveluiden vaatimustenmukaisuuden arvioinnissa ja valvonnassa kertyneen kokemuksen ja soveltamiskäytännön perusteella.

Muutokset ovat omiaan parantamaan tunnistusjärjestelmien turvallisuutta. Vaatimukset eivät ole teknologiariippuvaisia, joten niillä ei ole vaikutusta tunnistuspalveluiden ominaisuuksien kehittämiseen.

4.5.2 Tunnistusjärjestelmän kokonaisuus (arkkitehtuuri ja alihankkijat)

Tunnistusjärjestelmä (engl. eID scheme) tarkoittaa järjestelmää, jonka puitteissa sähköisen tunnistamisen menetelmiä eli tunnistusvälineitä myönnetään ja ylläpidetään käyttäjille. Tunnistusjärjestelmä kattaa tunnistuspalvelun tarjoajan tekniset järjestelmät, tietoturvallisuuden hallinnan ja muut säädetyt luotettavuusvaatimukset. Tunnistusjärjestelmä kattaa myös kaikki alihankitut osat ja toiminnot, jotka liittyvät tunnistuspalvelun tuottamiseen. Tunnistuslain termi on *sähköisen tunnistamisen järjestelmä*.

Tunnistusjärjestelmään sisältyvät esimerkiksi seuraavat:

- konesalit ja muut tilat
- tunnistustapahtumaan liittyvät palvelimet ja ohjelmistot
- tunnistamiseen liittyvät järjestelmäkomponentit
- tunnistusjärjestelmän osien väliset yhteydet, yhdyskäytävät ja kytkennät, ml. hallintayhteydet
- yhteyksien suojauskäytännöt, järjestelmän osien väliset rajapinnat ja muut seikat - ml. ulkoisten toimijoiden yhteyksien turvallisuuskontrollit
- verkon tietoturvallisuuskomponentit, kuten palomuurit
- tietovarannot

Alihankkijat. Määräyksessä ei käsitellä erikseen alihankkijoita. Tunnistuspalvelun tarjoaja vastaa tunnistus- ja luottamuspalvelulain 13 §:n mukaan siitä, että sen alihankintana käyttämät palvelut täyttävät vaatimukset. Tunnistusjärjestelmän ja tunnis-

tusmenetelmän toteuttamisessa käytetään tyypillisesti alihankintaa. Vaatimustenmukaisuuden arvioinnin kannalta alihankintaa käsitellään Liikenne- ja viestintäviraston tunnistuspalvelun arviointiohjeessa 211/2019.

Jos tunnistusjärjestelmässä käytetään pilvipalveluiden tuotteistettuja komponentteja tai tuotteita (esimerkiksi Amazon Web Services, Google, Microsoft Azure), tunnistusjärjestelmän vaatimukset koskevat näitä komponentteja ja ne täytyy sisällyttää myös vaatimustenmukaisuuden arvioinnin piiriin. Tunnistusjärjestelmässä voi käyttää vain komponentteja, jotka täyttävät vaatimukset ja joiden vaatimustenmukaisuudesta pystytään varmistumaan.

4.5.3 Säännös 5.1.1 Tunnistusjärjestelmän suojautumiskyky

Säännös 5.1.1 on uusi. Siinä tarkennetaan tunnistusjärjestelmän turvatoimenpiteiden ja teknisten määrittelyjen kokonaisuuden vaatimustaso.

Korotetun ja korkean varmuustason yksittäisiä vaatimuksia ei pääsääntöisesti ole määritelty määräyksessä erikseen. Sen sijaan sähköisen tunnistamisen varmuustasoasetuksen kohdan 2.4.6 mukaan edellytettyjen turvatoimenpiteiden eli teknisten kontrollien vaatimustaso määritellään varmuustasoasetuksen 2.3.1 kohdan hyökkäyspotentiaalilta suojautumiskyvyn perusteella. Vaatimus koskee koko tunnistusjärjestelmän suojautumiskykyä ja siten säännöksissä 5.2–5.4 tarkennettuja tietoliikenne-, tietojärjestelmä- ja käyttöturvallisuuden osatekijöitä.

Uhka- ja riskiarvioon ei määrätä tarkempaa kriteeristöä tai noudatettavaa standardia. Aineellisen arvion on perustuttava hyvään toimialaosaamiseen ja uhkien, haavoittuvuuksien ja teknisen kehityksen seurantaan.

Ks. sähköisen tunnistamisen varmuustasoasetuksen soveltamisohje, 2.3.1 (ote)

> *Varmuustasossa eri vakavuusasteista käytettävät termit ovat "korkeampi perustaso" (enhanced-basic), "kohtuullinen" (moderate) ja "korkea" (high). Nämä termit on lainattu standardeista ISO/IEC 15408 "Information technology – Security techniques – Evaluation criteria for IT security" ja ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation". Standardien teksti on vapaasti luettavissa osoitteessa www.commoncriteriaportal.org/cc (CCPART1-3 vastaa standardia ISO/IEC 15408 ja CEM standardia ISO/IEC 18045).*
>
> *Standardissa ISO/IEC 15408-1 hyökkäyksen vakavuusaste määritellään sen työn määräksi, jota [mekanismia] vastaan hyökkääminen edellyttää, ilmaistuna hyökkääjän asiantuntemuksena, resursseina ja motivaationa.*
>
> *Standardin ISO/IEC 18045 / CEM:n liitteessä B.4 ohjeistetaan, miten lasketaan todentamismekanismin tietyn heikkouden hyväksikäyttämisen edellyttämä hyökkäyksen vakavuusaste.*
>
> *Täytäntöönpanoasetuksessa säädettyjen vaatimusten täyttäminen edellyttää mahdollisten hyökkäysten sietokyvyn arviointia.*
>
> *Arvioinnissa olisi otettava huomioon asiaankuuluvat uhat. Standardissa ISO 29115 mainitaan esimerkiksi seuraavat: verkossa ja verkon ulkopuolella tapahtuva arvaaminen, tunnistetietojen toisintaminen, tietojen kalastelu, salakuuntelu, replay-hyökkäys, istuntokaappaus, mies välissä -hyökkäys, tunnistetietojen varastaminen, spoofing-hyökkäys ja toisena esiintyminen.*

4.5.4 Säännös 5.1.2

Säännös 5.1.2 on osittain uusi. Aikaisemmassa määräyksessä on määrätty tietojärjestelmäturvallisuuden kohdalla, että on käytettävä kansainvälisesti tai kansallisesti

suositeltuja salausratkaisuja *muutoin kuin 7 §:ssä säädetyltä osin.* Vaatimus kansainvälisesti tai kansallisesti suositeltujen salausratkaisujen käyttämisestä on lisätty myös tietoliikenne- ja käyttöturvallisuuden kohdalle ja suhde säännöksen 7 salausratkaisuihin määritellään säännöksen 5 kaikkien vaatimusten kannalta säännöksessä 5.1.2.

Määräyksen 7 kohdassa määrätään tiettyjen tietoliikenneyhteyksien ja sanomien erityiset salaus- tai suojausvaatimukset. Määräyksen 5 kohdan vaatimus koskee yleisesti muita yhteyksiä ja elementtejä eli esimerkiksi tunnistusjärjestelmän sisäisiä elementtejä, säilytettäviä tietoja sekä yhteyksiä alihankkijoiden järjestelmiin. Vaatimus ulottuu sekä 5.2. tietoliikenne- että 5.3 tietojärjestelmiin ja 5.4 operointiin. Näissäkin on suositeltavaa käyttää teknisesti soveltuvin osin säännöksessä 7 määrättyjä ratkaisuja, mutta suojautumisen voi toteuttaa myös muilla turvatoimenpiteillä.

4.5.5 Säännös 5.2 Tietoliikenneturvallisuus

Säännös 5.2 vastaa pitkälti määräyksen aikaisempaa sanamuotoa 5.1 §:n 1 alakohdassa. Säännökseen on tehty tarkennuksia.

Säännöksessä 5.2 määrättyjen vaatimusten lisäksi säännöksessä 14 määrätään tietoliikenneprotokollasta ja säännöksissä 7-9 tietoliikenteen ja sanomien suojaamisesta tunnistuspalveluiden välillä ja tunnistuspalveluiden ja niihin luottavien asiointipalveluiden välillä. Tunnistusvälineen käyttäjän ja tunnistusvälineen tarjoajan välisen yhteyden turvallisuus on osa todentamismekanismin vaatimuksia säännöksessä 6.

5.2.a) verkon rakenteellinen turvallisuus

Verkon rakenteellisella turvallisuudella huolehditaan, että *henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät sähköisen viestinnän kanavat on suojattu salakuuntelulta, manipuloinnilta ja toistolta.*

Verkon rakenne on dokumentoitava. Tunnistusjärjestelmän tietoliikennelaitteet ja -järjestelmät on tunnistettu ja dokumentoitu. Rakenteellinen turvallisuus koskee tunnistusjärjestelmän osien välisiä tietoliikenneyhteyksiä ja niiden suojauskäytäntöjä. Se koskee eri turvetason verkkoalueita, sekä niiden välissä toimivia suodatus- ja valvontajärjestelmiä. Rakenteellisen turvallisuuden vaatimus kattaa myös kaikki relevantit tietoliikenneyhteydet alihankkijoihin (infra, ohjelmistot, käyttöpalvelut, korttitehdas jne.).

5.2.b) tietoliikenneverkon vyöhykkeistäminen

Vaatimuksen tavoite on vähentää tietoliikenneyhteyksien kautta aiheutuvia riskejä verkkojen eheydelle, luottamuksellisuudelle ja käytettävyydelle.

Vyöhykkeistäminen tarkoittaa mm. sitä, että tuotantoverkon, ylläpito- ja hallinnointiverkon sekä muun toimistoverkon tulee olla eriytettynä toisistaan. Lisäksi käytössä on oltava tuotannosta eriytetty kehitysympäristö.

5.2.c) suodatussäännöt vähimpien oikeuksien periaatteilla

Vähimpien oikeuksien periaate tarkoittaa sitä, että kaikki muut kuin toiminnalle tarpeelliset yhteydet pitää kieltää tai sulkea. Tuotantoverkon yhteyksien julkiseen verkkoon tulee olla riskiperusteisia, vain palvelun toiminnallisuudet mahdollistavia yhteyksiä.

5.2 d) suodatuksen ja valvontajärjestelmien hallinnointi

Ei esimerkkejä soveltamisesta. [lisätään]

5.2.e) turvalliset hallintayhteydet

Säännökseen on lisätty tarkennus "turvalliset".

Hallintayhteydet voivat olla sekä organisaation sisäisiä että ulkoisia tietoliikenneyhteyksiä. Hallintaan käytettävä tietojenkäsittely-ympäristö tulee erottaa muista ympäristöistä.

Ks. myös määräyksen kohta 5.5.

5.2.f) *kansainvälisesti tai kansallisesti suositellut salausratkaisut*

Suositeltavien salausratkaisujen lähteistä ks. tämän perustelumuistion kohta 4.4.5.

4.5.6 Säännös 5.3 Tietojärjestelmäturvallisuus

Säännös 5.3 vastaa pitkälti määräyksen aikaisempaa sanamuotoa 5.1 §:n 2 alakohdassa. Säännökseen on tehty tarkennuksia.

5.3.a) pääsyoikeuksien hallinta vähimpien oikeuksien periaatteella

Säännökseen on lisätty tarkennus "vähimpien oikeuksien periaatteella".

Vähimpien oikeuksien periaate tarkoittaa, että pääsyoikeudet tulee myöntää vain tietojärjestelmän luokitteluun ja käyttäjän tehtäviin perustuen. Pääsyoikeuksien hallinnoinnin avulla täytyy rajoittaa pääsy tietoon ja tiedonkäsittely-ympäristöihin suunnitelmallisesti ja dokumentoidusti. Tarpeettomat käyttöoikeudet täytyy poistaa säännöllisesti.

Pääkäyttäjäoikeuksien määrittelyssä on oltava erityisen huolellinen ja järjestelmä- ja tapahtumalokien eheys on varmistettava.

Pääkäyttäjien oikeuksien määrittelyssä on käytettävä järjestelmien eriyttämistä ja lokien muuttumattomuuden varmistamista ja muita tarkoituksenmukaisia keinoja.

5.3.b) järjestelmien käyttäjien yksilöity tunnistaminen

Säännökseen on lisätty tarkennus "yksilöity". Käyttäjätunnusten täytyy olla henkilökohtaisia, eivätkä ne voi olla yhteiskäyttöisiä.

Tunnistamisella varmistetaan, että vain oikeat käyttäjät pääsevät järjestelmiin ja että tapahtumat voidaan jäljittää.

Tunnistusjärjestelmän tietojärjestelmien käyttäjät täytyy tunnistaa tunnetulla ja turvallisena pidetyllä menetelmällä. Pääsääntöisesti tulisi käyttää moneen tekijään perustuvaa tunnistusta (*2FA eli 2-factor-authentication, MFA eli multi-factor-authentication*). Jos käyttäjätunnus ja salasana arvioidaan kokonaisuutena muiden suojakeinojen perusteella jossain kohdin riittäväksi, salasanojen tulee olla riittävän vahvoja.

5.3.c) järjestelmien koventaminen

Järjestelmien koventamisella tarkoitetaan, että tunnistusjärjestelmässä käytetään vain sen toiminnan kannalta tarvittavia palveluita, toimintoja, prosesseja, laitteita ja komponentteja.

Niiden käyttö tulee määritellä siten, että asennuksesta on poistettu kaikki tarpeettomat oikeudet ja toiminnot. Kovennettu asennus sisältää vain sellaiset komponentit ja

palvelut, sekä käyttäjien ja prosessien oikeudet, jotka ovat välttämättömiä toiminta-vaatimusten täyttämiseksi ja turvallisuuden varmistamiseksi.

5.3.d) haittaohjelmasuojaus

Tunnistusjärjestelmässä täytyy huolehtia haitta-ohjelmien aiheuttamien haittojen ja uhkien havaitsemisesta, ennaltaehkäisystä, estämisestä ja korjaamisesta.

5.3.e) turvallisuuteen liittyvien tapahtumien jäljityskyky ja jäljitysprosessi

Säännökseen on lisätty tarkennus "kyky ja jäljitysprosessi".

Määräyksessä edellytetään siten, että olemassa on ennalta määritelty menettely, jota noudatetaan mahdollisen turvallisuuspoikkeaman jäljittämisessä ja korjaamisessa.

Seuraavassa kohdassa kuvatut lokitukset ovat osa tapahtumien jäljityskykyä.

Jäljityskyky edellyttää, että tunnistusjärjestelmän kellonaika ylläpidetään luotettavasti. Kellonaikaa tarvitaan tapahtuma-aikojen luotettavaa osoittamista varten. Kellonajan luotettavuus tarkoittaa luotettavaa aikalähdettä ja riittävän tiukkaa virhetoleranssia. Suositeltava virhetoleranssi on 0,5 sekuntia.

5.3.f) *poikkeamien havainnointikyky ja korjausprosessi*

Säännöksessä on korvattu ilmaus "toipuminen" ilmauksella "korjausprosessi".

Määräyksessä edellytetään, että tunnistusjärjestelmän poikkeamien havaitsemiseen on kyvykkyys ja ennalta määritellyt prosessit.

Määrittelyissä tulee huomioida järjestelmän tietoliikenneyhteyksien ja tietojärjestelmien komponenttien ja prosessien kriittisyys ja luokittelu ja se, että turvallisuuteen vaikuttavat tapahtumat kyetään jäljittämään myös jälkikäteen.

Havainnointikyky edellyttää, että tunnistusjärjestelmässä kerätään ja tallennetaan tapahtumalokeja järjestelmän toiminnasta ja tietoturvaan vaikuttavista tapahtumista ja poikkeamista. Poikkeamien ja tietoturvaloukkausten havaitseminen edellyttää, että tunnistusjärjestelmän toimintaa, muutoksia ja tapahtumalokeja monitoroidaan.

Lokien eheydestä huolehditaan mm. pääsyn- ja käyttöoikeuksien hallinnalla, ympäristön suojaamisella ja tarvittaessa siirtämällä lokitietoja pois kohdejärjestelmästä. Henkilöstön työtehtävien eriyttäminen on tarpeen ainakin siltä osin, ettei sama henkilö voi luoda tunnistusvälinettä ja hallinnoida tunnistusvälineen luomiseen ja käyttöönottoon liittyviä lokitietoja.

Korjausprosessi tarkoittaa sitä, että tunnistusjärjestelmän kaikki poikkeamat ja häiriöt käsitellään ja analysoidaan ja niiden vakavuus luokitellaan suunnitelmallisesti määriteltyjen menetelmien mukaan ja poikkeamat korjataan vakavuusluokittelun edellyttämällä tavalla.

5.3.g) *kansainvälisesti tai kansallisesti suositellut salausratkaisut*

Suositeltavien salausratkaisujen lähteistä ks. tämän perustelumuistion kohta 4.7.5.

4.5.7 Säännös 5.4 Käyttöturvallisuus

5.4.a) huolellinen muutosten hallinta

Säännöksen on lisätty "huolellinen".

Vaatimuksen tarkoitus on ennaltaehkäistä tunnistusjärjestelmään tehtävien muutosten aiheuttamia virhetilanteita tietoturvallisuuden tai käytettävyyden kannalta. Muutoksilla on usein kiire ja niiden vaikutukset voivat heijastua moniin järjestelmän yksityiskohtiin. Siksi niiden huolellinen suunnittelu, prosessien vakiointi ja riittävän ajan varaaminen muutoksille on tarpeellista. Katselmoinnit ja testaaminen ovat osa luotettavaa muutosprosessia. Sekä prosessit että tehdyt muutokset on syytä dokumentoida, jotta mahdollisten virheiden syyt ovat jäljitettävissä. Asianmukaisessa dokumentoinnissa tunnistusjärjestelmän hallintalokeihin tallennetaan tiedot tunnistusjärjestelmässä tehtävistä muutoksista, lokit eriytetään muista lokeista ja niiden eheydestä huolehditaan.

5.4.b) *tiedon luokitteluun perustuva salassa pidettävän aineiston käsittely-ympäristö ja säilytys*

Säännökseen on lisätty "tiedon luokitteluun perustuva" ja "säilytys".

Säilytettävien tietojen suojaus on siirretty tähän määräyksen 7 § 4 kohdasta, joka kuului: *Tunnistusjärjestelmässä säilytettävien tietojen eheydestä ja luottamuksellisuudesta on huolehdittava. Jos tiedon suojaaminen perustuu ainoastaan niiden salaukseen, sovelletaan 1 momentin allekirjoittamisen, symmetrisen salaamisen ja tiivistefunktioiden vaatimuksia.*

Tiedon käsittelyn perusedellytys on tiedon ja aineistojen luokittelu, jonka perusteella luokitellaan tietojärjestelmät ja niiden mahdollistamat toiminnot. Järjestelmien luokittelussa tulee huomioida suojattavan tiedon koko elinkaari.

Luokittelussa on huomioitava esimerkiksi liikesalaisuudet, turvallisuusjärjestelyt ja lokit. Edelleen on huomioitava henkilötiedot ja tunnistusmenetelmien myöntämiseen liittyvät kryptografiset salaisuudet.

Tiedon käsittelyn ja säilyttämisen turvatoimet täytyy mitoittaa ottaen huomioon muun muassa tiedon luokitteluperuste, määrä, muoto ja sijoitustilat suhteessa arvioituun uhkaan. Turvatoimenpiteillä kuten pääsynhallinnalla ja salauksella täytyy turvata säilytettävien tietojen eheys ja luottamuksellisuus. Esimerkkinä erityisen huolellisesti suojattavasta tiedosta ovat salaukseen tai allekirjoitukseen käytettävät avaimet tai juurivarmenteen allekirjoitusavaimet.

5.4.c) etäkäytön ja -hallinnan suojaaminen etäkäyttöympäristön uhkilta

Säännökseen on lisätty "suojaaminen etäkäyttöympäristön uhkilta".

Ei esimerkkejä soveltamisesta tässä kohdassa. Ks. määräyksen kohta 5.5.

5.4.d) *ohjelmistokehityksen ja ohjelmistohaavoittuvuuksien hallinta*

Säännökseen on lisätty tarkennus "ohjelmistokehityksen".

Määräyksessä edellytetään, että tunnistuspalvelulla tulee olla menetelmä yleisten haavoittuvuuksien seurantaan ja sen tulee kattaa tunnistusjärjestelmän turvallisuuteen vaikuttavat ohjelmistot

Tunnistusjärjestelmässä käytettävissä ohjelmistoissa tulee noudattaa turvallisen ohjelmoinnin periaatteita. Siinä täytyy huomioida myös kehitysympäristön turvallisuus.

Ohjelmistoturvallisuuden vaatimus kattaa esimerkiksi tunnistussovellukset ja ohjelmistokirjastot.

Haavoittuvuuksien hallinta tarkoittaa ohjelmistojen ja myös salausalgoritmien ja menetelmien haavoittuvuuksien seurantaa, tiedotteiden seurantaa ja järjestelmissä käytettyjen ohjelmistojen automaattisia ja säännöllisiä tarkistuksia sekä ulko- että sisäverkon osalta.

Vrt. PiTuKri, kohta KT-04 Haavoittuvuuksien hallinta, VIITE Traficomin julkaisu 13/2020 Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

> *Pilvipalvelun koko elinkaaren ajalle toteutetaan luotettavat menettelyt ohjelmistohaavoittuvuuksien hallitsemiseksi.*
>
> *Erityisesti huomioitava:*
>
> *a) Viranomaisten, laite- ja ohjelmistovalmistajien sekä muiden vastaavien tahojen tietoturvatiedotteita seurataan ja riskiperusteisesti tarpeellisiksi arvioidut turvapäivitykset asennetaan hallitusti (vrt. MH-01).*
>
> *b) Järjestelmät tarkistetaan tunnettujen haavoittuvuuksien varalta automaattisesti vähintään kuukausittain. Jos suunnitelluista asetuksista tai turvapäivitystasosta on poikettu, syyt analysoidaan, ja poikkeamat korjataan tai dokumentoidaan poikkeamahallintaprosessin mukaisesti (ks. TJ-04).*

Haavoittuvat algoritmit ja salausmenetelmät. Määräyksen 7 kohdan sidosryhmävalmistelussa on nostettu esille kysymys siitä, miten määräyksessä hyväksytyksi listattujen algoritmien tai menetelmien mahdollinen muuttuminen haavoittuviksi ja siitä aiheutuva tarve luopua niiden käytöstä vaikuttaa 7 kohdan soveltamiseen.

5.4 d) kohdan mukaan tunnistuspalveluilla on mahdollisuus ja velvollisuus hallita haavoittuvuuksia. Tarkoituksenmukainen tapa huomioida haavoittuvuudet on seurata niitä koskevia tiedotuskanavia ja luopua omaehtoisesti haavoittuvien menetelmien käytöstä.

Viraston käsitys on, että salausalgoritmit ja menetelmät eivät muutu haavoittuviksi yllättäen, vaan kysymyksessä ovat tyypillisesti vuosien tai jopa vuosikymmenten kehityskulut. Tämä mahdollistaa määräyksen muuttamisen tarvittaessa, mutta jos määräystä ei ehdittäisi muuttaa yllättävässä tilanteessa, virasto voi ohjata haavoittuvuuksiin reagoimista neuvonnalla.

5.4.e) *varmuuskopiointi*

Varmuuskopioinnin tarkoitus on varmistaa tietojen ja järjestelmien palauttaminen häiriötilanteessa ja tietojen jäljitys tarvittaessa.

Varmuuskopioinnista täytyy huolehtia suunnitelmallisesti ja huomioida tiedon luokittelu ja elinkaari. Säilyttämisessä täytyy huomioida fyysisen sijoituspaikan eriyttäminen varsinaisesta järjestelmästä.

5.4.f) *kansainvälisesti tai kansallisesti suositellut salausratkaisut*

Suositeltavien salausratkaisujen lähteistä ks. tämän perustelumuistion kohta 4.7.5.

4.5.8 Säännös 5.5 Tunnistusjärjestelmän tuotantoverkon hallinta- ja etäyhteydet

Säännöksessä 5.5 tarkennetaan etähallinnassa käytettävän päätelaitteen ja etäyhteyden vaatimukset korotetulla ja korkealla varmuustasolla. Säännös vastaa aikaisemman määräyksen 5 § 2 momenttia.

Järjestelmän toteutus ja kontrollit täytyy suhteuttaa varmuustason mukaan joko kohtuullisen tai korkean tason hyökkäyspotentiaaliin.

Työntekijöiden päätelaitteet, joilla nämä pääsevät hallintajärjestelmiin, voivat helposti muodostua tietoturvariskiksi, ellei asiaan kiinnitetä erityistä huomiota.

Korotetulla varmuustasolla päätelaitteita ei vaadita eriyttämään, mutta korkealla varmuustasolla edellytetään joko dedikoitua päätelaitetta tai virtualisoitua terminointia tai kvm-periaatteeseen (etätyöpöytä) perustuvaa ratkaisua.

Internetiä ja toimistoverkkoa pidetään ei-luotettuna verkkona, ellei toimistoverkko kuulu vaatimustenmukaisuuden arvioinnin piiriin.

Korotetun varmuustason vaatimukset ovat tavanomaisia ja ne katetaan jo esimerkiksi ISO 27001 -vaatimusten kautta, jos sovelletaan sitä. Tiedonsiirtokanavan täytyy siis olla etäkäytössä suojattu ja toimistoverkon aiheuttamat riskit täytyy huomioida.

Korkealla varmuustasolla vaatimukset voi toteuttaa ainakin siten, että etäkäytössä olevasta työasemasta estetään pääsy muihin organisaation palveluihin kuten sähköpostiin ja poistetaan työasemasta mahdollisuus käyttää muita kuin hallintaverkon käytön kannalta välttämättömiä toimintoja. Käytännössä tämä tarkoittaa siis erillistä työasemaa hallintakäyttöä varten.

Korkealla varmuustasolla edellytetty *kokonaisarvio* tarkoittaa sitä, että jos käytettään muuta kuin edellä kuvattua kovennettua työasemaa, otetaan toteutuksessa huomioon tuotantojärjestelmän eriyttäminen ja muut järjestelyt, joilla tietoturvauhkat voidaan hallita. Lähtökohtaisesti tällöin edellytetään virtualisoitua terminointia tai kvm-periaatteeseen (etätyöpöytä) perustuvaa ratkaisua.

Olennaista on, mitä tehdään sillä päätelaitteella, josta virtualisoitua yhteyttä otetaan ja siten esimerkiksi two-factor VPN-yhteys virtualisoituun työasemaan ei yksin riitä ratkaisuksi. Riittävää ei ole myöskään, että käytetään virustorjuntaa ja web-proxya.

Välttämättömien tiedostojen siirrossa koneelta toiselle on myös huomioitava haittaohjelmien riski mm. pitämällä huolta siitä, että käytetään vain luotettavia lähteitä ja varmistetaan tietoturvallisuus (eheys) kaikilla tarpeellisilla menetelmillä.

4.5.9 Säännös 5, muut ohjauskeinot

Ohje. Arviointiohjeessa 211/2019 on tarkennettu tietoturvallisuuden arvioinnin vaatimuksia.

Suositus. Määräysmuutostarvekyselyssä on toivottu viraston tarjoamaa testauspalvelua. Virastolla ei kuitenkaan ole vahvan sähköisen tunnistamisen valvonnassa säädettyjä operatiivisia tehtäviä kuten testaustoiminnan hankintaa tai ylläpitoa. Testaussuosituksen laatiminen tunnistuspalveluiden itse tarjoamille testaustoiminnoille olisi mahdollista luottamusverkostossa.

Yhteissääntely. Tietoturvallisuuden taso on sääntelyssä ja valvonnassa määritelty asia. Vahvan sähköisen tunnistuspalvelun tarjoajilla on mahdollisuus vaihtaa salassapitosäännösten estämättä tietoa turvallisuusuhkista ja -toimenpiteistä.

Informaatiolla ohjaaminen. Ei huomioita.

4.5.10 Säännös 5, harkitut sääntelyvaihtoehdot

4.5.10.1 Säännökset 5.1-5.4 ja tunnistusjärjestelmän korkean varmuustason vaatimukset

Määräysmuutostarvekyselyssä osa vastaajista toivoi korotetun ja korkean varmuustason teknisten vaatimusten tarkkaa määrittelyä määräyksessä. Ehdotuksia vaatimuksista, joissa tarkennuksia erityisesti tarvitaan, ei kuitenkaan tullut esille.

Virasto katsoo, että varmuustasojen vaatimusten tarkentaminen määräyksessä ei ole mahdollista, koska tunnistusjärjestelmään sisältyy lukuisia osatekijöitä. Yksityiskohtainen määrääminen ei olisi tarkoituksenmukaista, koska tekniset toteutukset ja uhkat muuttuvat jatkuvasti.

Määräyksessä on sen sijaan selvennetty ja tarkennettu kaikkien turvatoimenpiteiden suhteuttamista varmuustason mukaiseen hyökkäyspotentiaaliin.

4.5.10.2 Säännökset 5.2 - 5.4 ja eriyttämisvaatimukset tietoturvatoimenpiteenä

Vuoden 2021 määräysvalmistelussa ei ole ilmennyt perusteita tai tarvetta määrätä uusia eriyttämisvaatimuksia.

Eriyttäminen tietoturvatoimenpiteenä. Määräyksen valmistelussa arvioitiin vuonna 2016, onko tietoturvavaatimusten takia tarpeen jokin seuraavista: henkilöstön työtehtävien eriyttäminen, fyysisten työtilojen ja -välineiden eriyttäminen tai teknisen palveluympäristön ja palvelinympäristöjen mahdollinen eriyttäminen muusta tuotannosta.

Vaikutusarvioinnissa päädyttiin tuolloin siihen, että jätettiin eriyttäminen yksityiskohdiltaan pääosin yleisen tietoturvallisuuden hallinnan, suunnittelun ja auditoinnin varaan. Vaikutusarvioinnissa katsottiin 2016, että henkilöstön työtehtävien eriyttäminen on tarpeen ainakin siltä osin, ettei sama henkilö voi luoda tunnistusvälinettä ja hallinnoida tunnistusvälineen luomiseen ja käyttöönottoon liittyviä lokitietoja. Tämän oletettiin toteutuvan jo normaalin tietoturvallisuuden hallinnan, suunnittelun ja auditoinnin kautta, eikä asiasta ole tarpeen määrätä erikseen.

Hallintaverkossa ja toimistoverkossa käytettävien työasemien turvallisuusvaatimusten määrittely herätti 2016 valmistelussa niin paljon kysymyksiä, että vaatimukset selkeytettiin määräyksessä 5 §:n 2 momentilla ja perustelumuistion soveltamisohjeilla. Ne pidetään sellaisenaan määräyksessä ja perusteluissa.

4.5.11 Suositus tunnistusjärjestelmän kellonajan luotettavuudesta (määräyksen perustelumuistio 2016 C-osa kohta 1)

Määräysvalmistelussa on harkittu tunnistusjärjestelmän aikalähteen ja kellonajan virhetoleranssia koskevan suosituksen poistamista, koska sen soveltaminen ei ole tullut esille tunnistuspalveluiden ohjauksessa ja valvonnassa tai sidosryhmäpalautteessa.

Tunnistusjärjestelmän kellonaika on kuitenkin osa yleistä tietoliikenne- ja tietojärjestelmien hyvää ylläpitoa, joten asia säilytetään perusteluissa, mutta siirretään maininnat tunnistusjärjestelmän tietojärjestelmäturvallisuuden kohtaan.

Suositus MPS72 (sama 2.11.20216 ja 14.5.2018) C-osa kohta 1

Suositellaan, että tunnistuspalveluntarjoaja hankkii luotettavan aikalähteen, jonka kanssa ne synkronoivat tunnistusjärjestelmässään käytetyn kellonajan. Kellonaikaa tarvitaan tapahtuma-aikojen luotettavaa osoittamista varten. Suositeltava virhetoleranssi on 0,5 sekuntia. Synkronointia toimijoiden välillä ei tarvittane.

Aiheeseen liittyy suositus ITU-R TF.1876 (03/2010) Trusted time source for time stamp authority [51].

Mahdollisia aikalähteitä ovat esimerkiksi VTT:n/MIKESin NTP tai PTP, joista jälkimmäiseen liittyy myös saatavuustakuu. Muitakin on tarjolla.

4.6 Säännös 6 Tunnistusmenetelmän tietoturvavaatimukset

4.6.1 Säännös 6.1 Tunnistusmenetelmän ominaispiirteet ja suojautumiskyky

4.6.1.1 Säännös 6.1.1 Eritelty riskiarvio

Säännös on uusi.

Säännöksessä 6.1.1 tunnistusmenetelmän todentamistekijöiden ja todentamismekanismin muodostaman kokonaisuuden turvallisuusvaatimuksia tarkennetaan lisäämällä määräykseen vaatimukset erityisestä riskiarviosta ja siinä huomioitavista seikoista. Todentamistekijöiden ja todentamismekanismin uhkat on arvioitava erikseen. Tunnistusmenetelmä eli siinä käytettävät todentamistekijät ja turvatoimenpiteet on suunniteltava siten, että kokonaisuus suojaa arvioiduilta uhkilta.

Virasto arvioi, että tällainen malli on tarpeeksi joustava eri tunnistusmenetelmien ja todentamistekijöiden suhteen ja huomioi tunnistusmenetelmän turvakontrollit kokonaisuutena. Viraston mahdolliset valvontaratkaisut tulisivat perustumaan tunnistuspalvelun tarkkaan riskiarvioon, jossa huomioidaan myös turvakontrollien vaikutus.

Siirtymäaika. Virasto katsoo sidosryhmäpalautteen perusteella, että vaatimukselle ei tarvita siirtymäaikaa, vaan velvollisuus arvion laatimiselle voi tulla voimaan muutetun määräyksen voiman tullessa.

Valvonta. Virasto arvioi erikseen, valvotaanko arvion tekemistä ja tuloksia määräyksen voimaan tullessa vai sanan säännöllistä vaatimustenmukaisuuden määräaikaisarviointia vai erikseen. Erillinen arviointivaatimus koskee määräyksen voimaantulon jälkeen virastolle ilmoitettavia muutoksia tunnistusmenetelmissä.

Sidosryhmäpalautteen perusteella riskilähtöinen lähestymistapa on toimiva, mutta on hyvä ohjeistaa, mitä arvioidaan ja millä metodilla, jotta jäännösriskin hyväksyttävyys on mahdollisimman ennakoitava. Tässä sääntelymallissa tarkennetaan riskiarvion tekemisen vaatimusta ja osatekijöitä, jotka siinä on otettava huomioon. Soveltamista käsitellään seuraavissa kohdissa.

Vaihtoehtoiset sääntelytavat. Virasto on arvioinut 6.1.1 kohdan vaihtoehtoina sääntelymalleja, joissa määräyksessä tarkennettaisiin todentamistekijäkohtaiset vaatimukset tai tarkennettaisiin tunnistusmenetelmän suojautumiskyvyn vaatimukset. Todentamistekijäkohtaiseen sääntelytapaan liittyisi todentamistekijöiden moninaisuuden ja kehittymisen takia paljon yksityiskohtia, joita ei ole viraston arvion mukaan mahdollista eikä tarkoituksenmukaista pyrkiä kattamaan säännöstasolla. Myöskään uhkat tunnistusmenetelmän turvallisuudelle ja turvakeinot uhkilta suojaamiselle eivät ole puhtaasti todentamistekijätyyppikohtaisia. Suojautumiskyvyn mittareita tai muunlaisia tarkennuksia määräyksessä voisi ajatella.

*Vaikutukset. V*irasto arvioi, että vaatimus riskiarvion tekemisestä on luonteva osa tunnistuspalvelun tyyppisen tietoteknisen palvelun tuottamista ja osa säädettyä tietoturvallisuuden hallinnan vaatimusta. Määräyksen erityinen vaatimus voi tarkentaa arvioinnin vaatimuksia ja lisätä dokumentointivaatimuksia. Virasto arvioi, että vaatimus edistää tunnistusmenetelmien turvallista kehitystä ja tarjoaa perustellun pohjan viraston mahdollisille valvontatoimenpiteille.

4.6.1.2 Riskiarviossa huomioitavia uhkia

Uhka-arviossa huomioon otettavat uhkat perustuvat hyvään toimialaosaamiseen, tunnistuspalvelun ylläpidossa kertyvään tietoon, luottamusverkoston yhteistoiminta-ryhmässä saatavaan luottamukselliseen tietoon ja yleisesti saatavilla olevaan tietoon tietoturvauhkista ja haavoittuvuuksista.

Varmuustasoasetuksen soveltamisohje, LOA Guidance:

> *Arvioinnissa olisi otettava huomioon asiaankuuluvat uhat. Standardissa ISO 29115 mainitaan esimerkiksi seuraavat: verkossa ja verkon ulkopuolella tapahtuva arvaaminen, tunnistetietojen toisintaminen, tietojen kalastelu, salakuuntelu, replay-hyökkäys, istuntokaappaus, mies välissä -hyökkäys, tunnistetietojen varastaminen, spoofing-hyökkäys ja toisena esiintyminen.*

Tunnistusvälineen ja -menetelmän ominaispiirteistä riippuen uhka-arviossa huomioon otettavia uhkia ja niiden yhdistelmiä ovat ainakin esimerkiksi seuraavat (ISO 29115 -standardissa [VIITE] ja NIST 800-63B [VIITE] mainitut, https://pages.nist.gov/800-63-3/sp800-63b.html)

ISO 29115
- Online guessing/yhteydellinen arvailu
- Offline guessing/yhteydetön arvailu
- Credential duplication/tunnusten kopiointi
- Phishing/kalastelu, urkinta
- Eavesdropping/salakuuntelu
- Replay attack/toistohyökkäys
- Session hijacking/istunnon kaappaus
- Man-in-the-middle/väliintulohyökkäys
- Credential theft/tunnusten anastaminen
- Spoofing/huijaus, toisena esiintyminen, toisena esiintyminen tietojen väärentämisen avulla
- Masquerading/naamiointi, tekeytymishyökkäys

NIST 800-63B
- Assertion Manufacture or Modification/assertion/väärän vakuutuksen muodostamien tai vakuutuksen muuttaminen
- Theft/varkaus
- Duplication/kahdennus
- Eavesdropping/salakuuntelu
- Offline Cracking/yhteydetön murtaminen
- Side Channel Attack/sivukanavahyökkäys
- Phishing or Pharming/kalastelu/sivustoharhautus
- Social Engineering/käyttäjän manipulointi
- Online Guessing/yhteydellinen arvailu
- Endpoint Compromise/päätelaitteen vaarantaminen
- Unauthorized Binding/luvaton liittäminen/yhdistäminen

4.6.1.3 Todentamistekijöiden tyypilliset uhkat

Seuraavassa on esimerkkejä todentamistyyppikohtaisista uhkista. Lista ei ole kattava, vaan esimerkinomainen.

Varmuustasoasetuksen soveltamisohje, LOA Guidance:

> *Tyypillisiä hallussapitoon perustuviin todentamistekijöihin kohdistuvia hyökkäyksiä ovat varkaus, toisintaminen tai väärentäminen (muuttaminen) sekä hallussapitoa koskeviin todisteisiin kohdistuvat hyökkäykset todentamishetkellä.*

Painettu tunnuslukulista. Kopioitavuus, kalastelu, varastaminen, kohdepalvelun maskeeraus

SMS OTP. Päätelaitteessa olevat haittaohjelmat, SIM-kortin vaihto, SMS-yhdyskäytävien puutteellinen suojaus, puhelinlukitusten ohitus (SMS -viesti näkyy lukitun puhelimen ruudulla), kalastelu/huijaussivut, kohdepalvelun maskeeraus

Tunnuslukulaite. Sivukanavahyökkäys (side channel attack), varastaminen, kalastelu/huijaussivut.

Tunnistussovellus. Päätelaitteessa olevat haittaohjelmat, varastaminen ja tietoon perustuvan tekijän vakoilu (esim. olan yli) tai huono biometrinen sensori, istunnon kaappaus, kohdepalvelun "maskeeraus", tunnistussovelluksen aktivointi/luvaton kytkeminen kalastelun kautta

Varmuustasoasetuksen soveltamisohje, LOA Guidance:

> *Tyypillisiä tiedossa oloon perustuviin todentamistekijöihin kohdistuvia hyökkäyksiä ovat arvaaminen, tietojen kalastelu (phishing), salakuuntelu tai toisintaminen. Tiedossa oloon perustuville todentamistekijöille ominaista on, että sähköisen tunnistamisen menetelmää käyttävä henkilö ei välttämättä edes huomaa hyökkäyksiä. Esimerkkejä: raakaan voimaan tai sanakirjan käyttöön perustuvat hyökkäykset, joiden kohteena ovat salasanat, joiden entropia on heikko ja joita kysyttäessä ei lasketa uudelleenyritysten määrää; kirjeestä tai sähköpostiviestistä haltijan tai varmentajan huomaamatta kopioidut salasanat.*

Salasana/salasanalause. Arvaaminen, selvitys, varastaminen, kalastelu/huijaussivut.

PIN-koodi. Arvaaminen, selvitys, varastaminen, kalastelu/huijaussivut.

Oletettuun tietoon perustuvat tekijät (kysymys-vastausparit). Arvaaminen, selvitys, varastaminen, kalastelu/huijaussivut.

Varmuustasoasetuksen soveltamisohje, LOA guidance:

> *Luontaisissa todentamistekijöissä on syytä olla vaihtelua myös ominaisuuksiltaan samanlaisten ihmisten välillä, jotta henkilön yksilöinti on mahdollista; esimerkkejä ovat sormenjälki, kämmenjälki, kämmenen verisuonisto, kasvot, käden geometria ja silmän iiris. Biometrisiä tekijöitä käytettäessä on tärkeää varmistaa, että henkilö, johon todentamistekijä liittyy, on varmentamispaikassa fyysisesti läsnä. Näin vähennetään huijausten tai toisintamisen vaaraa.*

Sormenjälki. Teknisestä toteutuksesta johtuva suhdeluvultaan alhainen FAR (False Acceptance Rate), kopiointi (pinnoilta, valokuvista), haittaohjelmat, onko käyttäjä tiedoton.

Kasvot. Teknisestä toteutuksesta johtuva suhdeluvultaan alhainen FAR (False Acceptance Rate), presentaatiohyökkäykset.

Jatkuvaan mittaukseen perustuvat. Ei huomioita.

4.6.1.4 Todentamismekanismi (autentikointi)

Todentamismekanismi tarkoittaa niitä teknisiä toimenpiteitä, joilla todennetaan, että käyttäjällä on hallussaan, tiedossaan tai ominaisuutenaan häneen kytketyt tunnistusvälineen todentamistekijät. Vahvassa sähköisessä tunnistamisessa sääntelyssä edellytetään dynaamista todentamista eli sitä, että jokaisen tunnistusistunnon täytyy olla ainutkertainen, eikä se saa olla toistettavissa.

Kuten alla olevat esimerkit osoittavat, todentamisen uhkia ei voi tarkasti erottaa todentamistekijöihin liittyvistä uhkista. Todentamisen erityiset uhkat liittyvät viraston arvion mukaan ja varmuustasoasetuksen soveltamisohjeen valossa ainakin tietoliikenteeseen.

Sähköisen tunnistamisen varmuustasoasetuksen soveltamisohje, LOA Guidance:

> *Hyökkäysten sietokyvyn arvioinnissa on syytä ottaa huomioon koko todentamismekanismi, myös sähköisen tunnistamisen menetelmän hallussapidon varmentamisesta aiheutuvat riskit.*
>
> *Esimerkkejä:*
>
> - *Korkeassa varmuustasossa ei riitä, että älykortti suojaa salausavainta korkean vakavuustason väärentämisyrityksiltä, vaan myös salausprotokollan on suojattava avaimen hallussapidon varmentamista korkean vakavuustason väärentämis- tai toistoyrityksiltä.*
> - *Kun kyse on kertakäyttöisestä salasanatunnisteesta, jossa muodostettu kertakäyttösalasana toimitetaan suojatussa kanavassa (esimerkiksi TLS), hallussapitoon perustuvan tekijän vahvuuteen vaikuttavat tunnisteen vahvuus ja suojatun kanavan vahvuus.*
> - *Aikaperusteiselle kertakäyttösalasanojen muodostajalle hallussapidon todistamismekanismi on muodostetun kertakäyttösalasanan lähettäminen varmentajalle. Tämän mekanismin vahvuutta rajoittaa muun muassa kertakäyttösalasanan pituus, salasanan voimassaoloaika sekä toimitustavan luottamuksellisuus.*

Varmuustasoasetuksen soveltamisohje, LOA Guidance:

> *Dynaamisen todentamisen ensisijainen tarkoitus on vähentää esimerkiksi mies välissä (Man in the Middle) -tyyppisten hyökkäysten vaaraa tai riskiä siitä, että aiemmin tallennetun todentamiskerran varmentamistietoja käytetään uudelleen. Tähän sisältyvät esimerkiksi seuraavat:*
>
> - *replay-hyökkäykset eli varmentamistietojen kaappaaminen ja uudelleen käyttäminen toisessa todentamistilanteessa*
> - *tietynlaiset istuntokaappaukset, esimerkiksi tapaukset, joissa vaihdetaan keskenään osittain tai kokonaan kaksi tai useampia yhtäaikaisia todentamistilanteita.*
>
> *On syytä muistaa, että useaan tekijään perustuva ja dynaaminen todentaminen eivät tarkoita samaa asiaa. Useaan tekijään perustuvassa todentamisessa ei edellytetä, että todentaminen tapahtuu dynaamisesti (esimerkkejä ovat PIN-koodi ja sormenjälkitiedot), joten tällainen todentamistapa voi olla alttiimpi replay-hyökkäykselle kuin dynaaminen todentaminen.*

Dynaaminen todentaminen voidaan toteuttaa todentamistekijän avulla (esimerkiksi laitteesta saatava kertakäyttöinen avain) tai todentamismekanismilla (esimerkiksi dynaaminen kysymys haaste-vaste-todentamisessa).

Esimerkkejä dynaamisista todentamistavoista:

- *henkilön hallussa oleva älykortti, jolle tallennettu yksityinen avain varmennetaan haaste-vaste-menetelmällä*
- *protokollat, jotka perustuvat tilapäisiin Diffie-Hellman-avaimiin ja tuottavat todentamismenetelmän (esimerkiksi PACE), salaukseen tarkoitetun tilapäismuodosteen (nonce), aikaleiman ja/tai kertaluonteisen numerosarjan.*
- *protokollat, jotka perustuvat staattisesti muodostettuihin tilapäisiin DiffieHellman-avaimiin, jos luottava osapuoli antaa tilapäisen avaimen (esimerkiksi laajennettu pääsynvalvonta)*
- *dynaamisesti muodostettavat kertakäyttöiset pääsykoodit (esimerkiksi OTP-tunnisteet) tai haaste-vaste-protokollat, joissa kertakäyttöinen koodi on tuotettu aiemmin ja jaettu kaistan ulkopuolella ja joissa koodi valitaan dynaamisesti todentamisen yhteydessä (esimerkiksi OTP-kortit).*

Jos henkilön yksityinen avain on tallennettu etäpalveluna (keskitetysti esimerkiksi tunnistustietojen tarjoajan käyttämälle HSM-laitteelle), yksityisen avaimen käyttämiseen vaadittavan todentamistavan on myös oltava dynaaminen.

4.6.1.5 Turvatoimenpiteet

Sähköisen tunnistamisen varmuustasoasetuksen soveltamisohje, LOA guidance:

Hallussapitoon perustuvan todentamistekijän (esimerkiksi tunnistevälineen) olennaisena turva-ominaisuutena on se, että se on yksinomaan omistajansa hallinnassa. Tämä edellyttää, että todentamistekijän jäljentäminen on kolmannelle osapuolelle niin vaikeaa ja epätodennäköistä, että tällainen vaara on merkityksetön. Varmuustasoon vaikuttaa jäljentämisyritysten sietokyky.

Esimerkkejä: epäsymmetriset (yksityiset) salausavaimet, erityiseen laitteeseen (esimerkiksi älykortille) tallennetut yksityiset avaimet, ohjelmistotunnisteet, yksilöitävät tunnisteet (esimerkiksi matkapuhelimen SIM-kortti) tai kertakäyttöistä salasanaa (esimerkiksi RSA-tunnistetta tai paperikortilla olevaa salasanaa) käyttävät laitteet.

Painettu tunnuslukulista. Käyttäjän ohjeistus

SMS OTP. Tunnistuspalvelun ulottumattomissa; SMS-yhdyskäytävän turvaaminen, SIM-korttien/eSIM:n vaihtoprosessi. Käyttäjän ohjeistus, luottavan osapuolen nimen näyttäminen käyttäjälle selainkäyttöliittymässä

Tunnuslukulaite. Sertifiointi, sertifioitujen sirujen/teknologisten ratkaisujen käyttö, jotka ovat vastustuskykyisiä sivukanavahyökkäykselle, käyttäjän ohjeistus, luottavan osapuolen nimen näyttäminen käyttäjälle selainkäyttöliittymässä

Tunnistussovellus. Tunnistuspalvelun arviointiohjeessa 211/2019 liitteen C kriteerit, istuntotunnisteen näyttäminen käyttäjälle (*session binding*), luottavan osapuolen nimen välittäminen sovellukselle asti, käyttäjän ohjeistus. Hallussapidon varmistamiseksi tulee huomioida uuden tunnistussovelluksen (instanssin) aktivoinnissa/kytkemisessä käyttäjän tiedotus käyttäen toista kanavaa ja varmistettuja yhteystietoja.

Sähköisen tunnistamisen varmuustasoasetuksen soveltamisohje, LOA guidance:

Jos tietoa käytetään todentamistekijänä, on syytä yrittää tehdä kyseisen tiedon arvaamisesta (joko satunnaisesti tai ns. raa'an voiman/laskentatehon avulla) vastapuolelle mahdollisimman vaikeaa.

Esimerkki: kun tieto on salasana, hyvä toimintatapa edellyttää sopivaa salasanakäytäntöä (ks. esimerkiksi BSI IT-Grundschutz -opas S.2.11 "Provisions concerning the use of passwords" sekä NIST 800-63-2, liite A, kohdat "Single Token Authentication" ja "Password Entropy").

Salasana/salasanalause. Käyttäjien ohjeistus, vaatimukset monimuotoiselle salaisuudelle, väärien yritysten määrän rajoittaminen

PIN-koodi. Käyttäjien ohjeistus, pituusvaatimus, sovelluksen/alustan tarjoamien turvakeinojen käyttö syöttövaiheessa, väärien yritysten määrän rajoittaminen

Oletettuun tietoon perustuvat tekijät (kysymys-vastausparit). Käyttäjien ohjeistus, useampi kysymys-vastauspari, kysymysten ei pidä pohjautua muista rekistereistä tai lähteistä saatavaan tietoon.

Sähköisen tunnistamisen varmuustasoasetuksen soveltamisohje, LOA guidance:

Luontaisissa todentamistekijöissä on syytä olla vaihtelua myös ominaisuuksiltaan samanlaisten ihmisten välillä, jotta henkilön yksilöinti on mahdollista; esimerkkejä ovat sormenjälki, kämmenjälki, kämmenen verisuonisto, kasvot, käden geometria ja silmän iiris. Biometrisiä tekijöitä käytettäessä on tärkeää varmistaa, että henkilö, johon todentamistekijä liittyy, on varmentamispaikassa fyysisesti läsnä. Näin vähennetään huijausten tai toisintamisen vaaraa.

Tunnistuspalvelun arviointiohjeessa 211/2019 liitteessä C on kriteerejä biometrisen todentamistekijän käytöstä sovelluksen yhteydessä. Turvatoimenpiteissä on huomioitava sekä sovelluksen että laitteen ominaisuudet.

Ominaisuuteen perustuvan tekijän kohdalla on pyrittävä arvioimaan päätelaitteen sensorien kyvykkyys ja vertailualgoritmien toteutus. Yleisesti käytetyt termit, kuten FAR (False Acceptance Rate) ja FRR (False Rejection Rate) ovat nykyisin käytettyjä mittareita. Näistä olennaisempi on False Acceptance Rate, joka tarkoittaa sitä suhdetta kuinka todennäköistä on saada hyväksytty vastaus väärälle henkilölle. Uusintayritysten määrä nostaa todennäköisyyttä saada hyväksytty vastaus väärälle henkilölle, joten ominaisuuteen perustuvassa tekijässä tulee huomioida myös tämä vaikutus rajoittamalla yritysten määrää. Hyväksytyt FAR -arvot tulee perustaa riskiarviointiin.

Ominaisuuteen perustuvien toteutusten tunnuslukuja voi tarkastella ja testata esim. Face Recognition Vendor Test (FRVT) projektin sivuilla, https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt

On huomattava, että näihin tekijöihin tunnistuspalvelun tarjoaja ei yleensä voi vaikuttaa, kun käytetään päätelaitteen omia rajapintoja. Tunnistuspalvelun tarjoaja voi lähinnä pyrkiä selvittämään ja seuraamaan sellaisten toimintojen laatua, joita ottaa käyttöön omassa tunnistusmenetelmässään.

Koottu esimerkkilista mahdollisista turvatoimenpiteistä

- Istunnon pituuden rajoittaminen
- Virheellisten yritysten enimmäismäärä
- Salasanan pituus ja satunnaisuus
- Useamman todentamistekijän vaatimus
- Sietorajat false positivelle (sormenjälki, kasvot, muu biometrinen)
- Salaus
- salaisuuksien käsittely ja säilyttämisen turvallisuus

- Kopioinnin esto

4.6.1.6 Riskiarvio ja hyökkäyspotentiaali

Riskinhallinta on osa säännöksen 4.2 3 alakohdassa edellytettyä tunnistuspalvelun tietoturvallisuuden riskien hallintaa, joten tunnistuspalveluilla on oletettavasti jo käytössä jokin riskinhallintamalli. Riskihallinnan vaatimuksia ja mahdollisia standardeja käsitellään edellä säännöksen 4 perusteluissa.

Tunnistusmenetelmän riskinsieto ja jäännösriskin hyväksyttävyys on suhteutettava suojautumiskyvyn vaatimukseen tietyntasoista hyökkäyspotentiaalia vastaan.

Sähköisen tunnistamisen varmuustasoasetuksen soveltamisohjeessa mainitaan hyökkäyksen vakavuusasteen arvioinnin referenssinä kaksi standardia seuraavasti:

Sähköisen tunnistamisen varmuustasoasetuksen soveltamisohje, LOA guidance:

> *Todentamisvaiheessa käytetyillä todentamismekanismeilla ei voi estää täysin kaikkia hyökkäyksiä, vaan niillä voidaan vain vastustaa hyökkäyksiä tietyllä turvallisuus- tai varmuustasolla. Tavanomainen tapa mitata eri mekanismien tuottamaa sietokykyä on asettaa mekanismit järjestykseen sen mukaan, miten hyvin ne kestävät tietyn vakavuusasteen hyökkäyksiä (eli hyökkääjän voimaa).*
>
> *Varmuustasossa eri vakavuusasteista käytettävät termit ovat "korkeampi perustaso" (enhanced-basic), "kohtuullinen" (moderate) ja "korkea" (high). Nämä termit on lainattu standardeista*
>
> *ISO/IEC 15408 "Information technology – Security techniques – Evaluation criteria for IT security" ja ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation". Standardien teksti on vapaasti luettavissa osoitteessa www.commoncriteriaportal.org/cc (CCPART1-3 vastaa standardia ISO/IEC 15408 ja CEM standardia ISO/IEC 18045).*
>
> *Standardissa ISO/IEC 15408-1 hyökkäyksen vakavuusaste määritellään sen työn määräksi, jota [mekanismia] vastaan hyökkääminen edellyttää, ilmaistuna hyökkääjän asiantuntemuksena, resursseina ja motivaationa.*
>
> *Standardin ISO/IEC 18045 / CEM:n liitteessä B.4 ohjeistetaan, miten lasketaan todentamismekanismin tietyn heikkouden hyväksikäyttämisen edellyttämä hyökkäyksen vakavuusaste.*
>
> *Täytäntöönpanoasetuksessa säädettyjen vaatimusten täyttäminen edellyttää mahdollisten hyökkäysten sietokyvyn arviointia.*

4.6.1.7 Säännös 6.1.2 Todentamistekijöiden riippumattomuus

Säännöksessä 6.1.2 lisätään myös vaatimus tunnistusmenetelmän ominaispiirteistä ja turvatoimenpiteistä todentamistekijöiden riippumattomuuden varmistamiseksi. Tekijöiden riippumattomuus on välttämätön turvatoimenpide etenkin, jos eri tekijöitä käytetään samalla päätelaitteella kuten älypuhelimella. Eriyttämisen käytännön toteutus ja mahdolliset turvatoimenpiteet riippuvat menetelmästä.

4.6.1.8 Säännös 6.1.3 Tunnistusmenetelmän ja todentamisen salausvaatimukset

Säännöksessä 6.1.3 tarkennetaan tunnistusmenetelmän ja todentamismekanismin salausvaatimuksia. Säännös vastaa säännöstä 5.1.2, jossa määrätään koko tunnistusjärjestelmän salausteknisestä laadusta.

Muutoin tunnistuspalveluiden ja luottavan osapuolen tietoliikenteen salauksesta määrätään säännöksessä 7 ja sanomien suojaamisesta säännöksessä 9.

Säännöksellä 6.1.3 tarkennetaan 6.1.1 kohdan suojausvaatimuksia salausratkaisujen osalta. Säännöksen mukaan on käytettävä kansainvälisesti tai kansallisesti suositeltuja ratkaisuja. Salausratkaisujen määrittelyssä ja valinnassa on samoin kuin muissakin suojautumistoimenpiteissä huomioitava riskiarvio. Tietoliikenteen osalta lähtökohtana salausratkaisuissa ovat säännöksen 7 algoritmit, menetelmät ja arvot. Ilmaus teknisesti soveltuvin osin tarkoittaa ylipäätään teknisesti soveltuvia osia ja riskiarvion huomioiminen tarkoittaa sitä, että muut turvatoimenpiteet voivat kokonaisuutena arvioiden olla peruste soveltaa säännöksen 7 ratkaisuja vain osittain.

Yleisesti luotettavaksi tunnettuja salausmenetelmiä täytyy käyttää tunnistusvälineeseen liittyvien

- haltijakohtaisten salaisuuksien luomisessa ja ylläpidossa,
- haltijakohtaisen salaisuuden (yleensä yksityisen avaimen) suojaamisessa päätelaitteessa tai taustajärjestelmässä
- ylipäätään kaikissa tunnistusmenetelmän eheyteen ja luottamuksellisuuteen vaikuttavissa toiminnoissa

Määräyksen säännöksen 7 mukaiset tietoliikenteen salausvaatimukset koskevat

- käyttäjän hallinnassa olevan tunnistusvälineen ja tunnistusjärjestelmän välistä tietoliikennettä eli tunnistusvälineen haltijan autentikointia siltä osin, kuin sanomia eivät koske säännöksen 9 vaatimukset sanomien suojaamisesta. Verrattuna säännöksessä 9 määrättyyn sanomien salaamiseen säännöksessä 6.1.3 tarkoitetaan esimerkiksi niitä haaste-vaste -sanomia, joita todentamisessa käytetään tunnistusvälineen haltijan ja tunnistusvälineen tarjoajan järjestelmän välillä.

- Esimerkkinä arviointiohjeesta 211/2019 voi poimia hard fail certificate pinningin mobiilisovelluksen sovelluksen ja taustajärjestelmän välillä

Käyttäjän tunnistusvälineen osana oleva mobiilisovellus on nykyisissä tunnistusmenetelmissä yhteydessä tunnistusvälineen tarjoajan taustajärjestelmään. Tämän osuuden tietoturvallisuudesta määrätään säännöksessä 6. Sirukortilla käytettävissä tunnistusmenetelmissä käyttäjän väline puolestaan on yhteydessä tunnistusvälineen tarjoajan kortinlukijasovellukseen, joka on osa tunnistusjärjestelmää.

Jos tunnistusmenetelmät kehittyvät esimerkiksi itsehallittavan identiteetin (Self Sovereign Identity) mallien mukaisesti siten, että käyttäjän päätelaitteessa oleva sovellus (nk. lompakkosovellus, wallet) välittää tunnistusanomia tai attribuuttien vahvistuksia luottaville osapuolille, vaatimusten toteuttaminen edellyttää todennäköisesti uutta tarkastelua. Samalla tulevat todennäköisesti arvioitavaksi vastuut ja menettelyt osapuolten varmentamisessa.

4.6.2 Säännös 6.2 Erityiset turvatoimenpiteet

4.6.2.1 Säännös 6.2.1 Asiointitapahtuman yksilöintitiedon näyttäminen käyttäjälle (session binding)

Vaatimus on uusi.

Tunnistustapahtuman tai asiointitapahtuman yksilöintitiedolla tarkoitetaan mitä tahansa merkkijonoa, kuvaa tai muuta tietoa, joka näytetään tunnistusvälineen käyttäjälle sekä tunnistusvälineessä ja asiointipalvelun sovelluksessa tai selainistunnossa (session binding). Tiedon perusteella käyttäjän tulee pystyä helposti yhdistämään tunnistuspyyntö asiointitapahtumaan. Tarkoitus on mahdollistaa se, että tunnistusvälineen käyttäjä voi jättää vahvistamatta mahdolliset väärät tai petolliset tunnistuspyynnöt.

Vaatimus koskee luonnollisesti vain sellaista tunnistusmenetelmää, jossa on oma näyttö. Esimerkiksi kertakäyttösalasanageneraattorissa näyttäminen ei yleensä ole teknisesti mahdollista. Tunnistuspalvelun arviointiohjeen 211/2019 liitteen C mobiilisovelluskriteeristössä menettely on huomioitu ("binding message").

Esitettävä tieto voi olla muodoltaan monenlaista, merkkijonoja, lauseita, kuvia, QR-koodi. Luettavuus ja ymmärrettävyys on kuitenkin huomioitava, jotta käyttäjä pystyy helposti assosioimaan asiointitapahtuman ja tunnistuspyynnön toisiinsa. [Lisätään informatiivinen viittaus saavutettavuuslain esteettömyysvaatimuksiin]

Säännöksessä ei oteta kantaa siihen, onko velvollisuus tiedon näyttämiselle tunnistusvälityspalvelulla vai tunnistusvälineen tarjoajalla.

Siirtymäaika…ks. säännös 24

4.6.2.2 Säännös 6.2.2 Luottavan osapuolen nimen näyttäminen käyttäjälle (SP-name)

Vaatimus on uusi.

Tieto luottavasta osapuolesta tarkoittaa asiointipalvelua, jolle vahvistus tunnistamisesta ollaan toimittamassa. Määräyksen tarkoitus on, että kun käyttäjälle näytetään sen asiointipalvelun nimi, johon vahvistus tunnistuksesta on pyydetty ja menossa, käyttäjällä on mahdollisuus jättää vahvistamatta mahdollinen väärä tai petollinen tunnistuspyyntö. Tämä vähentää osaltaan riskiä siitä, että käyttäjää johdetaan harhaan siitä, mihin asiointipalveluun hän on tunnistautumassa.

Kuten säännöksessä 6.2.1 määrätty tunnistuspyynnön yksilöintitieto, myös tieto luottavasta osapuolesta on mahdollista näyttää vain sellaisessa tunnistusvälineessä, jossa on näyttö.

Tunnistustapahtumien toteutus ja käyttäjää informoiva taho tunnistusketjussa vaihtelee, joten ei ole tarkoituksenmukaista määritellä sitovasti, näyttääkö tiedon käyttäjälle tunnistusvälityspalvelu vai tunnistusvälineen tarjoaja. Tiedon näyttämisen määrittelyssä on syytä huomioida mahdollisimman kattavasti kaikki vaiheet, joissa tieto on mahdollista esittää käyttäjälle. Olennaisia ovat etenkin ne tunnistusprosessin vaiheet ja käyttöliittymät, joissa käyttäjältä vaaditaan toimenpiteitä, esim. tunnistusmenetelmän valintaikkuna, mahdollinen tunnistusvälityspalvelun esittämä käyttöliittymä, tunnistusvälineen tarjoajan selainkäyttöliittymä tai tunnistussovellus tai muu näyttämisen mahdollistava tunnistusvälineen tai todentamisen osa.

[Lisätään informatiivinen viittaus saavutettavuuslain esteettömyysvaatimuksiin]

Tieto määrätään pakolliseksi attribuutiksi tunnistusvälineen ja tunnistusvälityspalvelun välisessä rajapinnassa säännöksessä 12.1. Tiedon tuottaa tunnistusvälityspalvelu. Attribuutti on ollut määriteltynä rajapintasuosituksiin (*ftn_spname*) jo aikaisemmin vapaaehtoisena, joten valmius voi olla osalla tunnistuspalveluista jo määriteltynä rajapinnoissa.

Siirtymäaika…ks. säännös 24

4.6.2.3 Säännös 6.2.3 Kertakirjautuminen (SSO)

Säännös on uusi.

Kertakirjautumisen tarjoaminen on viraston tulkinnan mukaan tunnistus- ja luottamuspalvelulain valossa mahdollista, kunhan sen turvallisuudesta, luotettavuudesta ja vaatimustenmukaisuudesta vastaa rekisteröity tunnistuspalvelun tarjoaja ja toteutuksen vaatimustenmukaisuus on arvioitu.

Säännöksessä määrätään yleisellä tasolla tunnistusmenetelmän ja todentamisen turvallisuuden hallintaan liittyvistä tekijöistä, jotka koskevat erityisesti kertakirjautumista. Näitä ovat ainakin istuntojen keston hallinta, istuntojen siirtäminen luottavien osapuolten välillä ja istuntojen lopettaminen eli kertauloskirjautuminen.

Säännöksessä 6.2.3 määrätään, että säännöksen 6.2.2 vaatimus luottavan osapuolen nimen näyttämisestä koskee myös niitä erityistilanteita, joissa tunnistuspalvelu tarjoaa useammalle kuin yhdelle luottavalle osapuolelle tunnistusvälineen haltijan tunnistuksen kertakirjautumisella. Kertakirjautumisesta voi käyttää myös termiä federointi.

Käyttäjän kannalta kertakirjautumisessa on kysymys siitä, että hän siirtyy asioidessaan luottavan osapuolen asiointipalvelusta toisen luottavan osapuolen asiointipalveluun tunnistautumatta uudestaan eli todentamatta uudestaan olevansa vahvan sähköisen tunnistusvälineen oikea haltija. Säännöksen 6.2.3 mukaan käyttäjälle on annettava siirtymisen yhteydessä tieto siitä, että hän on siirtymässä toiseen palveluun ja annettava tieto kyseisen palvelun nimestä, kuten säännöksessä 6.2.2 edellytetään. Käyttäjällä on oltava mahdollisuus hyväksyä tai hylätä siirtyminen. Huom. säännös 12.1 4) koskee siten vain ensimmäistä luottavaa osapuolta. Lokitiedot kertakirjautumisella toteutetuista istunnoista on tallennettava.

Säännöksessä ei otetaan kantaa siihen, näyttääkö tiedon käyttäjälle tunnistusvälityspalvelu vai tunnistusvälineen tarjoaja.

Sen sijaan virasto arvioi, että säännöksen 6.2.1 tunnistustapahtuman/asiointitapahtuman tiedon (istuntotunniste, *session binding*) näyttäminen ei ole teknisesti mahdollista kaikissa kertakirjautumiseen liitetyissä istunnoissa, joten sitä ei edellytetä muissa kuin kertakirjautumisen ensimmäisessä vaiheessa eli todentamisessa.

Muut ohjauskeinot

Kertakirjautumiseen on liittynyt paljon oikeudellisia tulkintakysymyksiä ja tekniseen toteuttamiseen ja turvallisuuteen liittyvää tiedonvaihtoa. Virasto on antanut asiassa neuvontaa tulkinnoista ja teknisiä seikkoja on työstetty yhdessä tunnistuspalveluiden kanssa. Tämä työ jatkuu ja virasto harkitsee työn edetessä tarkoituksenmukaiset ohjauskeinot. Tunnistuspalveluiden eriävien näkemysten takia lähinnä viraston *ohje, suositus tai tulkintalinjaukset* näyttävät tarkoituksenmukaisilta.

4.6.3 Säännös 6.3 Tunnistusvälineen kytkeminen henkilöön

Säännös 6.3.1 on selvyyden vuoksi määräykseen lisätty perusvaatimus, että todentamistekijät on kytkettävä tunnistusjärjestelmässä tunnistusvälineen haltijaan.

Kytkeminen on luonnollisesti erilaista eri todentamistekijöillä, esim. PIN-koodien ja biometristen tekijöiden käsittely eroaa sovelluksen tai tunnuslukulaitteen kytkemisestä.

Säännös 6.3.2 vastaa vuoden 2016 määräyksen 6 §:n vaatimusta, jolla tarkennetaan eräitä tunnistusvälineen luomiseen ja myöntämiseen liittyviä yksityiskohtia, joihin on liittynyt soveltamiskysymyksiä. Ne koskevat yksittäisiä, lähinnä tunnistusvälineen myöntämiseen liittyviä menettelyjä, joilla turvataan sitä, että väline on ainoastaan sen oikean haltijan käytettävissä. Vastaavat vaatimukset ovat olleet voimassa jo ennen vuotta 2016 myös aikaisemmassa määräyksessä 8, mutta vaatimusta on vuonna 2016 joustavoitettu aikaisempaan nähden siten, että se sallii erilaiset prosessit tunnistusvälineen myöntämisessä.

Säännöksen 6.3.2 vaatimus tarkoittaa sitä, että tunnistusvälineitä ei voida lähtökohtaisesti luoda ikään kuin varastoon odottamaan mahdollisia asiakkaita siten, että

henkilötiedot on liitetty tunnistusvälineeseen. Ensitunnistaminen täytyy siis lähtökohtaisesti tehdä ennen kuin henkilötiedot yhdistetään tunnistusvälineeseen.

Säännöksellä 6.3.2 mahdollistetaan myös sellainen prosessi, jossa henkilötiedot yhdistetään haettuun välineeseen jo ennen kuin tunnistus- ja luottamuspalvelulain 17 §:n mukainen ensitunnistaminen tehdään. Tälle voi olla tarvetta esimerkiksi, jos ensitunnistaminen tehdään henkilökohtaisella käynnillä ja halutaan järjestää myöntämisprosessi yhdellä käynnillä. Tällaisia tarpeita on perustellusti esimerkiksi Digi- ja väestötietoviraston ulkomailla oleville henkilöille myöntämien tunnistusvarmenteiden tuottamisessa.

Jos henkilötiedot yhdistetään tunnistusvälineeseen ennen ensitunnistamista, on muussa haku- ja myöntämisprosessissa käytettävä sellaisia turvatoimenpiteitä, että riski virheellisesti luoduista (väärillä henkilötiedoilla tai ilman aikomusta hakea tunnistusvälinettä) tunnistusvälineistä ja riski tunnistusvälineen päätymisestä käyttöön ennen ensitunnistamista on huomioitu. Näitä riskejä voi vähentää esimerkiksi tekemällä VTJ-tarkistuksen ennen henkilötietojen yhdistämistä välineeseen, estämällä teknisesti tunnistusvälineiden käytön ennen ensitunnistamista ja tarkistamalla, että haetut ja tilatut tunnistusvälineet vastaavat toimitettuja tunnistusvälineitä.

Liikenne- ja viestintävirasto suosittelee ensisijaisena suojakeinona sitä, että estetään tunnistusvälineen käyttö teknisesti esimerkiksi sulkulistan avulla, kunnes sen myöntämisen ja toimittamisen edellytykset on kokonaan täytetty. Peruutettua varmennetta ei saa säädännön perusteella palauttaa käyttöön, mutta tämä kielto ei estä järjestelyä, jossa vasta vireillä oleva varmenteen käyttö on teknisesti estetty ja varmenne aktivoidaan käyttöön hakijan ensitunnistamisen jälkeen.

Tunnistusvälineen luovuttamisesta hakijalle säädetään tarkemmin tunnistus- ja luottamuspalvelulain 21 §:ssä. EU:n varmuustasoasetuksen kohdan 2.2.2. mukaan korkean varmuustason tunnistusvälineiltä edellytetään lisäksi erillistä aktivointiprosessia.

Lisäksi prosessissa täytyy luonnollisesti pitää huolta siitä, että ensitunnistaminen liittyy tunnistusvälineen myöntämiseen ja käyttäjä on tästä tietoinen. Samassa yhteydessä voidaan toki tarjota muitakin palveluita kuten matkaviestinliittymä tai pankkipalveluita ja tunnistaa henkilö myös niitä varten.

Tunnistusvälineen myöntämisen yhteydessä ja kytkettäessä välinettä henkilöön on suositeltavaa pyrkiä hallitsemaan riskiä luvattomasta kytkemisestä esimerkiksi tiedottamalla käyttäjää toisen kanavan kautta ja käyttämällä varmistettuja yhteystietoja.

4.6.4 Säännös 6.4 Tunnistusmenetelmän haltijakohtaisten tietojen käsittely

Vaatimuksilla tarkennetaan eräitä tunnistusvälineen luomiseen ja myöntämiseen liittyviä yksityiskohtia, joihin on liittynyt soveltamiskysymyksiä. Ne koskevat yksittäisiä, lähinnä tunnistusvälineen myöntämiseen liittyviä menettelyjä, joilla turvataan sitä, että väline on ainoastaan sen oikean haltijan käytettävissä. Tunnistusmenetelmän ja -järjestelmän turvallisuudesta säädetään tunnistus- ja luottamuspalvelulain 8 ja 8 a §:issä.

Säännöksessä tarkoitettuja salaisia tietoja ovat ainakin tunnistusvälineeseen liittyvä yksityinen avain ja sen käyttöön tarvittava PIN-koodi, salasana tai biometrisen todentamistekijän template.

Säännöksen 6.4.1 mukaan on varmistettava, etteivät tunnistusvälineeseen liittyvät salaiset tiedot paljastu tunnistuspalvelun tarjoajan henkilöstölle missään tilanteessa. Vaatimus on ollut voimassa jo ennen vuotta 2016 annetussa määräyksessä.

Virasto katsoo, että vaatimus on syytä säilyttää, sillä myöntämiskäytännössä tulee edelleen aika ajoin valvonnassa vastaan tilanteita, joissa salaiset tiedot kuten PIN-koodi voivat myöntämisprosessissa tulla palveluntarjoajan henkilökunnan tietoon.

Säännöksen 6.4.2 vaatimuksella turvataan sitä, että salaiset tiedot ovat ainoastaan tunnistusvälineen hakijan (haltijan) tiedossa tai käytettävissä. Tällä varmistetaan se, ettei kukaan muu voi käyttää tunnistusvälinettä.

Vaatimus tarkoittaa käytännössä sitä, että esimerkiksi tunnistusvälineeseen liittyvä PIN-koodi ei saa paljastua missään vaiheessa rekisteröintipisteen henkilöstölle, eikä sitä voi välittää sellaisten tietojärjestelmien kautta, joihin siitä jää kopio, kuten sähköpostitse.

Vrt. sähköisen tunnistamisen varmuustasoasetus

> 2.2.1/ *2. Sähköisen tunnistamisen menetelmä on suunniteltu siten, että sitä voidaan olettaa käytettävän vain, jos se on sen henkilön hallinnassa tai hallussa, jolle se kuuluu.*
>
> 2.3.1/2. *Jos henkilön tunnistetiedot tallennetaan osana todentamismekanismia, nämä tiedot on suojattu niiden menetykseltä ja vaarantamiselta, mukaan lukien analyysi verkkoympäristön ulkopuolella.*
>
> 2.4.6/ *3. Pääsy arkaluonteiseen salaustekniseen aineistoon, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, rajoitetaan tiukasti niihin tehtäviin ja sovelluksiin, jotka edellyttävät tällaista pääsyä. On varmistettava, ettei tällaista aineistoa koskaan tallenneta pysyväisluonteisesti ilmitekstinä. ...Arkaluonteinen salaustekninen aineisto, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, on suojattu luvattomalta käsittelyltä*.

4.6.5 Harkitut sääntelyvaihtoehdot, säännös 6.1 tunnistusmenetelmän turvallisuusvaatimukset

Säännöksen 6.1 valmistelussa on pohdittu, miten määritellään turvalliset tai turvattomat todentamistekijät ja tunnistusmenetelmän kokonaisuus. Vaihtoehtoja on harkittu ja arvioitu seuraavasti:

a) Määräyksessä tarkennettaisiin todentamistekijäkohtaiset vaatimukset

Hallussapitoon, tietoon tai biometriseen ominaisuuteen liittyvät mahdolliset todentamistekijät ovat hyvin erilaisia ja niitä on paljon. Vertailun vuoksi PSD2-sääntelyssä on säädetty tarkennetut vaatimukset kullekin päätyypille, esimerkiksi hallussapitoon perustuva tekijän suojaaminen kopioinnilta.

Tällaiseen sääntelytapaan liittyisi todentamistekijöiden moninaisuuden ja kehittymisen takia paljon yksityiskohtia, joita ei ole mahdollista eikä tarkoituksenmukaista pyrkiä kattamaan säännöstasolla. Myöskään uhkat tunnistusmenetelmän turvallisuudelle ja turvakeinot uhkilta suojaamiselle eivät ole puhtaasti todentamistekijätyyppikohtaisia.

Esimerkkinä tästä sääntelytavasta olisi määrätä hallussapitoon perustuvan todentamistekijän kopioitavuuden estovaatimus ja vaatimus siitä, että hallussapitoon perustuvan todentamistekijän on perustuttava kryptografiseen salaisuuteen. Tällöin olisi selvää, että paperinen tunnuslukulista ei täyttäisi vaatimuksia, ja määräyksessä olisi harkittava myös siirtymäaika paperisen tunnuslukulistan käytön lopettamiselle tai vahvistamiselle kopioinnilta suojaavalla lisätekijällä, joka perustuu kryptografiseen salaisuuteen.

Sidosryhmävalmistelun perusteella osa tunnistuspalveluista aikoo edelleen käyttää paperisia tunnuslukulistoja osana tunnistusmenetelmää, vaikkakin niiden käyttö on korvautumassa mobiilisovelluksilla ja tunnuslukulaitteilla. Valmistelussa on nostettu esille se, että esimerkiksi SMS-vahvistuksen lisääminen tunnistustapahtumaan aiheuttaa kustannuksia, mitä on kritisoitu suhteessa tunnistustapahtumille luottamusverkostossa säädettyyn enimmäishintaan tunnistusvälineen ja tunnistusvälityspalvelun välillä. Liikenne- ja viestintävirasto ei ole kartoittanut tekstiviestipalveluiden hintoja tunnistuspalveluille.

b) Määräyksessä tarkennettaisiin tunnistusmenetelmän suojautumiskyvyn vaatimukset

Korotetun ja korkean varmuustason tunnistusmenetelmän todentamismekanismin hyökkäyksensietokyky kohtuullisen tai korkean asteen hyökkäyspotentiaalia vastaan säädetään tunnistuslaissa ja sähköisen tunnistamisen varmuustasoasetuksessa. Varmuustasoasetuksessa mainitaan myös säännöksen tasolla uhkatyyppejä.

Suojautumiskyvykkyys kohtuullisen tai korkean tason hyökkäyspotentiaalia vastaan on kokonaisuus, joka perustuu todentamistekijöiden eri turvaominaisuuksien ja tunnistusmenetelmän turvallisuustoimenpiteiden yhdistelmään ja muuttuvien uhkien jatkuvaan seurantaan.

Suojautumiskyvyn mittareita tai muunlaisia tarkennuksia määräyksessä voisi ajatella määriteltäväksi viittauksella johonkin yleisesti käytettyyn riskiarviostandardiin. Varmuustasoasetuksen soveltamisohjeessa mainitaan hyökkäyksen vakavuusasteen arvioinnin referenssinä *ISO/IEC 15408 "Information technology – Security techniques – Evaluation criteria for IT security"* ja *ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation"*.

Virasto katsoo, ettei standardien soveltuvuudesta kaikkiin tunnistusmenetelmiin ole riittävästi tietoa, jotta niihin olisi perusteltua viitata määräyksessä velvoittavana.

Sen sijaan virasto katsoo, että suojautumiskyvyn vaatimusta voidaan tarkentaa määräyksessä listaamalla osatekijöitä, joita arvioinnissa on huomioitava.

c) Määräyksessä tarkennetaan tunnistusmenetelmän uhka- ja riskiarvion vaatimukset

EU:n varmuustasoasetuksen soveltamisohjeessa todetaan, että eri tekijät on valittava niin, että niillä torjutaan eri uhkia/hyökkäystapoja ja että on syytä ottaa huomioon paitsi itse tekijät, myös tekijöiden varmentamisessa käytettävä menettely. Soveltamisohjeessa on myös edellisessä kohdassa mainitut standardiviittaukset.

Tässä sääntelymallissa tarkennetaan riskiarvion tekemisen vaatimusta ja osatekijöitä, jotka siinä on otettava huomioon. Todentamistekijöiden ja todentamismekanismin riskit on arvioitava erikseen ja tunnistusmenetelmän suojautumiskyvyn on perustuttava varmuustason mukaiseen uhka- ja riskiarvioon.

Virasto arvioi, että tällainen malli on tarpeeksi joustava eri tunnistusmenetelmien ja todentamistekijöiden suhteen ja huomioi tunnistusmenetelmän turvakontrollit kokonaisuutena. Viraston mahdolliset valvontaratkaisut tulisivat perustumaan tunnistuspalvelun tarkkaan riskiarvioon, jossa huomioidaan myös turvakontrollien vaikutus.

Ensimmäisessä kuulemisessa työpajassa 10.3.2021 toimijat pitivät mallia hyvänä. Soveltamisohjeeseen ehdotettiin lisättäväksi tarkennuksia jonkin yleisesti käytetyn riskiarviostandardin perusteella, jotta vaatimuksenmukaisuuden arviointi olisi mah-

dollista. Lisäksi tuotiin esille, että esimerkiksi kalastelulta suojaavat keinot voivat vähentää käyttäjän käyttömukavuutta ja että keinojen käyttöönotto tulisi tehdä kaikissa tunnistusvälineissä, jotta kilpailu on tasapuolista. Edelleen tuotiin esille, että riskit vaihtelevat tunnistusvälineen tarjoajan käyttäjämäärän perusteella ja hyökkäys suuren palveluntarjoajan käyttäjiin ja menetelmään on rikollisille houkuttelevampaa. Virasto katsoo, että luottamusverkoston yhteistoimintaryhmän tiedonvaihdossa voidaan tunnistuslain 16 §:n perusteella käsitellä yhteisiä tietoturvallisuusuhkia. Tunnistuslain 12 a §:ssä säädetään luottamusverkostossa kielto käyttää kilpailijoista saatuja tietoja muuhun kuin siihen tarkoitukseen, jota varten ne on tunnistuspalvelun tarjoajalle annettu.

4.6.6 Säännös 6 ja Tunnistuslain/eIDAS-asetuksen ja PSD2-sääntelyn yhteensopivuus

Pankki- ja maksupalveluissa käytettävää vahvaa tunnistusta säännellään PSD2-direktiivissä ja sen nojalla annetussa komission täytäntöönpanosäädöksessä. Kansallisesti maksupalveluista säädetään maksupalvelulaissa.

eIDAS-asetuksen ja tunnistuslain sääntely on toimialariippumatonta eli neutraalia sen suhteen, millä toimialalla ja missä palvelussa tunnistusta käytetään.

Monia tunnistuslain mukaan rekisteröityjä vahvoja sähköisiä tunnistusmenetelmiä käytetään Suomessa myös maksupalvelusääntelyn mukaisena vahvana tunnistamisena. Siitä seuraa kysymys, ovatko sääntelyjen vaatimukset ristiriitaisia ja voiko samaa tunnistusmenetelmää tarjota sekä toimialariippumattomassa tunnistamisessa että erityisesti säännellyssä maksupalvelutoiminnassa.

Vuonna 2018 Liikenne- ja viestintävirasto (tuolloin Viestintävirasto) ja Finanssivalvonta tarkastelivat 2018 sääntelyjen teknistä yhteensopivuutta ja pyysivät arviosta lausuntoja toimialalta Finanssivalvonnan PSD2-yhteistyöryhmältä ja Viestintäviraston eIDAS-työryhmältä. **Arvion ja lausuntojen perusteella saman tunnistusmenetelmän käyttämiselle molempien sääntelyjen puitteissa ei havaittu 2018 esteitä, kunhan yksittäisistä vaatimuksista noudatetaan aina tiukempaa tai tarkempaa.**

Vuoden 2018 yhteistarkastelun jälkeen Finanssivalvonta on linjannut, että painetut tunnuslukulistat eivät täytä maksupalvelusääntelyn vaatimuksia ilman jotain lisävahvistustekijää. Maksupalveluissa tunnistusmenetelmiin, joissa on yhtenä todentamistekijänä painettu tunnuslukulista, on lisättävä jokin tekijä tunnuslukulistan (ja haltijan tietoon tai ominaisuuteen perustuvan tekijän) lisäksi. Tyypillisesti pankit käyttävät tunnuslukulistan lisävahvistuksena tekstiviestiä eli käyttäjän on osoitettava sekä tunnuslukulistan että puhelinliittymän hallussapito.

2020 Liikenne- ja viestintävirasto kokosi määräyksen muutostarpeiden ennakkokyselyä varten virkatyönä vertailutietoa sähköisen tunnistamisen varmuustasoasetuksen soveltamisesta ja maksupalvelusääntelyn soveltamisesta ja soveltamisohjeista sääntelyjen erojen tunnistamiseksi ja erojen vaikutusten arvioimiseksi. **Vertailussa tai toimialapalautteessa 2020-2021 ei noussut esille uusia havaintoja tai muita olennaisia eroja kuin painetun tunnuslukulistan arviointi.**

4.7 Säännös 7 Tunnistusjärjestelmän rajapintojen salausvaatimukset

4.7.1 Säännös 7.1 Tietoliikenteen salausmenetelmät

Säännöksessä 7.1 määrätään tietoliikenteen salauksesta. Tarkoitus on varmistaa tunnistustapahtumien eheys ja luottamuksellisuus tietoliikennetasolla.

Vaatimuksia on sovellettava tunnistuspalveluntarjoajien välillä sekä tunnistuspalvelun tarjoajien ja luottavien osapuolten eli asiointipalveluiden välillä. Vaatimukset koskevat tietoliikennettä erityisesti silloin kun tietoliikenne kulkee suojatun fyysisen tilan ulkopuolella ja ei-luotetussa verkossa. Ei-luotetulla verkolla tarkoitetaan internetiä tai toimistoverkkoa tai muuta verkkoa, jonka tietoturvallisuutta ei ole kattavasti arvioitu. Vaatimuksia sovelletaan myös, kun tietoa siirretään alihankkijalle.

Säännöksessä luetellut algoritmit, arvot ja menetelmät koskevat pakottavasti säännöksen käyttötarkoitusta *"Salauksessa, avaintenvaihdossa sekä salaukseen liittyvässä allekirjoituksessa…".* Siten esimerkiksi sinänsä heikoksi todetun SHA-1 -algoritmin tietyille käyttötapauksille ei ole vielä löydetty sellaista hyökkäystä, joka estäisi sen käytön kyseisissä käyttötapauksissa. Algoritmin käyttöä ei suositella mm. koska soveltajan voi olla vaikea arvioida mahdollisesti turvalliset käyttötapaukset. Tunnistuspalveluissa sitä on käytetty esimerkiksi satunnaisuuden luomiseen, mutta olisi hyvä luopua käytöstä, ellei se ole tarkan arvion perusteella turvallista ja välttämätöntä.

Säännöksen 7.1.1 alakohdat 1-4 ja niiden järjestys perustuvat tyypilliseen kryptografian suunnittelujärjestykseen ja vaatimuksiin.

Johdantovirkkeeseen on lisätty selvyyden vuoksi sana varmenne, koska se on käytännössä välttämätön osa tietoliikennesalausta.

Turvallisten menettelyjen, algoritmien ja arvojen määrittelyssä on käytetty pääasiallisena lähteenä Liikenne- ja viestintävirastossa toimivan NCSA:n salaustuotteiden hyväksyntäviranomaisen CAA:n ohjetta salaustuoteratkaisujen turvallisuuden arviointia varten niissä tilanteissa, joissa tietoa siirretään ei-luotetussa verkossa. [Viite X, xxx]

Tavoitteena on 112 bitin vahvuustaso.

NCSA (National Communications Security Authority) vastaa turvaluokitellun aineiston sähköiseen tiedonsiirtoon ja -käsittelyyn liittyvistä turvallisuusasioista. NCSA-toiminto toimii kansallisena salaustuotteiden hyväksyntäviranomaisena (*CAA, Crypto Approval Authority*). CAA-viranomaisen tehtäviin kuuluu turvaluokiteltua tietoa suojaamaan tarkoitettujen salaustuotteiden arvioinnit ja hyväksynnät. Tehtävä perustuu EU:n neuvoston turvallisuussäännöstöön (2013/488/EU) ja lakiin kansainvälisistä tietoturvallisuusvelvoitteista (588/2004).

Määräyksessä 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)
EdDSA = Edwards-curve Digital Signature Algorithm (allekirjoitusmenetelmä)
RSA = Rivest-Shamir-Adleman (epäsymmetrinen salaus- ja allekirjoitusmenetelmä)
SHA = Secure Hash Algorithm (tiivistefunktio)
TLS = Transport Layer Security (salausprotokolla)

7.1.1 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.

https://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml
Transform Type 4 - Diffie-Hellman Group Transform IDs [Viite X, xxx]

7.1.1 2) alakohdassa perusteena on se, että RSA on NCSA:n arvioima ja suosittelema standardi ja ECDSA ja EdDSA tarjoavat vastaavan luotettavuustason. Muita vaihtoehtoja ei viraston arvion mukaan käytännössä ole tarjolla. Kohtaan lisätään EdDSA. Kohtaan lisätään soveltuminen epäsymmetriseen salaukseen, koska käytettäessä RSA:ta määräyksen 9 kohdan mukaiseen sanomien salaamiseen on kysymys epäsymmetrisestä salauksesta.

7.1.1 3) alakohtaan on lisätty salausalgoritmi ChaCha20. Alakohtaan on lisätty myös salausmoodi CCM. Salausmoodi CBC säilytetään määräyksessä. Joissakin arviointityökaluissa se esitetään vanhentuneena, mutta virasto katsoo, että se on riittävän turvallinen, kunhan käytetään oikeita määrittelyjä ja päivitettyjä kirjastoja. On syytä huomata, että 3DES on poistettu suosituksista jo vuonna 2016. Alakohdasta poistetaan salausmoodi XTS, sillä se ei sovellu tietoliikennesalaukseen vaan levysalaukseen.

7.1.1 4) alakohtaan lisätään autentikaatiokoodi Poly1305. Virasto arvioi, että ChaCha20+Poly1305 - yhdistelmä voidaan katsoa riittävän turvalliseksi tunnistustoiminnan yhteydessä, vaikka NCSA-FI tai SOGIS MRA eivät ole vielä vahvistaneet POLY1305:ttä niihin tarkoituksiin, joihin kyseisiä referenssejä käytetään. Yhdistelmän salliminen mahdollistaa nykyistä laajemmin tunnistuspalveluille erilaisten ICT-palveluiden ja niissä tarjolla olevien uusimpien ratkaisujen käytön.

SHA-2 funktioilla tarkoitetaan funktioita SHA-224, SHA-256, SHA-384 ja SHA-512. SHA-3 funktioilla tarkoitetaan funktioita SHA3-224, SHA3-256, SHA3-384, SHA3-512. Tämä tarkennus siirretään määräyksestä perusteluihin.

7.1.2 Kohta on uusi.

Sen mukaan 7.1.1 1-4 kohdissa lueteltujen algoritmien ja menetelmien lisäksi voidaan käyttää NCSA:n tai SOGIS MRA:n turvallisiksi arvioimia algoritmeja ja arvoja, jotka ilmenevät määräyksessä viitatuista lähteistä. Lähteistä on käytettävä ajantasaista tuoreinta asiakirjaa. Virasto pitää NCSA:n listaa soveltuvana lähteenä, ja sitä on muutoinkin käytetty perustana ja vertailukohtana määräystä annettaessa. Toisena ajantasaisena ja relevanttina lähteenä virasto pitää SOGIS MRA:n ylläpitämää listaa.

Lisäyksen tarkoitus on mahdollistaa luotettavien menettelyjen käyttö tilanteessa, jossa määräykseen ei ehditä tehdä muutoksia riittävän nopeasti.

Vaihtoehtoiset sääntelytavat, 7.1 tietoliikenteen salaus. Virasto on arvioinut kohdan 7.1 valmistelussa toimialapalautteessa ehdotettua vaihtoehtoa, että määräyksen luettelo korvattaisiin kokonaan viittauksella NCSA:n ohjeeseen. Virasto katsoo ensinnäkin myös valvontakokemuksen perusteella, että vähimmäisvaatimukset on tarpeellista määrätä yksiselitteisesti. Toiseksi virasto arvioi, että NCSA:n ja SOGIS MRA:n listoja ylläpidetään eri tarkoitukseen ja ne voivat joltain osin olla tarpeettoman tiukkoja korotetun varmuustason tunnistamisen vaatimuksiin nähden. Määräyksen vaatimuksissa on tarpeen huomioida tunnistuspalveluiden turvallisuuden vaatimustaso eikä sidota vaatimuksia kansallisen tai kansainvälisen turvaluokitellun tiedon vaatimustasoon.

Säännöksen 7.1.3 vaatimus salausasetusten teknisestä pakottamisesta tarkoittaa sitä, että järjestelmiä konfiguroitaessa ei saa sallia heikompia oletusarvoja tai sallia sitä, että järjestelmä voisi ohittaa vaatimukset. Vaatimusta ei muuteta.

Ohjelmistojen ja laitteiden oletustoiminnot perustuvat usein toimivuuden tukemiseen joustavasti mahdollisimman monilla vaihtoehtoisilla määrityksillä, mutta tunnistusjärjestelmän salauksissa asetuksissa on estettävä heikompi salaus.

4.7.2 Säännös 7.2. Tietoliikenteen salausprotokolla (TLS)

Säännöksessä 7.2 määrätään tietoliikenteen salausprotokollasta. Kohdassa tarkennetaan vaatimus vain TLS-protokollalle, sillä se on käytännössä vallitseva.

TLS-vähimmäistaso nostetaan versioon TLS 1.2.

Vuoden 2016 määräyksessä sallittua TLS 1.1 -poikkeusta ei enää jatkossa sallita. TLS 1.1 on vuodelta 2006 ja siinä on tiedossa haavoittuvuuksia.

Tietoliikenneyhteyksien TLS-protokollan versio vaikuttaa siihen, kuinka vanhoja päätelaitteita tai selaimia käyttäjät voivat käyttää. Virasto arvioi mm. toimijoiden palautteen perusteella, että käyttäjien päätelaitekanta tukee hyvin kattavasti vähintään TLS 1.2 -versiota. Käytössä on jo myös versio TLS 1.3.

Virasto arvioi sidosryhmäpalautteen perusteella, että siirtymäaikaa vaatimukselle ei tarvita. TLS-version päivittäminen on osa tavanomaista teknistä kehittämistä. Tunnistuspalveluiden tarjonnan ja tasapuolisen kilpailun kannalta on edellisestä sääntelymuutoksesta eli TLS 1.0 kieltämisestä saadun kokemuksen perusteella hyvä, että kaikilla on velvollisuus tehdä muutos samaan aikaan.

Jos tunnistuspalvelu käyttää tietoliikenteen eheyden ja luottamuksellisuuden varmistamiseen muuta kuin TLS-protokollaa (esimerkiksi IPSec tai SSH), toteutuksen on tarjottava vastaava kryptografinen vahvuustaso. Virasto arvioi, että muiden yhteyskäytäntöjen kuin TLS määrittelylle ei edelleenkään ole tarvetta määräyksessä.

4.7.3 Suositus 7.1 kohdan tiukennuksista korkean varmuustason tunnistuspalvelussa

Vuoden 2016 määräyksen perustelujen suositus 7 § 1 momentin eli muutetun määräyksen 7.1 kohdan soveltamisesta päivitetään. Suosituksessa jätetään pois eräitä määräyksessä lueteltuja kevyimpiä menettelyjä ja arvoja. Suositus vastaa saaustuotteiden hyväksyntäviranomaisen CAA:n arviointiohjeen määrittelyä turvaluokalle TL IV.

Vaihtoehtoiset sääntelytavat, 7.1 korkealla varmuustasolla. Valmistelussa on harkittu, säilytetäänkö suositus perusteluissa vai siirretäänkö se pakottavana määräykseen korkean varmuustason vaatimuksena. Virasto arvioi, että korkean varmuustason suosituksen arvojen muuttaminen pakolliseksi ei aiheuttaisi yhteentoimivuusongelmia, koska tunnistusvälityksessä on teknisesti mahdollista valita algoritmit tapahtumakohtaisesti. Virasto katsoo kuitenkin, että vaikutus korkean varmuustason tunnistusta käyttäviin luottaviin osapuoliin on vaikeampi arvioida.

Suositus

Korkealla varmuustasolla tunnistusjärjestelmässä suositellaan sovellettavaksi määräyksessä 7.1 kohdassa edellytettyjen korotetun varmuustason vaatimusten sijaan seuraavassa esitettyjä suluissa olevia arvoja, **joilla saavutetaan vähintään 128 bitin vahvuustaso:**

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 **4096**) 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 **~~1615~~ - 21**) toteuttavat edellä mainitut edellytykset.*

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

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

4) ***Tiivistefunktiot**: Tiivistefunktion tai autentikaatiokoodin on oltava SHA-2, SHA-3, Whirlpool tai Poly1305.*

   *SHA-2:lla tarkoitetaan funktioita ~~SHA224~~, SHA256, SHA384 ja SHA512 (korkealla varmuustasolla **SHA-3-256, SHA-3-384, SHA-3-512**.*

5) Edellä kohdissa 1-4 mainittujen lisäksi voidaan noudattaa menetelmiä ja arvoja, jotka on arvioitu turvallisiksi mainituissa kohdissa tarkoitettuun käyttöön seuraavissa asiakirjoissa taikka niiden uudemmissa versioissa:

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

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

4.7.4 TLS 1.2 ja TLS 1.3 salausprofiilit

Tässä kohdassa neuvotaan, mitkä ovat 7.1 kohdan vaatimukset täyttäviä ciphersuiteja.

Kaikkia kohdassa 7.1 mainittuja algoritmeja, menetelmiä ja arvoja ei voi käyttää TLS:ssä, mutta luettelosta voidaan poimia yhdistelmät TLS 1.2 ja TLS 1.3 -profiileihin. Jotta salausvaatimukset käytännössä järjestelmässä täyttyvät, on ciphersuiten määrittämisen lisäksi TLS-konfiguraatiossa varmistettava myös mm. DH-parametrien ja epäsymmetristen avainten ja varmenteiden riittävästä vahvuudesta.

Ciphersuitet, joita NCSA käyttää arvioidessaan salaustuotteita (tasolla TL IV)
- DHE-RSA-AES-128-CBC-SHA256

Commented [LA2]: Tarkistetaan vielä

Commented [LA3]: Tarkistetaan vielä

- 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:ssa listatut (https://tools.ietf.org/html/rfc7905)

- ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256
- ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256
- DHE-RSA-WITH-CHACHA20-POLY1305-SHA256

RFC 8446:ssa listatut TLS 1.3 ciphersuitet

- AES-256-GCM-SHA384
- CHACHA20-POLY1305-SHA256
- AES-128-GCM-SHA256
- AES_128_CCM_SHA256

4.7.5 Lähteet kansallisesti tai kansainvälisesti suositelluista salausratkaisuista

- NCSA-toiminnon Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset suojaustasot (ohje 28.11.2018 dnro 190/651/2015)
  - https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf
- 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.
- 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
  - https://datatracker.ietf.org/doc/html/rfc8446
- RFC 7905 ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS)
  - https://tools.ietf.org/html/rfc7905

- 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

- ~~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?~~

Commented [IP4]: Poistetaanko

- -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
- 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 (1.7.2020 dnro 1240/651/2017) https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/NCSA_salausratkaisut.pdf

4.8 Säännös 8 Tietoliikenteen osapuolten varmentaminen

4.8.1 Säännös 8.1 Tietoliikenneyhteyden osapuolten tunnistaminen

Säännöksessä 8 tarkennetaan ja tiukennetaan vuoden 2016 määräyksen 8.2 §:n vaatimusta tietoliikenteen osapuolten tunnistamisesta, ulotetaan vaatimus tunnistuspalvelun ja luottavan osapuolen välille ja tarkennetaan avaintenvaihdon ja päivittämisen perusvaatimukset.

Säännöksessä 8.1 määrätään siitä, miten tietoliikenneyhteyden perustamisessa täytyy varmistua siitä, että liikennöinnin toinen osapuoli on oikea taho. Tietoliikenteen osapuolen varmentaminen on perusluonteinen osa luotettavaa sähköistä tunnistuspalvelua. Sähköisessä tunnistamisessa on huolehdittava siitä, että tietoliikenne ja sanomat ovat aitoja ja pysyvät luottamuksellisina.

Vaatimukset ovat samat luottamusverkoston toimijoiden välillä ja tunnistuspalvelun ja luottavan osapuolen eli asiointipalvelun välillä. Luottavan osapuolen todentaminen on yksi olennainen keino suojata tunnistusvälineen käyttäjää petollisten tunnistuspyyntöjen vahvistamiselta.

Luottamussuhde voidaan perustaa luotettavasti toimitettuihin TLS-varmenteisiin tai sanomien suojaamiseen tarkoitettuihin avaimiin.

Suora kahdenvälinen menettely määräyksessä tarkoittaa sitä, että osapuolen varmenne ja salausavaimet on toimitettava siten, että haltijasta voidaan nimenomaisesti varmistua. Määräyksessä ei oteta tyhjentävästi kantaa menettelyn yksityiskohtiin ja siihen, mikä on riittävä tapa tunnistaa toinen osapuoli. Esimerkiksi vahvan sähköisen tunnistamisen käyttäminen on hyvä käytäntö. Toimijoiden välillä tehdään aina sopimus, joten käytännön toimet on mahdollista yhdistää sopimusprosessiin.

Kahdenvälisen menettelyn vaatimus merkitsee voimassa olevan vaatimuksen tiukentamista. Osapuolen varmentamisessa ei siis voida tukeutua pelkästään protokollissa määriteltyihin peruskäytäntöihin, vaan edellytetään erityisiä menettelyjä varmistamaan tietoliikenteen varmenteen tai avainten kuuluminen tietoliikenteen osapuolelle.

Kahdenvälinen tarkoittaa sitä, että tunnistaminen ei voi perustua pelkästään toisen osapuolen varmenteeseen riippumatta siitä, minkä laatuinen kyseinen varmenne on.

Virasto katsoo, että muutoin varmenne ei sinänsä osoita, että sen varmentama avainpari on oikealla haltijalla. Varmenteen haltijan avaintenhallinnan käytännöt eivät sisälly varmenteen myöntämisen vaatimuksiin.

Virasto arvioi myös, että vaikka varmenteen myöntävä CA ja varmenne olisivat erittäin luotettavia, voi tietoliikenneyhteyden konfiguroinnissa helposti käytännössä jäädä varmistamatta, että kelpuutetaan vain kyseinen varmenne, koska tämä ei ole tyypillinen perustoiminne.

TLS-varmenteen ja siihen liittyvän avaimen tai sanomien suojaamiseen liittyvän avaimen voi kuitenkin toimittaa eIDAS-asetuksen mukaisella hyväksytyllä sähköisellä allekirjoituksella allekirjoitettuna tai hyväksytyllä sähköisellä leimalla leimattuna. Hyväksytty sähköinen allekirjoitus ja leima edellyttävät sertifioidun luontivälineen käyttöä (QSCD) ja tämä turvaa sen, että allekirjoituksen tai leiman luomisessa käytettävät avaimet ovat oikean henkilön hallinnassa.

Ks. eIDAS-asetus

> Art. 35.2: *2. Hyväksyttyyn sähköiseen leimaan liitetään olettama tietojen eheydestä ja niiden tietojen alkuperän oikeellisuudesta, joihin hyväksytty sähköinen leima on liitetty.*
>
> Art. 25.2: *2. Hyväksytyllä sähköisellä allekirjoituksella on oltava samanlaiset oikeusvaikutukset kuin käsin kirjoitetulla allekirjoituksella.*

Vertailun vuoksi virasto toteaa, että TUPAS-käytännön aikana luottamussuhde perustettiin reaalimaailman avaintenvaihdolla. Jos käytäntö nyt tässä kohdin muuttuisi siten, että luotetaan tavanomaisen liikennöintikäytännön mukaisesti varmenteisiin, turvallisuus ei olisi enää samalla riittävällä tasolla. Tässä suhteessa määräyksen vaatimukset eroavat esimerkiksi PSD2-sääntelyn vaatimuksesta maksutoimeksiantopalveluun ja tilitietopalvelun (nk. TPP-toimijat, *Third Party Providers*) varmentamisessa, missä luotetaan eIDAS-asetuksen mukaiseen hyväksyttyyn verkkosivujen todentamisen tai hyväksyttyyn sähköisen leiman varmenteeseen. Lisävaatimuksena PSD2-sääntelyssä kuitenkin on, että kyseiset TPP-toimijat ovat finanssisektorin valvontaviranomaisen valvonnassa ja löytyvät viranomaisen rekisteristä.

Teknisestä soveltamisesta virasto toteaa, että OpenID Connect -protokollaa käytettäessä *jwks_uri -osoite* ei yksistään riitä luotettavaan osapuolen varmentamiseen, vaan on käytettävä myös muita menettelyjä. *Jwks_uri* -osoitteen varmistaminen myöskään kiinteän IP-osoitteen perusteella ei ole riittävä varmistus toisesta osapuolesta. Niin ikään SAML-protokolla käytettäessä on todennettava metadatan allekirjoittaja.

Siirtymäaika…ks. säännös 24

4.8.2 Säännös 8.2 Varmenteiden ja avainten uusiminen

Säännöksessä 8.2 määrätään tietoliikenneyhteyden luottamussuhteen ylläpidosta. Perustamismenettelyssä käyttöön otetut luottamuksellisuuden ja eheyden takaavat avaimet eivät voi olla voimassa pysyvästi, vaan ne on uusittava säännöllisesti.

Määräyksellä tarkennetaan vaatimukset avainten ylläpidolle. Määräyksessä määritellään reunaehdot sille, millä edellytyksillä avainten uusimisessa voidaan hyödyntää automaattisia menettelyjä.

Virasto katsoo, että hyvän tietoturvakäytännön mukainen sykli on uusia avaimet vähintään kahden vuoden välein. Avaimet on luonnollisesti uusittava säännöllisestä syklistä riippumatta, jos niiden luotettavuus on vaarantunut tietoturvauhkan tai poikkeaman takia.

Säännöksen 8.2 a - c alakohdissa määrätään menettelyvaihtoehdot, joilla varmenteiden ja avainten uusiminen voidaan katsoa riittävän luotettavaksi. Näillä menettelyillä siis luodaan säännöksen 8.1 vaatimuksen täyttäviä luottamusankkureita. Aikaisempia avaimia ja varmenteita toki on tuettava rinnakkain niin kauan kuin uusien avainten ja varmenteiden käyttäminen/käyttöönotto edellyttää.

Uusien varmenteiden ja avainten aitouden ja eheyden varmistamiseksi uusiminen on tehtävä joko:

a) 8.1 kohdan mukaisella menettelyllä,

b) …

c) …

8.2.a) alakohdassa todetaan selvyyden vuoksi sinänsä itsestään selvä vaihtoehto uusia avaimet 8.1 kohdan perustamismenettelyn mukaisesti.

Kohtien b ja c menettelyissä nojataan perustamisvaiheessa rakennettuun luottamukseen.

Uusien varmenteiden ja avainten aitouden ja eheyden varmistamiseksi uusiminen on tehtävä joko:

a) …

b) toimittamalla uudet avaimet tietoliikenneyhteydellä, jonka eheys ja luottamuksellisuus on varmistettu sitomalla osapuolten tietoliikenne kohdan 8.1 mukaisesti toimitettuihin varmenteisiin tai avaimiin, tai

c) …

8.2 b) alakohdan menettely perustuu siihen, että luotetaan perustamismenettelyllä aikaisemmin kahdenvälisellä menettelyllä toimitettuun varmenteeseen ja varmennetaan sillä tietoliikenneyhteys, jolla uudet avaimet toimitetaan. Menettelystä käytettävä tekninen termi on *secure channel, jonka mahdollisia toteutustapoja voivat olla certificate pinning tai key pinning ja mutual TLS (mTLS)*. OSI-mallin kannalta menettely toteutetaan liikennetasolla (transport).

Menettely on sinänsä tavanomainen ja toteutettavissa tietoliikenteessä, mutta se ei ole oletusarvoisesti ja vakiintuneesti käytössä tietoliikenneyhteyksillä. Virasto korostaa, että tekniset konfiguraatiot edellyttävät huolellisuutta, jotta ohjelmistot eivät voi ohittaa tätä kovennusta.

Teknisestä soveltamisesta virasto toteaa, että varmenteen julkinen avain yksilöi haltijan ja kun tietoliikenneyhteys kiinnitetään tähän julkiseen avaimeen, sitominen toteuttaa tietoliikenneyhteyden eheyden ja luottamuksellisuuden. Ei siis ole riittävää, että liikenne sidottaisiin CA:han, vaan se on tehtävä nimenomaiseen varmenteeseen tai julkiseen avaimeen. Tässä tarkoituksessa käytettävän varmenteen salausmateriaalin huolellinen suojaaminen ja uusiminen on tärkeää.

Vaikutus. Viraston käsityksen mukaan c alakohdan mukaisesti varmistettuja tietoliikenneyhteyksiä käytetään jo jossain määrin luottamusverkoston sisällä ja vaihtoehdon voi olettaa olevan tarkoituksenmukaisesti toteuttavissa tunnistuspalveluiden välillä. Tämä vaihtoehto mahdollistaa sanomien suojaamisessa käytettävien avainten uusimisen automatisoinnin.

Luottavien osapuolten tietoliikenteen varmentamisessa *certificate pinning* voi olla epätarkoituksenmukainen. Sen sijaan näissä tapauksissa *key pinning* tai *mTLS* voi olla käyttökelpoinen ja täyttää vaatimukset.

Certificate/key pinning -toteutuksessa asiointipalvelut voivat tyypillisesti käyttää esimerkiksi edullisia Let's Encryptin tyyppisiä DV-varmenteita, jotka vaihdetaan jopa 3 kuukauden välein. Vaikka luottamussuhde perustettaisiin huolellisesti säännöksen 8.1 mukaisesti, varmenteen vaihtuessa on pystyttävä varmistumaan siitä, että uusi varmenne myönnetään samalle avainparille ja aikaisempi avain säilyy käytössä teknisessä määrittelyssä.

Mutual TLS, mTLS -toteutuksessa todennetaan tietoliikenneyhteyden osapuolet käyttämällä palvelinvarmenteen lisäksi asiakasvarmennetta (*client authentication*) tapahtuvalla tunnistuksella. mTLS on vaihtoehtoinen tapa tietoliikenteen osapuolten todentamiselle ja tiedon luottamuksellisuuden ja eheyden turvaamiselle.

Määräyksessä mahdollistettu certificate/key pinning tai mTLS-menettely mahdollistaa automatisoidun prosessin sanomien suojaamisessa käytettävien avainten ylläpidossa (JWK set).

TLS-yhteyden kiinnitys (pinning) ja mTLS eroavat toisistaan hallinnan osalta. Kiinnitetyissä yhteyksissä osapuolet normaalisti hankkivat itse omat varmenteensa, mutta tyypillisesti mTLS-käyttötapauksessa toinen osapuoli toimittaa varmenteen (client certificate) omalle asiakkaalleen.

Uusien varmenteiden ja avainten aitouden ja eheyden varmistamiseksi uusiminen on tehtävä joko:
a) …
b) …
c) allekirjoittamalla uudet avaimet 8.1 kohdan mukaisesti toimitetulla avaimella.

8.2 c) alakohdan menettely perustuu siihen, että luotetaan perustamismenettelyllä aikaisemmin toimitettuun avaimeen ja varmenteeseen. Uusi avain allekirjoitetaan aikaisemmin toimitetulla avaimella. OSI-malliin nähden menettely toteutetaan sovellustasolla.

Vaihtoehto ei ole käytännössä todennäköinen, mutta virasto haluaa sallia sen määräyksessä, jotta ei suljeta pois toteutuksia, jotka voisivat tukeutua tähän.

Teknisestä soveltamisesta virasto toteaa, että säännöksen vaatimus edellyttää, että OpenID Connect -protokollaa käytettäessä jwks-uri -avaimet allekirjoitettaisiin säännöksen 8.1 mukaisesti toimitetulla allekirjoitusavaimella.

Tämä lienee teknisesti mahdollista, mutta standardissa ei kuitenkaan ole valmista määrittelyä tälle menettelylle. Säännöksen 8.2 c) alakohdan valmistelussa virasto on arvioinut erityisesti mahdollisuutta toteuttaa automatisoituja päivityksiä. Tämä menettely olisi esimerkiksi 8.2. c) mukainen uusien uusien jwks-avainten (OpenID Connect -protokollaa käytettäessä) allekirjoittaminen ja salaaminen luotetuilla avaimilla. Tämä ei niinkään ole kovennusvaatimus ohjelmistoihin, vaan edellyttäisi kokonaan uuden toiminnon rakentamista luottavien osapuolten järjestelmiin. Määrittelyyn liittyvät osaset sinänsä olisivat olemassa, mutta yhteensopiva toteutus edellyttäisi koordinointia ja yhteistä kehittämistä.

Viraston käsityksen mukaan uusimista ei siis välttämättä voida toteuttaa automaattisesti siten, että allekirjoituksen varmentaminen sidottaisiin nimenomaisesti säännöksen 8.1 mukaisesti toimitettuun varmenne/avain-kokonaisuuteen. Jos kuitenkin pystytään varmistumaan siitä, että tarkistus sidotaan nimenomaisesti 8.1. toimitettuun varmenteeseen ja avaimeen, menettely voi täyttää 8.2 c alakohdan vaatimuksen. Jos tähän menettelyyn tukeudutaan, on tärkeää, että tämä otetaan huomioon tunnistusvälityspalvelun ja luottavan osapuolen/asiointipalvelun menettelyistä määriteltäessä ja sovittaessa.

On epätodennäköistä, että luottavat osapuolet tekisivät tällaista kehitystyötä määritelläkseen menettelyn, jota ei ole standardissa valmiina eli kehitystyö olisi tehtävä luottamusverkostossa. Jos menettely ei olisi kaikilla standardinmukainen, yhteensopivuus tunnistusvälityspalveluiden ja luottavien osapuolten välillä ei olisi mahdollista. Epäyhteensopivuudet ja virheet aiheuttavaisivat korjaus- ja neuvontaprosessitarvetta.

Virasto arvioi, että ei ole tarkoituksenmukaista lähteä asiasta omaa määrittelyä luottamusverkostolle, koska menettelyyn sisältyy ilmeinen käytännön yhteentoimivuusongelmien riski.

Virasto ei ole tarkistanut, onko SAML - standardissa valmis määrittely metadatan allekirjoittamiselle manuaalisesti toimitetuilla avaimilla.

Yhteenveto säännöksen 8.2 teknisestä soveltamisesta. Virasto arvioi, että ainakin seuraavat standardin mukaiset vaihtoehdot ovat käytettävissä.

- Sanomatason salausvaatimus ja kohdan 8.1 mukainen salausavainten vaihto, jos käytössä on TLS suojattu yhteys, jossa ei ole käytössä certificate tai key pinning.
- Käytössä on päästä päähän suojattu TLS yhteys, jossa 8.1 mukainen certificate pinning (tietty palvelinvarmenne) tai key pinning tai mTLS, tällöin sanomatason salaus ei ole pakollista ja salausavaimen vaihto voidaan automatisoida (JWKS, ja avainrotaatio)
- Sanomatason salausvaatimus on aina voimassa silloin kun tunnistusviestit kierrätetään käyttäjän selaimen tai päätelaitteen kautta (esim. SAML front-channel)

Sanomatason salaus on toki suositeltavaa kaikissa yhteyksissä, joissa se on mahdollista.

Siirtymäaika …ks. säännös 24

4.8.3 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 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.

4.8.4 Säännöksen 8 tavoitteet ja vaikutusarviointi

4.8.4.1 Tavoitteet

Vaatimusten tarkoitus on varmistaa, että tunnistustapahtumat välitetään luottamusverkoston sisällä ja luottamusverkostosta ulos vain luotettavasti varmennetuille organisaatioille. Luottavan osapuolen todentaminen on yksi olennainen keino suojata tunnistusvälineen käyttäjää petollisten tunnistuspyyntöjen vahvistamiselta.

Tarkoitus on myös varmistaa tietoliikenteen ja sanomien eheys ja luottamuksellisuus. Sähköisessä tunnistamisessa on huolehdittava myös siitä, että tietoliikenne ja sanomat ovat aitoja ja pysyvät luottamuksellisina.

Tarkoitus on selkeyttää vaatimukset ja varmistaa turvallisten menettelyjen yhtenäinen käyttö tunnistuspalvelusta riippumatta. Vaatimukset ovat olleet käytännössä epäselviä ja aiheuttaneet paljon tulkintakysymyksiä sekä turvallisuudeltaan vaihtelevia menettelyjä etenkin luottavien osapuolten eli asiointipalveluiden varmentamisessa.

Määräyksen tarkentaminen selkeyttää ja yhdenmukaistaa menettelyjä etenkin luottavien osapuolten kanssa. Virasto arvioi, että vaatimukset voivat kokonaisuutena tiukentaa joidenkin toimijoiden käyttämiä menettelyjä, mutta tavoitteena on varmistaa tunnistamisen turvallisuuden jatkuva kehitys ja varmistaa tasapuolinen kilpailu.

4.8.4.2 Tiukennus peruskäytäntöihin

Tietoliikenteen osapuolen varmentaminen on perusluonteinen osa luotettavaa sähköistä tunnistuspalvelua. Vaatimuksilla saavutetaan parempi turvallisuus kuin protokollien peruskäytännöissä, joissa luotetaan mihin tahansa internetissä yleisesti luotettuihin varmenteisiin.

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 standardeissa olisi teknisesti standardoituja menettelyjä tietoliikenteen käynnistämiseen uuden osapuolen kanssa. Siksi on ollut 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.

Vaatimusten toteuttaminen edellyttää prosessien määrittelyä avainten ja varmenteiden toimittamisessa ja erilaisia asetusten määrittelyjä palvelinohjelmistoissa sekä tunnistuspalveluissa että asiointipalveluissa.

Vaihtoehdon arviointi. Valmistelussa on harkittu vaihtoehtona sitä, että määriteltäisiin varmenteet, joihin voisi luottaa ilman kahdenvälisen toimittamismenettelyn vaatimusta. JA QWAC/QCA eSeal/EV - nämä olisivat kuitenkin kustannustekijä ja epätodennäköistä, että yritykset hankkivat näitä - virasto arvioi, että avaintenhallinta ei silti ole taattu.

Kuten edellä on todettu, virasto katsoo, että muutoin varmenne ei sinänsä kerro, että sen varmentama avainpari on oikealla haltijalla. Varmenteen haltijan avaintenhallinnan käytännöt eivät sisälly varmenteen myöntämisen vaatimuksiin.

Virasto arvioi myös, että vaikka varmenteen myöntävä CA ja varmenne olisivat erittäin luotettavia, voi tietoliikenneyhteyden konfiguroinnissa helposti käytännössä jäädä varmistamatta, että kelpuutetaan vain kyseinen varmenne, koska tämä ei ole tyypillinen perustoiminne.

4.8.4.3 Luottamusverkoston ja luottavien osapuolten ero

Rekisteröityjen tunnistuspalveluiden lukumäärä on rajallinen, kun taas tunnistusta käyttävien asiointipalveluiden määrä on suuri ja kasvaa toivottavasti jatkuvasti. Siksi on ollut 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.

4.8.4.4 Luottamussuhteen perustaminen ja avaimen toimittaminen

Säännöksen 8.1 kahdenvälisen menettelyn vaatimus aiheuttaa muutostarpeita tunnistusvälityspalvelun ja sen asiakkaana olevan sähköistä asiointipalvelua tarjoavan luottavan osapuolen tietoliikenneyhteyden perustamiseen.

Viraston rajapintasuosituksissa 212 ja 213 on ollut hyvänä käytäntönä välttää luottamuksen johtamista internetin/selainten yleisesti luotetuista CA:ista, mutta määräysvalmistelussa on selvinnyt, että luottavien osapuolten varmentaminen tehdään käytännössä usein edellä kuvattuun *jwks-urin* perusteella ja luottavien osapuolten varmenteiden laatu vaihtelee paljon sen suhteen, perustuuko varmenteen haltijan todentaminen tämän omaan ilmoitukseen vai todentaako varmenteen myöntäjä haltijan jotenkin.

Vaatimus vaikuttaa ensinnäkin siihen, miten luottamussuhteen perustamisprosessi toteutetaan. 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.

Jos sopimukseen tekemiseen liittyy käyntiasiointi, samassa yhteydessä on mahdollista vaihtaa tarvittavat avaimet.

Tavallisemmin sopimukset tunnistuspalvelusta luottavan osapuolen kanssa kuitenkin tehtäneen sähköisesti ja tällöin joudutaan määrittelemään tarpeeksi **luotettava sähköinen tapa toimittaa osapuolen julkinen avain**. Määräyksessä on esimerkkinä suoraan eIDAS-asetuksessa luotettavaksi säädetty tapa, mutta muut mahdolliset tavat on harkittava kokonaisuutena, jossa otetaan huomioon riskit siitä, että toimitettu tieto on väärennetty tai tulee väärältä taholta. Siten osana prosessia on tarpeen toisen osapuolen sähköinen tunnistaminen, missä vahva sähköinen tunnistaminen tarjoa paremman luotettavuuden kuin muut tavat. Tiedonvälityskanavan eheys on toinen arvioitava tekijä. On selvää, että pelkän sähköpostin turvallisuus on riittämätön, mutta erilaiset turvapostiratkaisut voivat taata riittävän eheyden ja luottamuksellisuuden, jos ne on toteutettu laadukkaasti siten, että lähettäjä ja vastaanottaja on tunnistettu ja viestintä on salattu. Myös muut osapuolilla käytössä olevat sähköiset asiointiratkaisut kuten pankkipalveluiden turvatut viestipalvelut tai useampien toisistaan riippumattomien kanavien käyttäminen voivat olla käytössä avaimen toimittamisessa.

Tunnistusvälityspalvelun kannalta vaatimukset vaikuttavat siihen, että sen on sopimussuhteissaan luottavien osapuolten kanssa huolehdittava teknisten vaatimusten informoinnista, sillä ei ole todennäköistä, että nämä olisivat niitä tarkkaan selvillä. Tunnistuslain valossa tunnistusvälityspalvelu vastaa siitä, että se toimittaa tunnistuspalvelut luottaville osapuolille vaatimusten mukaisesti. Samoin kuin tietosuojavelvoitteiden osalta on arvioitu (luottavan osapuolen oikeus käsitellä henkilötietoja, jotka sille luovutetaan tai vahvistetaan), vastuu koskee vaatimusten ja mahdollisten virhetilanteiden käsittelyn huomioimista sopimuksessa, eikä aiheuta esimerkiksi velvollisuutta auditoida luottavien osapuolten tietojärjestelmiä. Tunnistusvälityspalvelu voi luonnollisesti halutessaan tarjota myös teknisiä neuvonta-, ylläpito- tai asennuspalveluita.

Sopimussuhteeseen kuuluu myös seuranta luottavien osapuolten avainten voimassaolosta, huolenpito siitä, että niitä uusitaan säännöllisesti ja uusien avainten käyttöönotto tunnistuspalvelun tarjoajan järjestelmässä. Tekniset tarkistukset vähintään kerran kahdessa vuodessa ovat viranomaisen arvion mukaan sinänsä paikallaan ja hyvä käytäntö.

Siirtymäajan tarve vanhoille sopimusasiakkaille. On huomioitava tavanomaiset ICT-hankkeiden syklit ja niiden suunnittelu- ja budjetointi sekä tunnistusvälityspalveluilla että luottavilla osapuolilla. Uusille asiakkaille menettelyt voinee ottaa käyttöön nopeammin.

4.8.4.5 Luottavan osapuolen eli asiointipalvelun järjestelmien koventamisvaatimukset

Luottavien osapuolten tai niiden teknisten alihankkijoiden tietotaito voi myös vaihdella ja siksi on otettava huomioon myös ne tekniset osaamisvaatimukset, joita vaatimuksesta seuraa.

On otettava huomioon tekninen toteutettavuus yleisesti saatavilla olevilla teknisillä ratkaisuilla ja ohjelmistoilla, mahdolliset tavanomaisesta ICT-ylläpidosta poikkeavat kustannukset ja myös erehdysten ja inhimillisten virheiden mahdollisuus, joita koventamiseen liittyy.

On erotettava uuden luottamussuhteen perustaminen ja varmenteiden ja avainten uusiminen sopimussuhteen aikana.

Perustamisvaihe. Luottavan osapuolen on pystyttävä huomioimaan se, että sen toimittama varmenne/julkinen avain on juuri se, jota tullaan käyttämään tunnistusvälityspalvelua käytettäessä joko tietoliikenneyhteyden TLS-salaukseen tai tunnistusvälityspalvelulle lähetettävien tunnistuspyyntöjen allekirjoittamiseen ja salaamiseen sa-

nomatasolla. Julkiseen avaimeen liitetyn yksityisen avaimen käsittelyn luottavan osapuolen järjestelmässä täytyy myös olla siinä määrin huolellista, ettei sitä saa tietoon tai haltuun.

Perustamisvaiheeseen liittyy luottavan osapuolen tietojärjestelmissä myös se kovennusvaatimus, että TLS-yhteyden säännöksen 7 mukainen salaus on konfiguroitava siten, että siinä käytetään vain luotettua avainparia. Tämä edellyttää huolellista, mutta verraten tavanomaista teknistä määrittelyä ohjelmistoissa.

Jos avaimen päivittämisen turvallisuus halutaan perustaa 8.2 b) mukaiseen TLS-yhteyden varmentamiseen, TLS-yhteyden certificate pinning tai key pinning tai mTLS olisi tehtävä nimenomaan avaimeen tai varmenteeseen, ei CA:han. Tämä on koventamisvaatimus luottavalle osapuolelle ohjelmiston määrittelyissä, missä yleensä luotetaan internetin CA:ihin.

Viraston käsityksen mukaan certificate tai key pinning tai mTLS on sinänsä standardien kanssa täysin yhteensopiva menettely. Todennäköisesti tarkoituksenmukainen menettely TLS-yhteyden kiinnittämisessä olisi key pinning, koska se mahdollistaisi tiheät varmenteen vaihdot, mikä on luonteenomaista esim. Let's Encryptin varmenteille.

Nämä alkuvaiheen konfiguroinnit ovat siten olennaisia. Vaikka perustamisvaihe olisi tehty huolellisesti, ilman kovennuksia voi käydä niin, että huolellisesti vaihdettu varmenne vaihdetaan automaattisesti päivityksen yhteydessä tarkistamattomaan varmenteeseen, tai vaadittavia tarkistuksia ei tehdä tietoliikenneyhteyden luomisvaiheessa.

Kovennusvaatimusten tekninen vaativuus ja kustannukset luottaville osapuolille. Edellä mainitut 8.1 ja 8.2 b kohdan menettelyjen kovennustarpeet ovat viraston käsityksen mukaan sinänsä kohtuullisen helposti luottavan osapuolen tehtävissä, mutta ne edellyttävät sitä, että asiaankuuluvat prosessit ja ylläpito/toteutusvastuut huomioidaan luottavan osapuolen teknisessä ylläpidossa ja toki ne edellyttävät jossain määrin syvempää osaamista ohjelmistojen peruskäytön lisäksi. Usein teknisestä toteutuksesta vastaa tekninen ostajahankkija ja tunnistus liittyy johonkin laajempaan ICT-kokonaisuuteen. Muutokset aiheuttavat myös kustannuksia luottaville osapuolille. Osapuolten varmentajainen ja salausavainten hallinta aiheuttavat siis jonkin verran kustannuksia, mutta tätä voitaneen pitää tunnistuspalveluissa perusluonteisena ICT-toteutuksiin liittyvänä kustannuksena.

Viraston arvio on, että muutokset ovat teknisesti toteutettavissa ja tarpeellisia vahvan sähköisen tunnistuksen turvallisuuden jatkuvassa kehittämisessä. Vaatimuksille on kuitenkin tarpeen varata siirtymäaikaa etenkin suhteessa asiointipalveluihin ja muutosten läpivieminen edellyttää yhteistyötä neuvonnassa ja viestinnässä.

4.8.5 Säännös 8, viitteet ja muut lähteet (kesken)

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

- eIDAS Cryptographic Requirements for the Interoperability Framework, version 1.2

4.8.6 Säännös 8.2, teknisen soveltamisen vaihtoehtojen arviointi

Säännöksen 8.2 valmistelussa virasto on arvioinut myös, voisiko DNSSEC:in käyttö turvata tietoliikenneyhteyden luottamuksellisuuden ja OpenID Connect -protokollaa käytettäessä standardin mukaisen JWKS-endpoint -tekijän yhtä luotettavasti kuin liikenteen sitominen luotettuun varmenteeseen. DNSSEC on yleisesti ottaen hyvä ja ehdottomasti suositeltava käytäntö tietoliikenteessä. Tähän tukeutuminen olisi mahdollistanut OpenID Connectia käytettäessä avainten automaattisen uusimisen.

Virasto arvioi kuitenkin, että toteutuksen turvallisuuden edellyttämiä tarkkoja teknisiä määrittelyjä ei voida riittävän luotettavasti varmistaa varsinkaan luottavien osapuolten järjestelmissä. Turvallinen toteutus edellyttäisi, että käytössä olisi oltava DANE ja sovelluksen (clientin) resolverinimipalvelin olisi määriteltävä käyttämään DNSSEC-tekniikkaa hard fail -tilassa. DANEn käytölle ei välttämättä ole laajalti tarjolla ohjelmistotukea. Siten menettelyä EI ole otettu mukaan määräyksen 8.2 kohdan menettelyvaihtoehtoihin. (Kovennetuilla määrittelyillä TLS with DNSSEC, JWT Encryption, Rotation of encryption keys (JWKS))

4.9 Säännös 9 Tunnistussanomien eheys ja luottamuksellisuus

4.9.1 Säännös 9.1 Sanomien suojaaminen tunnistuspalveluiden ja luottavan osapuolen välillä

Säännökseen 9 yhdistetään vuoden 2016 määräyksen 7 ja 9 §:ien vaatimukset tunnistusanomien salaamisesta. Vaatimuksia tarkennetaan ja muutetaan.

Säännöksen 9.1. a) alakohdassa määritellään sanomien salaamisen ja allekirjoittamisen rinnalle vaihtoehtoinen suojaamismenettely. Se perustuu tietoliikenneyhteyden luottamuksellisuuden ja eheyden erityiseen varmistamiseen ja on mahdollinen, jos sanomia ei välitetä käyttäjän selaimen tai päätelaitteen kautta. Tällä lisäyksellä joustavoitetaan vuoden 2016 määräyksen kategorista sanomatason salausvaatimusta.

Säännöksen 9.1 a) alakohdan mukaan tunnistussanomien eheys ja luottamuksellisuus voidaan toteuttaa varmistamalla tietoliikenneyhteyden eheys ja luottamuksellisuus sitomalla osapuolten tietoliikenne molemmissa päissä säännöksen 8 mukaisesti toimitettuihin varmenteisiin. Tällöin pystytään varmistamaan päästä-päähän sekä tietoliikenneyhteyden molempien päiden varmenteen luotettavuus ja se, että liikennettä ei pureta muualla kuin osapuolten tunnistuspalvelun tuottamiseen liittyvissä järjestelmissä.

Menettely ja varmenteen luotettavuuden vaatimukset vastaavat säännöksessä 8 kohdassa määrättyä. Pohjaoletuksena on luonnollisesti, että tietoliikenneyhteys ("TLS-putki") on salattu määräyksen 7 kohdan vaatimusten mukaisesti. Jos tietoliikenneyhteyden suojauksessa ja salaamisessa käytetään TLS-salauksen sijasta IPsec-VPN (virtual private network) -toteutusta, siinä on tehtävä vastaavat sanomien luottamuksellisuutta turvaavat toimenpiteet.

Vaihtoehtojen arviointi. Virasto katsoo, että esimerkiksi MPLS-yhteydet eivät tarjoa riittäviä turvakontrolleja tähän tarkoitukseen, sillä ne eivät oletusarvoisesti tarjoa eheyttä ja luottamuksellisuutta. Ks. Pitukri, kohta SA-02: Internet, sekä operaattorin tarjoamat MPLS-verkot ja esimerkiksi niin sanotut mustat kuidut (dark fiber) tulkitaan julkisiksi verkoiksi.

Henkilötiedot. Henkilötiedoiksi katsotaan yleisen tietosuojasääntelyn kannalta kaikki tiedot, jotka ovat suoraan tai välillisesti yhdistettävissä henkilöön eli myös esim. pseudonyymit tai transaktiotunnisteet, jotka ovat eri lähteistä koottuna/yhdistettynä yhdistettävissä henkilöön. Tunnistamisessa käytetyistä henkilötiedoista henkilötunnusta koskee tietosuojasääntelyssä erityinen suoja. Liikenne- ja viestintävirastolla ei

kuitenkaan ole objektiivista perustetta rajata muitakaan henkilötietoja suojan ulkopuolelle. Siten määräyksessä ei määrätä tunnistussanominen suojaamisvelvoitetta sen perusteella, millainen henkilötieto tunnistussanomassa välitetään ("*on alaikäinen*" vrt. on "*121212+999Å, Alma Virtanen*"). Henkilötietojen luokittelulle olisi vaikea määritellä objektiivisia ja kattavia perusteita ja tekniset toteutukset on yksinkertaisinta tehdä kaikille tunnistustapahtumille samalla tavalla.

4.9.2 Vaikutukset ja toteutettavuus

Tunnistussanomien suojaamisvaatimuksen tarkoitus on, että henkilötiedot eivät paljastu oikeudettomasti käyttäjän päätelaitteen selaimessa tai palvelimilla. 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.

Tunnistussanomien salaus ja allekirjoitus yhdessä säännöksen 8 vaatimusten kanssa suojaa osaltaan myös tunnistustapahtuman väärentämiseltä ja toisintamiselta (tamper/replay). Edelleen suojaamismenettelyllä turvataan osaltaan sitä, että vahvistus autentikoinnista ja henkilötiedot toimitetaan todentamisessa vain oikealle asiointipalvelulle. Siten ei ole perusteita erotella vaatimusta luottamusverkoston sisällä ja luottamusverkoston ja asiointipalveluiden välillä. Vaatimus koskee yhtäläisesti tunnistuspalveluiden välisiä ja tunnistuspalveluiden ja luottavien osapuolten välisiä yhteyksiä.

Määräyksen vaatimus on edelleen teknisesti neutraali, mutta mahdollisuudet toteuttaa muita suojaustapoja voivat vaihdella eri protokollissa (OIDC, SAML, ETSI MSS) ja toteutuksissa. Muutoksen tarkoitus on huomioida paremmin eri protokollien ja standardien ominaisuudet. Muutos lisää teknisen toteutuksen joustavuutta OIDC-toteutuksissa ja mahdollistaa myös nykyisen ETSI MSS-standardia käyttävän mobiilivarmenneratkaisun, jota ei arvioitu riittävästi määräyksen 2016 valmistelussa. SAML-toteutuksissa käytetään käyttäjän selainta, joten niissä on toteutettava aina sanomien salaus. SAML mahdollistaisi myös muunlaiset toteutukset, joita ei kuitenkaan tyypillisesti käytettäne.

4.9.3 Säännös 9.1.2 tunnistussanomien allekirjoitus

Säännös 9.1.2 on uusi.

Säännöksellä 9.1.2 lisätään vaatimus allekirjoittaa tunnistussanomat eli luottavan osapuolen tunnistusvälityspalvelulle tekemät tunnistuspyynnöt ja tunnistusvälityspalvelun luottavalle osapuolelle toimittamat vastausanomat.

Vaatimus koskee vain luottamusverkoston tunnistusvälityspalvelun ja luottavan osapuolen välisiä tunnistussanomia eli tunnistuspyyntöjä ja vastaussanomia. Tarkoitus on todentaa se, että luottavan osapuolen tunnistuspyyntö tulee oikealta järjestelmältä ja todentaa luottavan osapuolen nimen ilmaiseva SPname -attribuutti, joka säännöksen tunnistusvälityspalvelun tarjoajan on säännöksen 12.1 mukaan varmennettava.

Vaatimus koskee siis sovellustasolla myös tilanteita, joissa käytetään kuljetus/liikennetasolla 9.1.a) alakohdan mukaista varmistettua tietoliikenneyhteyttä. Tarkoitus on erityisesti todentaa ne sovellukset, jotka luottavan osapuolen tietojärjestelmistä pyytävät tunnistusta.

Vaatimusta ei määritellä pakolliseksi luottamusverkoston tunnistuspalveluiden välillä, koska niiden järjestelmien tietoturvallisuus on kokonaisuutena arvioitu, mutta se on toki hyvä käytäntö sielläkin.

Vaikutus/toteutettavuus. Luottavan osapuolen tunnistuspyyntöjen allekirjoitus on tullut esille rajapintasuositusten valmistelussa. Se on valmistelussa saadun palautteen perusteella yleisesti toivottu turvallisuutta lisäävä menettely. Menettely on tietoteknisesti tavanomainen.

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

Rajat ylittävän tunnistamisen teknisten vaatimusten määrittelyssä käytetään vain SAML-protokollaa. Määrittelyssä sanomien allekirjoittaminen on määritelty pakolliseksi ja sanoman sisällön allekirjoitus ja salaaminen on valinnaista.

> *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.*

4.9.4 Säännös 9.2 Sanomien salaaminen käyttäjärajapinnassa

Säännöksen 9.2 tarkoitus on selkeyttää sitä, että määräyksen vaatimukset vaikuttavat myös käyttäjän päätelaiterajapintaan.

Jos tunnistussanoman välittämisessä tunnistuspalvelun ja luottavan osapuolen eli asiointipalvelun välillä käytetään käyttäjän selainta, asiointisovellusta tai päätelaitetta muutoin, sanoman salaaminen TLS-yhteyden 7 kohdan mukaisen salaamisen lisäksi on edelleen pakollista.

Käyttäjän selain tai asiointisovellus voi olla sähköisen asiointi- ja tunnistustapahtuman aikana yhteydessä asiointipalveluun, tunnistusvälitykseen ja tunnistusvälineen myöntäjään. Luotettavalla salauksella halutaan suojata henkilötietoja koko prosessissa.

On huomattava, että määräys ei koske luottavan osapuolen eli asiointipalvelun ja käyttäjän välistä rajapintaa muutoin, mutta velvoittaa tunnistusvälineen ja tunnistusvälityspalvelun tarjoajan toteuttamaan tunnistuspalvelunsa siten, että henkilötietojen luottamuksellisuudesta huolehditaan käyttäjän päätelaiterajapinnassa.

4.9.5 Säännös 9.3 Salausalgoritmit ja menettelyt

Säännöksessä 9.3 viitataan säännökseen 7.1, jossa luetellaan turvalliset algoritmit ja menettelyt. Sanomien salaamisessa on käytettävä määrättyjä menettelyjä siltä osin, kun ne soveltuvat teknisesti. Säännöstä 7.1 on muutettu siten, että se soveltuu myös sanomatason salaukseen.

Teknisestä soveltamisesta virasto toteaa, että hyvä vallitseva käytäntö on käyttää RSAES-OAEP:ia.

Tässä ei ole soveltamisesimerkkejä sanomien salaamismenetelmistä, mutta virasto toteaa, että RFC 7519 on tarvittaessa hyvä lähde määrittelyssä.

Viite RFC 7519 https://tools.ietf.org/html/rfc7519

> *Support for encrypted JWTs is OPTIONAL. If an implementation provides encryption capabilities, of the encryption algorithms specified in [JWA https://tools.ietf.org/html/rfc7519#ref-JWA], only "RSAES-PKCS1-v1_5 with 2048-bit keys ("RSA1_5"), AES Key Wrap with 128- and 256-bit keys ("A128KW" and "A256KW"), and the composite authenticated encryption algorithm using AES-CBC and HMAC SHA-2 ("A128CBC-HS256" and "A256CBC-HS512") MUST be implemented by conforming implementations. It is RECOMMENDED that implementations also support using Elliptic Curve Diffie-Hellman Ephemeral Static (ECDH-ES) to agree upon a key used to wrap the Content Encryption Key ("ECDH-ES+A128KW" and "ECDH-ES+A256KW") and AES in Galois/Counter Mode (GCM) with 128- and 256-bit keys ("A128GCM" and "A256GCM"). Support for other algorithms and key sizes is OPTIONAL.*

Viraston OIDC-rajapintasuosituksessa 213 on ennestään seuraavia ohjeita sanomatason salauksesta. Vastaava on suosituksessa 212 SAMLille.

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	OPTIONAL

			and MGF1 with SHA-256	
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**

4.10 Säännös 10 Tietoturvavaatimukset kansallisen solmupisteen rajapinnassa

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

Säännöksessä 10 määrätään siitä, että luottamusverkoston ja kansallisen solmupisteen 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 1.2, 31 August 2019* [viite] *https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20Cryptographic%20Requirement%20v.1.2%20final.pdf?version=2&modificationDate=1571068651805&api=v2*

4.11 Säännös 11 Tunnistuspalveluntarjoajan häiriöilmoitukset Liikenne- ja viestintävirastolle

4.11.1 Säännös 11.1 Merkittävät uhkat tai häiriöt (ilmoituskynnys)

Säännöksellä 11 tarkennetaan tunnistus- ja luottamuspalvelulain 16 §:n velvoitetta ilmoittaa Liikenne- ja viestintävirastolle ilman aiheetonta viivästystä palvelun toimivuuteen, tietoturvaan tai sähköisen henkilöllisyyden käyttöön kohdistuvista merkittävistä uhkista tai häiriöistä.

Virastolla on tunnistuslain 42 §:n nojalla toimivalta määrätä siitä, *milloin 16 §:ssä tarkoitettu häiriö on merkittävä sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.*

Ilmoituksen tarkoitus on tukea viraston tilannekuvaa tunnistuspalveluiden luotettavuudesta, uhkista ja häiriötilanteista. Tiedon perusteella virasto arvioi, onko vaatimuksia noudatettu ja onko tilanteesta tarvetta tiedottaa laajemmin kuin palveluntarjoaja on tehnyt. Liikenne- ja viestintävirasto voi myös tarjota tietoa tilanteesta toipumiseksi, jos sellaista on käytettävissä.

Säännös 11.1 vastaa pääosin aikaisemman määräyksen 11 §:n 2 momenttia. Säännökseen on tehty valvonta- ja soveltamiskäytännön mukaisia selvennyksiä. Ilmoituskynnystä tai ilmoitettavia tietoja ei ole tarkoitus muuttaa, vaan ainoastaan selkeyttää säännöstä.

Määräyksen 11.1 kohdassa määritellään yleisellä tasolla niitä tekijöitä, jotka ovat olennaisia häiriön tai uhkan merkittävyyden eli ilmoituskynnyksen kannalta. Tällaisia merkittäviä häiriöitä ovat muun muassa:

- tunnistusvälineen myöntäminen väärälle henkilölle

- sellaiset sulkulistojen toimivuuteen liittyvät häiriöt, joissa ajantasaista sulkulistaa ei ole saatavilla

- tunkeutuminen palveluntarjoajan järjestelmiin

- tunnistusvälineen tarjoajan varmenteiden allekirjoitusavaimien paljastuminen

- tunnistusvälineiden vakavat väärinkäytökset kuten tapaukset, jotka liittyvät tunnusten ketjuttamiseen

- vakavat sisäiset väärinkäytökset.

Sähköisen henkilöllisyyden virheitä tai väärinkäytöksiä pidetään merkittävinä hyvin matalalla kynnyksellä, samoin esimerkiksi haavoittuvuuksia tai virheitä, jotka vaarantavat tunnistamistiedon oikeellisuuden. Sen sijaan käytettävyys- tai laatuongelmien ilmoituskynnys on lähtökohtaisesti korkeampi ja niiden merkittävyyttä lisää lähinnä se, että ongelma vaikuttaa muihin luottamusverkoston toimijoihin. Tällaisia ongelmia ovat pitkät tunnistusvälineen tai tunnistusvälityspalvelun häiriötilanteet, jotka estävät tunnistuspalveluiden välittämän asioimispalveluille. Myös ensitunnistamisen ketjuttamisen pitkään estävä häiriö on merkittävä.

Yleisesti virasto arvioi, että häiriöilmoitusten tekeminen on lisääntynyt vuoden 2016 tilanteeseen nähden. Virasto toteaa, että toimijoiden menettelyissä on tässä suhteessa edelleen paljon eroja. Virasto toteaa, että häiriöilmoituksia voi mielellään tehdä myös vapaaehtoisesti.

Liikenne- ja viestintävirastolle tehdyssä ilmoituksessa annettuja tietoja käsitellään viranomaisen toiminnan julkisuudesta annetun lain (621/1999) mukaisesti ja tietoa luovutetaan ulkopuolisille tai luottamusverkoston jäsenille vain lain sallimilla edellytyksillä.

Tunnistus- ja luottamuspalvelulain 16 §:ssä säädetään myös toimijoiden välisen ilmoittamisen velvollisuudesta ja oikeudesta. Tietoa voi olla tarpeen antaa vain osalle luottamusverkoston jäsenistä. Laissa säädetään myös Liikenne- ja viestintäviraston mahdollisuudesta teknisesti välittää toimijoiden välisiä ilmoituksia. Virastolla ei ole tarjolla järjestelmää, jolla olisi mahdollista ilman erityistä teknistä kehitystyötä välittää tietoa automaattisesti toimijoiden välillä salattuna ja siten, että tieto välittyisi tapauskohtaisesti vain osalle luottamusverkostosta. Liikenne- ja viestintävirasto ylläpitää sähköpostilistaa, jolla tunnistuspalvelut voivat informoida toisiaan häiriöasioista, jotka eivät edellytä tietoturvallisempaa kanavaa.

Luottamusverkoston sisällä välitetyn häiriö- ja uhkatiedon käytölle on säädetty tunnistuslain 12 a §:ssä erityisiä rajoituksia, joiden tarkoitus on madaltaa tiedottamisen kynnystä tunnistuspalveluntarjoajien välillä.

4.11.2 Säännös 11.2 Ilmoitettavat tiedot

Säännös vastaa aikaisemman määräyksen 11 §:n 1 momenttia.

11.2 kohdassa määrätään niistä tiedoista, jotka tunnistusvälineen tai tunnistusvälityspalvelun tarjoajan on annettava Liikenne- ja viestintävirastolle tehtävässä ilmoituksessa. Ilmoituksessa edellytetään häiriön tai uhkan kuvauksen lisäksi tietoa vaikutuksista eri tahoihin.

Ilmoituksesta tulisi käydä ilmi häiriön tai uhkan tapahtumisen ja havaitsemisen ajankohta ja arvioitu kesto tai toteutunut kesto, jos se on tiedossa.

Teknisestä tapahtumakuvauksesta tulisi käydä ilmi, mihin osaan tunnistus-järjestelmästä häiriö tai uhka on vaikuttanut, havainnot tapahtumien etenemisestä, kuvaus mahdollisista toisten palveluntarjoajien osallisuudesta tapahtumiin ja tiedot tapahtuman aiheuttajasta.

Ilmoituksesta tulisi käydä ilmi häiriön pohjasyy eli onko häiriön syy inhimillinen virhe, järjestelmä- tai ohjelmistovirhe, laiterikko, palvelunestohyökkäys tai muu hyökkäys tai muu ulkoinen uhka tai luonnonilmiö.

Jos kysymys on tietoturvauhasta, ilmoituksesta tulisi käydä ilmi, onko kyseessä esimerkiksi haittaohjelma, ohjelmistohaavoittuvuus, tietomurto tai luvaton käyttö, varmenteiden tai avaintenliikenteen muuttaminen tai väärentäminen tai muu vastaava.

Häiriön tai uhkan ja sen vaikutusten kuvauksesta täytyy käydä ilmi mm., onko se vaikuttanut tietojen luottamuksellisuuteen, eheyteen tai käytettävyyteen ja ovatko henkilötiedot vaarantuneet.

Ilmoituksessa tulisi myös kertoa, millaiseen määrään käyttäjiä ja asiointipalveluita häiriö tai uhka on vaikuttanut. Ilmoituksessa on hyvä kertoa, jos on tiedossa, että häiriö tai uhka on vaikuttanut yhteiskunnan kannalta keskeiseen tai kriittiseen palveluun tai toimintoon.

Edelleen ilmoituksesta täytyy käydä ilmi lyhyen ja pitkän tähtäimen korjaustoimenpiteet, joihin on ryhdytty tai aiotaan ryhtyä häiriön tai uhkan vaikutusten poistamiseksi, lieventämiseksi ja vastaavien tilanteiden ennalta ehkäisemiseksi.

Ilmoituksesta täytyy käydä ilmi, miten asiointipalveluille, käyttäjille ja muille luottamusverkostoon kuuluville tunnistusvälineen ja tunnistusvälityspalvelun tarjoajille on tiedotettu häiriöstä tai uhkasta. Tiedotuskynnys ja tiedottamisen sisältö ja ajankohta eri osapuolille voi luonnollisesti vaihdella. Tiedottamisessa täytyy huomioida tiedon saajan mahdollisuus ja tarve suojautua häiriön tai uhkan vaikutuksilta ja sen vaikutusten minimointi.

4.11.3 Säännös 11.3 Ilmoitusmenettely

Säännös on uusi. Sillä on tarkoitus selventää määräykseen vakiintunut menettely.

Tunnistus- ja luottamuspalvelulain 16 §:n mukaan ilmoitus on toimitettava *ilman aiheetonta viivästystä.* Määräyksessä ei määrätä tiettyjä aikarajoja, mutta Liikenne- ja viestintävirasto suosittelee, että 11.1 kohdan ilmoituskynnyksen ylittävistä uhkista ja häiriöistä ilmoitetaan virastolle viimeistään 1-2 vuorokauden kuluessa niiden tapahtumisesta tai havaitsemisesta. Mitä vakavampi häiriö on, sitä nopeammin virastolle tulisi ilmoittaa.

Koska täydellisiä tietoja häiriöstä ei aina ole käytettävissä siinä vaiheessa, kun häiriö havaitaan ja sitä ryhdytään korjaamaan, ensi vaiheessa voi ilmoittaa tiedossa olevat seikat ja ilmoitusta voi täydentää myöhemmin.

Liikenne- ja viestintäviraston verkkosivuilla on lomake, jolla tiedot häiriötilanteesta voi ilmoittaa. Verkkolomakkeella voi toimittaa myös salassa pidettävää tietoa, mutta

Commented [LA5]: Info: vrt. Teletoiminnan häiriömääräys 66, perustelumuistio:

Ilmoitukset toimitetaan Liikenne- ja viestintävirastolle riippuen siitä, miten vakavasta häiriöstä on kyse (ks. pykäläkohtaiset velvoitteet erilaisista ilmoituksista).

Häiriönhallintajärjestelmä: https://eservices.traficom.fi/HHJ/

Ensi-ilmoitusten, seurantailmoitusten ja loppuraporttien sähköposti: viat@traficom.fi

Puhelin: 0295 390 80

tarkat verkkoturvallisuuteen liittyvät tiedot on syytä toimittaa muulla tavoin kuten turvapostilla. Ilmoituksen voi toimittaa myös sähköpostilla eidas@traficom.fi.

Erityisen vakavissa ja kiireellisissä häiriötilanteissa häiriöstä voi ilmoittaa virastolle puhelimitse, puhelin: 0295 390 80. Vakavia ja kiireellisiä ovat uhkat tai häiriöt, joiden haittavaikutuksia yhteiskunnassa on tarpeen ryhtyä nopeasti ehkäisemään kyberturvallisuuskeskuksen koordinaatio- ja tiedotuskeinoilla.

Commented [LA6]: Tarkistettava prosessi, vrt. yllä.

4.11.4 Muut ohjauskeinot

Ohje. Ei huomioita.

Suositus. Ei huomioita.

Yhteissääntely. Luottamusverkoston yhteistoimintaryhmässä on laadittu käytänne häiriöiden ja uhkien tiedonvaihdosta toimijoiden välillä.

Informaatiolla ohjaaminen. Ei huomioita.

4.11.5 Säännös 11, harkitut sääntelyvaihtoehdot

Viraston kyselyyn määräyksen muutostarpeista annetuissa vastauksissa esitettiin huoli, että kaikki eivät ilmoita häiriöistä virastolle riittävän alhaisella kynnyksellä ja että kaikki tunnistuspalvelut eivät informoi toisiaan häiriötilanteista.

Virasto arvioi, että näihin havaintoihin on vaikutettava ensisijaisesti valvonnalla ja tehostamalla edelleen luottamusverkoston keskinäistä informointia. Jälkimmäinen ei kuulu määräystoimivallan piiriin.

Virasto ei myöskään pidä palautteen perusteella tarkoituksenmukaisena tai tarpeellisena laatia määräykseen toimivuushäiriöille uusia tarkkoja ilmoituskynnyksiä, joilla määriteltäisiin merkittävän häiriön ajallinen ja käyttäjämäärien laskemiseen perustuva ilmoituskynnys. Arviota ei muuteta vuonna 2016 tehdystä arviosta. On myös huomattava, että tunnistuslaissa ei ole nimenomaisia vaatimuksia tunnistuspalveluiden toimintavarmuudesta, varmistamisesta tai varautumisesta eikä siten toimivaltuutta määrätä niistä.

4.12 Säännös 12 Luottamusverkostossa välitettävät vähimmäistiedot

4.12.1 Säännös 12.1 Pakolliset tiedot (attribuutit)

Säännöksessä määritellään tiedot eli attribuutit, joita tunnistustapahtumassa täytyy välittää tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun välillä tai joiden välittämiseen täytyy olla valmius. Attribuutit vastaavat EU:n komission yhteentoimivuusasetuksessa (EU) 2015/1501 määriteltyjä pakollisia tietoja.

Määräyksen 12.1 1-3 kohdissa määrätään ne tunnistetiedot, jotka tunnistusvälineen tarjoajan on välitettävä tunnistustapahtumassa tunnistusvälityspalvelulle. Määräystä on selkeytetty lisäämällä näihin kohtiin maininta, että 1 ja 2 kohdissa kysymyksessä ovat tunnistusvälineen tarjoajan varmentamat tiedot.

Tarkoitus on turvata yhteentoimivuus eli se, että tunnistusvälineen ja tunnistusvälityspalvelun tarjoajat pystyvät sopimaan sujuvasti tunnistustapahtumien välityksestä tarvitsematta määritellä attribuutteja erikseen jokaisessa sopimussuhteessa. Tarkoitus on myös varmistaa se, että kotimaisia tunnistusvälineitä voidaan käyttää rajat ylittävässä asioinnissa, jos tunnistusvälineitä notifioidaan EU:lle.

Luonnollisen henkilön tunnistustapahtumassa tulee välittää henkilön yksilöivä tunniste, joka on joko henkilötunnus (HETU) tai henkilön sähköinen asiointitunnus (SATU) säädösten sen salliessa. Osapuolet sopivat käytettävästä yksilöivästä tunnisteesta keskenään. Lisäksi tunnistetietoihin sisältyvät henkilön etu- ja sukunimi ja

syntymäaika. Tunnistus- ja luottamuspalvelulain 7 §:n mukaan tunnistusvälineen tarjoajan on hankittava ja päivitettävä luonnollisen henkilön tunnistuspalvelun tarjoamiseksi tarvitsemansa tiedot väestötietojärjestelmästä. Lain 6 §:n mukaan Tunnistuspalvelun tarjoajan tulee tarkastaa hakijalta tämän henkilötunnus tarkastaessaan hakijan henkilöllisyyden.

Oikeushenkilön tunnistustapahtumassa tulee välittää ainakin oikeushenkilöä edustavan luonnollisen henkilön yksilöivä tunniste, henkilön sukunimi, henkilön etunimi ja organisaation yksilöivä tunniste. Tunnistus- ja luottamuspalvelulain 7 a §:n perusteella tunnistusvälineen tarjoajan on hankittava ja päivitettävä oikeushenkilön tunnistuspalvelun tarjoamiseksi tarvitsemansa tiedot yritys- ja yhteisörekisteristä.

Kansallisessa luottamusverkostossa käytettävän tunnistusvälineen varmuustaso voi olla eIDAS-asetuksen määrittelemä korotettu tai korkea. Tieto välineen varmuustasosta tulee välittää tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa.

Säännöksen 12.1. 4) alakohtaan kohtaan lisätään pakollisiin tietoihin tunnistusvälityspalvelun varmistama tieto luottavasta osapuolesta eli asiointipalvelun nimi. Rajapintasuosituksissa attribuutti esitetään lyhenteellä SPname eli service provider name.

Tarkoitus on lisätä uusi keino sähköisen tunnistamisen turvallisuuden varmistamiseen. Attribuutin tarkoitus on mahdollistaa käyttäjän informointi luottavasta osapuolesta, jolle vahvistus ja henkilötiedot ollaan toimittamassa. Säännöksessä 6.2 määrätään velvollisuudesta näyttää tieto tunnistusvälineen käyttäjälle ja säännöksen 6 perusteluissa käsitellään tarkemmin turvallisuusvaikutuksia.

Tieto asiointipalvelun nimestä määritellään tunnistusvälityspalvelun ja luottavan osapuolen välisessä suhteessa. Luotettavuuden takia vastuun attribuutista on oltava tunnistusvälityspalvelulla, koska asiointipalvelun antaman tiedon käyttäminen vesittää tarkoituksen.

Teknisestä soveltamisesta virasto toteaa, että attribuutti on ollut jo ennestään määriteltynä rajapintasuosituksiin ja valmistelussa saatujen tietojen perusteella sen toteuttaminen on teknisesti ongelmatonta. Nimien määrittelyssä on käyttötarve huomioiden suositeltavaa käyttää nimiä, joiden perusteella käyttäjä todennäköisesti tunnistaa palvelun. Ei siis ole välttämätöntä käyttää esimerkiksi yrityksen kaupparekisteriin merkittyä toiminimeä, jos yrityksellä on käytössä palvelulle paremmin tunnettu nimi.

Nimet on tarpeen määritellä ennalta staattisesti. Dynaamisesti tunnistustapahtumittain määriteltävien nimien oikeellisuuden varmistaminen lennossa edellyttäisi työläitä prosesseja ja lisäisi virheriskiä esimerkiksi kirjoitusvirheiden takia.

*Tunnistusvälineen tarjoaja***.** Aloite attribuutin pakollisuuteen on tullut määräysvalmistelussa tunnistusvälineen tarjoajien puolelta. Attribuutti on ollut jo ennestään määriteltynä rajapintasuosituksiin, joten valmius voi olla osalla tunnistusvälineen tarjoajista jo määriteltynä rajapinnoissa. Tunnistusvälineen tarjoajalta se edellyttää kentän lisäämistä käytössä oleviin rajapintamäärittelyihin ja käyttäjälle annettavan informaation lisäämistä tunnistuspyynnössä.

Tunnistuslain 12 a §:n 5 momentissa säädetään luottamusverkostossa saadun tiedon käyttörajoituksista ja vahingonkorvausvastuusta. Tällä perusteella liikenne- ja viestintävirasto arvioi, että tunnistusvälineen tarjoaja ei voi käyttää saamaansa tietoa tunnistusvälityspalvelun asiointipalveluasiakkaista esimerkiksi oman kilpailevan tunnistusvälityksensä markkinoinnissa.

Pakolliset attribuutit sisältyvät tunnistuslain 12 b §:n perusteella tunnistustapahtuman enimmäishintasääntelyn piiriin, mutta hintasääntely koskee tunnistusvälineen tarjoajan tuottamia tietoja, joten sääntelyllä ei tässä tapauksessa ole merkitystä.

Tunnistusvälityspalvelu. Tunnistusvälityspalvelu tuottaa SPname-attribuutin (luottava osapuoli, jolle tunnistus ollaan välittämässä). Asiointipalveluiden kanssa on joka tapauksessa tehtävä sopimukset, joten palvelunimen määrittely sopimussuhteessa ei aiheuttane olennaisia lisäkustannuksia. Sisällöllisen määrittelyn lisäksi muutos edellyttää kentän lisäämistä käytössä oleviin rajapintamäärittelyihin. Attribuutti on ollut määriteltynä rajapintasuosituksiin, joten valmius voi olla osalla tunnistusvälineen tarjoajista jo määriteltynä rajapinnoissa.

Asiointipalvelu/luottava osapuoli. Asiointipalvelun on yhdessä tunnistusvälityspalvelun kanssa määriteltävä käyttäjälle informoitava palvelunsa nimi. Tällä ei ole olennaista taloudellista vaikutusta.

Muut ohjauskeinot

Ohje. Valvonnan havaintojen ja kyselyssä saadun palautteen perusteella virasto arvioi, että attribuutin käyttöönotto kaikissa tunnistuspalveluissa ei välttämättä toteutuisi pelkällä ohjeella, vaan edellyttää sitovaa määräystä.

Suositus. Attribuutti on jo viraston rajapintasuosituksissa. Se status muutetaan suositusten päivityksessä pakolliseksi.

Yhteissääntely. Luottamusverkostossa voidaan tarvittaessa vaihtaa tietoa asiointipalvelun nimen määrittelyyn liittyvistä havainnoista ja tiedon esittämisestä käyttäjälle.

Informaatiolla ohjaaminen. Ei huomioita.

4.12.2 Säännös 12.2 Valinnaiset tiedot

Säännöksessä 12.2 kohdassa määrätään valinnaiset tiedot. Attribuutit vastaavat EU:n komission yhteentoimivuusasetuksessa (EU) 2015/1501 määriteltyjä valinnaisia tietoja.

Rajat ylittävälle tunnistamiselle olisi tarvetta jo nyt ja kysyntä on lisääntymässä myös yksityisellä sektorilla. Valinnaisten attribuuttien tarkoitus on tukea tunnistusta ja asiointia niissä tilanteissa, joissa pakolliset attribuutit eivät ole riittäviä esimerkiksi tarkistettaessa, onko henkilö ennestään rekisteröity asiointipalvelussa (*identity matching, identity linking*).

Määräyksen 25 §:n 4 momentissa määrättiin vuoden 2018 määräysmuutoksessa siirtymäaika valmiudelle välittää 2 momentissa tarkoitettuja valinnaisia attribuutteja luottamusverkostossa käytettävässä rajapinnassa: *Valmius määräyksen 12 §:n 2 momentin mukaisten tietojen välittämiseen tunnistusjärjestelmässä on suunniteltava teknisesti viimeistään 1.10.2018.* Samalla tuolloin tarkennettiin perusteluissa, mitä valmiudella määräyksessä tarkoitetaan.

Säännökseen 12.2 on lisätty siirtymäsäännöksessä ollut tarkennus, jonka mukaan valmiuden on oltava *teknisesti suunniteltu*.

Valmius välittää valinnaisia attribuutteja tarkoittaa, että valinnaisten attribuuttien käsittely täytyy suunnitella rajapinnassa ja tunnistusjärjestelmässä siten, että tunnistuspalvelun tarjoajalla on käsitys käyttöönotossa tarvittavista teknisistä toimenpiteistä. Tekninen suunnittelu edellyttää suunnitelman dokumentointia.

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

Liikenne- ja viestintävirasto katsoo, että valmiutta on tarkoituksenmukaista lisätä asteittain ja huomioiden yritysten järjestelmien kehittämisen aikataulut. Ensivaiheessa on riittävää, että attribuutit huomioidaan tunnistusjärjestelmän suunnittelussa. Virasto arvioi, että suunnittelu nopeuttaa käyttöönottoa tarvittaessa. Tässä voidaan tukeutua viraston julkaisemiin SAML- ja OIDC-rajapintasuosituksiin. Attribuutteja ei ole tarpeen viedä järjestelmiin tuotantoon ennen kuin niille syntyy käyttötarve.

4.12.3 Säännös 12.3. Tunnistuksen pseudonymisointi (köyhdyttäminen)

Säännös on uusi. Sen tarkoitus on selventää attribuuttivaatimuksia tunnistusvälineen tarjoajan ja tunnistusvälityksen tarjoajan välisessä rajapinnassa siinä tapauksessa, että luottavalle osapuolelle eli asiointipalvelulle toimitetaan vain ns. köyhdytetty vahvistus käyttäjän todentamisesta.

Tunnistus- ja luottamuspalvelulain 8 §:n 2 momentin mukaan *Mitä 1 momentissa säädetään, ei estä palvelun tarjoamista palvelukohtaisesti siten, että tunnistuspalvelun tarjoaja ilmoittaa tunnistuspalvelua käytävälle palveluntarjoajalle tunnistusvälineen haltijan salanimen tai ainoastaan rajoitetun määrän henkilötietoja.*

Laissa tai tässä määräyksessä ei säädetä siitä, mitä henkilötietoja luottavalle osapuolelle toimitetaan tai todennetaan vahvalla sähköisellä tunnistamisella. Määräyksessä määrätään attribuuteista, joita todentamisessa käsitellään luottamusverkoston sisällä. Luottavalle osapuolelle toimitetaan tyypillisesti esimerkiksi nimi ja henkilötunnus, mutta laissa todetulla tavalla luottavalle osapuolelle voidaan toimittaa myös salanimi tai rajoitettu määrä henkilötietoja. Tällöinkin käyttäjä on todennettava vahvasti ja tunnistustapahtuman tiedot on tallennettava lain 24 §:n mukaisesti.

Määräyksessä käytetään salanimen sijaan termiä pseudonyymi, koska henkilötietojen sääntelyn kannalta kysymys on viraston arvion mukaan pseudonyymistä henkilötiedosta. Vaikka tieto olisi luottavan osapuolen näkökulmasta sikäli anonyymiä, että luottava osapuoli ei välttämättä voi yhdistää sitä tiettyyn henkilöön, tieto on yhdistettävissä henkilöön tunnistuspalveluiden tallentamien tietojen perusteella.

Pseudonyymi voi olla kertaluonteinen ja pysyvämpi riippuen siitä, miten tunnistuspalvelu on tuotteistettu. Luottavalle osapuolelle voidaan myös toimittaa esimerkiksi vahvistus käyttäjän täysi-ikäisyydestä. Edelleen luottavalle osapuolelle voitaisiin toimittaa käyttäjän osoite tai jokin muu yksittäinen henkilötieto tai joukko henkilötietoja ilman tietoa henkilötunnuksesta tai henkilötunnuksen varmentamisesta, jolla käyttäjä voidaan yksilöidä henkilönä.

Liikenne- ja viestintävirasto arvioi, että kuvatulla tavalla köyhdytettyjen tunnistuspalveluiden tarjoaminen voisi lisätä vahvan sähköisen tunnistamisen käyttötilanteita ja turvallista asiointia myös niissä tilanteissa, joissa luottavalla osapuolella ei ole oikeutta tai tarvetta käyttäjän henkilöllisyyden vaan ainoastaan jonkin muun tiedon luotettavalle todentamiselle. Määräyksen valmistelussa saatujen tietojen perusteella pseudonymisointi ja köyhdyttäminen olisi teknisesti melko triviaalia, mutta palveluille ei vaikuta olleen ainakaan toistaiseksi erityistä kysyntää. Yhteentoimivuuden edistämiseksi eri tunnistusvälineiden ja välityspalveluiden välillä olisi mahdollisesti tarpeellista määritellä luottamusverkostossa yhteisiä profiileja.

Viraston tiedossa ei ole, että tällaisia palveluita olisi tarjolla, mutta vertailun vuoksi esimerkiksi maksukortilla maksamisen yhteydessä maksajan ja maksunsaajan mak-

supalveluiden välillä tiettävästi todennetaan vahvasti vain, että maksaja on maksunsaajalle kerrotun maksukortin haltija, eikä maksupalveluiden välillä välitetä henkilötietoja.

Käyttäjää olisi informoitava henkilötietojensa käsittelystä luottamusverkostossa ja luottavalle osapuolelle annettavista tiedoista yleisen tietosuojasääntelyn mukaisesti.

Muut ohjauskeinot

Ohje. Ei huomioita.

Suositus. Liikenne- ja viestintäviraston rajapintasuosituksissa olisi tarvittaessa mahdollista kirjata yhtenäisiä käytäntöjä.

Yhteissääntely. Luottamusverkostossa voitaisiin tarvittaessa vaihtaa tietoa köyhdyttämisen toteuttamisesta ja laatia yhteisiä malleja.

Informaatiolla ohjaaminen. Ei huomioita.

4.12.4 Säännös 12, harkitut sääntelyvaihtoehdot

4.12.4.1 Uudet valinnaiset attribuutit

Määräysvalmistelussa on tarkasteltu, olisiko tarvetta lisätä luonnollisen valinnaisiin attribuutteihin kansalaisuus, syntymämaa, syntymäkaupunki, asuinmaa, puhelinnumero ja/tai sähköposti. Edelleen on tarkasteltu, olisiko tarvetta lisätä oikeushenkilön valinnaisiin attribuutteihin puhelinnumero ja/tai sähköposti.

Mainitut attribuutit ovat keskustelussa rajat ylittävän tunnistamisen teknisessä eIDAS -ryhmässä. Attribuutit edistäisivät rajat ylittävän tunnistamisen yhteentoimivuutta ja mahdollisuutta yhdistää henkilö tunnistuksen vastaanottomaassa asiointipalvelussa häntä koskeviin mahdollisiin aikaisempiin henkilötietoihin.

Attribuuttien lähteet ja mahdollisuus niiden luotettavaan varmentamiseen vaihtelee. Attribuuteilla voisi olla eri luotettavuustasoja.

Lisätiedot voi hankkia, varmentaa ja tarjota tunnistusvälineen tarjoaja tai tunnistusvälityspalvelu.

Tunnistus- ja luottamuspalvelulain 12 b §:ssä viitataan vahvassa sähköisessä tunnistamisessa käsiteltävien tunnistetietojen osalta komission täytäntöönpanoasetukseen (EU) 2015/1501. Muiden kuin näiden henkilötietojen käsittelyperusteet ja tietosuojaan liittyvät velvoitteet olisi arvioitava ja huolehdittava yleisen tietosuoja-asetuksen perusteella.

Attribuutit, jotka eivät sisälly komission täytäntöönpanoasetukseen, eivät kuulu tunnistus- ja luottamuspalvelulain 12 c §:n hintasääntelyn piiriin.

Toimialan arvion mukaan attribuuttien lisääntyminen on odotettavissa Self Sovereign Identity (SSI) –mallien kehittyessä ja on tärkeää, ettei tätä kehitystä estetä. Nykyisessä toimintamallissa akuuttia tarvetta ei kuitenkaan nähdä. Myöskään 2020 tehdyssä markkinakartoituksessa ei tullut esille, että asiointipalveluilla olisi selvästi tunnistettavia tarpeita uusille attribuuteille.[1]

[1] Ks. Traficomin tutkimuksia ja selvityksiä 2/2021 Sähköisen tunnistamisen markkinat, Sähköinen tunnistaminen turvallisen asioinnin mahdollistajana, kohta 5.2 Yritysten tarpeet, Sähköisten

Linjaus

Virasto ei tee lisäyksiä, koska uusille valinnaisille attribuuteille ei ole nähtävissä sellaista tarvetta, että niiden määrittelyä olisi nyt tarpeen edistää määräyksellä.

Muut ohjauskeinot

Ohje. Ei huomioita.

Suositus. Yhteentoimivuuden mahdollistamiseksi valinnaiset attribuutit ja niiden esitystavat voidaan listata rajapintasuosituksissa.

Yhteissääntely. Luottamusverkostossa voidaan tarvittaessa vaihtaa tietoa asiointipalveluiden attribuuttitarpeista.

Informaatiolla ohjaaminen. Yhteentoimivuus edellyttää yhtenäisiä rajapintamäärittelyjä. Pelkkä informaatio eri tunnistuspalveluilla käytössä olevista attribuuteista ei ole toimiva keino yhteentoimivan attribuuttilistan ja esitystavan määrittelemiseksi monitoimijaympäristössä.

4.12.4.2 Ensitunnistamisen attribuutit

Vuonna 2016 määräysvalmistelussa tuotiin pidemmän tähtäimen kehityksenä esiin toivomus siitä, että rajapinnan kautta voitaisiin välittää tietoa ensitunnistamisesta (esim. mihin henkilökohtainen ensitunnistaminen on perustunut: passi, henkilökortti, sähköinen tunnistaminen).

Määräysvalmistelussa on nyt arvioitu uudestaan, olisiko tarpeen lisätä määräykseen ensitunnistamisen ketjuttamisessa välitettäviä tietoja luotetusta tunnistusvälineestä.

Tunnistus- ja luottamuspalvelulain 17 §:n muutoksella on mahdollistettu se, että tunnistusvälineen tarjoajat voivat rajattomasti ketjuttaa tunnistamista eli luoda uusia sähköisiä tunnistusvälineitä luottamalla muiden tarjoamiin sähköisiin tunnisteisiin.

Liikenne- ja viestintäviraston rajapintasuosituksissa on määriteltynä ensitunnistustapahtumalle attribuutti *FTN chain level.* Tämä esitetään tunnistusvälineen tarjoajan toiselle tunnistusvälineen tarjoajalle tekemässä tunnistuspyynnössä. Pyyntö- ja tunnistus uuden tunnistusvälineen myöntämistä varten voidaan säännösten estämättä välittää myös tunnistusvälityspalvelun kautta.

Virasto ehdotti määräysvalmistelussa, että määräyksessä määriteltäisiin pakolliseksi joitain luotettuun tunnistusvälineeseen liittyviä tietoja. Viraston ennakkoarvion mukaan tietoturvallisuuden ja sähköisen tunnistuksen yleisen luotettavuuden kannalta tietojen välittäminen olisi eduksi. Hintasääntelyn takia ensitunnistuksen ketjutuksen käytön voi olettaa lisääntyvän.

Tietoturvaloukkausten selvittämistilanteessa on tärkeää, että tieto ketjuttamisesta on tavalla tai toisella selvitettävissä nopeasti ja tehokkaasti. Jos tunnistusvälineen tarjoaja myöntää esimerkiksi tunnisteita varastettujen tai väärennettyjen henkilöllisyystodistusten perusteella, on pystyttävä selvittämään, onko näillä väärän henkilön hallussa olevilla sähköisillä tunnistusvälineillä haettu sähköisesti uusia tunnistusvälineitä.

Tarpeellisia tietoa voisivat olla esimerkiksi tieto tunnistusvälineen myöntämisajankohdasta ja siitä, onko luotettu tunnistusväline myönnetty hakijan henkilöllisyyden

asiointipalvelujen näkemyksiä tulevaisuuden tarpeista, s. 53 Lähes kaikki eli 98 prosenttia näkemyksensä antaneista vastaajista pitää vahvan sähköisen tunnistamisen yhteydessä saatavia tietoja riittävinä.

osoittavan asiakirjan (passin henkilökortin tai ennen vuotta 2019 ajokortin) perusteella vai vahvan sähköisen tunnistamisen perusteella. Ensitunnistamisen ketjuttamisessa virasto esitti kysymyksen, olisiko mahdollinen aikaisempi tunnistusketju tarpeen ja välitettävissä.

Viraston ennakkoarvion mukaan tarvittavia tietoja olisi tekniseltä kannalta tunnistusjärjestelmissä valmiina, koska ensitunnistamisen tietojen tallentaminen on tunnistus- ja luottamuspalvelulain 24 §:n mukaisesti pakollista. Vaatimusten toteuttaminen edellyttäisi siten määräyksen lisäksi rajapintamäärittelyjen laatimista rajapintasuosituksiin ja sen mukaisia muutoksia tunnistusvälineen tarjoajien rajapintoihin ja tietokantojen käyttöön.

Tieto ensitunnistamisen tekemisestä ja ketjussa olevista toimijoista tukisi viraston käsityksen mukaan riskin arviointia ja hallintaa. Toisen tunnistusvälineeseen luottava välineen myöntäjä kantaa tunnistus- ja luottamuspalvelulain 17.4 §:n säännöksen perusteella vahinkovastuun. Ketjuttaminen edellyttääkin sitä, että ketjuttamista hyödyntävä välineen myöntäjä arvioi, millainen riski luotettuun tunnisteeseen mahdollisesti liittyy. Tähän riskiin vaikuttavia tekijöitä ovat se (seuraavassa lainaus vuoden 2016 arviosta), kuinka kauan sitten ja minkä henkilöllisyystodistuksen perusteella alkuperäinen henkilökohtainen tunnistaminen on tehty, onko ketjussa useampi tunnistusvälineen myöntäjä, onko jokin ketjussa ollut tunnistusvälineen myöntäjä lopettanut toimintansa ja onko ketjussa oleville tunnistusvälineen myöntäjille tapahtunut tietoturvaloukkauksia, jotka ovat voineet vaikuttaa tiedon eheyteen.

Tunnistuspalvelun tarjoajat ovat määräysvalmistelussa tuoneet yksimielisesti näkemyksenään esille, että uusien attribuuttien määrittelyn kustannusten kattaminen säädetyllä ensitunnistamisen 3 sentin enimmäishinnalla veisi kauan, virheselvitystilanteita on vähän ja määrittelykustannukset ylittäisivät virheiden selvittämisessä saadut hyödyt ja että tietojen saaminen, tallentaminen ja välittäminen vaatii kehitystyötä. Ymmärrettävien tietojen yhdenmukainen määrittely olisi työlästä. Samoin kuin vuonna 2016 ja nyt uudestaan tunnistuspalvelut esittivät, että viranomaisen, esimerkiksi Digi- ja väestötietoviraston ylläpitämä tietokanta ensitunnistamisen ketjutuksista (eli käyttäjälle myönnetyistä tunnistusvälineistä) toteuttaisi turvallisuustavoitteet ja mahdollistaisi kaikkien ketjutettujen tunnistusvälineiden sulkemisen.

Liikenne- ja viestintävirasto on ottanut huomioon toimijoiden perustelut ja sen, että virastolle tehtyjen häiriöilmoitusten perusteella ensitunnistamisen ketjuttamiseen liittyvät häiriöt ovat hyvin harvinaisia. Virasto pitää myös tarkoituksenmukaisena seurata käynnissä olevan valtion digitaalisen henkilöllisyyden kehittämishankkeen mahdollisia vaikutuksia sähköiseen ensitunnistamiseen.

Muut ohjauskeinot

Ohje. Ei huomioita.

Suositus. Liikenne- ja viestintävirasto seuraa mahdollisia häiriötilanteita ja arvioi tarvittaessa, olisiko ensitunnistamisen ketjuttamisessa välitettäviä tietoja hyödyllistä määritellä vapaaehtoisena rajapintasuosituksissa. Määräysvalmistelussa saadun palautteen perusteella on kuitenkin epätodennäköistä, että tunnistuspalvelut välittäisivät attribuutit vapaaehtoisesti.

Yhteissääntely. Luottamusverkoston häiriöryhmässä voidaan tarvittaessa vaihtaa tietoa ja tarkentaa käytänteitä häiriötilanteiden selvittämisestä.

Informaatiolla ohjaaminen. Ei huomioita.

4.13 Säännös 13 Rajat ylittävän tunnistamisen edellyttämät tiedot

4.13.1 Tunnistus julkisella sektorilla

eIDAS-asetuksen tavoite on, että jäsenvaltion eli myös Suomen notifioimia tunnistusvälineitä on mahdollista käyttää tulevaisuudessa ulkomaisiin julkisen hallinnon asiointipalveluihin tunnistautumisessa ja toisaalta ulkomaisilla notifioiduilla tunnistusvälineillä on mahdollisuus tulevaisuudessa tunnistautua suomalaisiin julkisen hallinnon asiointipalveluihin.

Säännös 13 koskee tilannetta, jossa suomalainen tunnistuspalvelu on ilmoitettu (notifioitu) eIDAS-asetuksen mukaisesti komissiolle ja tunnistusvälineen käyttäjä tunnistautuu välineellään toisen jäsenvaltion julkisen sektorin sähköisessä palvelussa. Tunnistaminen suomalaisella välineellä tapahtuisi tunnistusvälineen tarjoajalta tunnistusvälityspalvelun ja Digi- ja väestötietoviraston ylläpitämän kansallisen solmupisteen kautta.

Säännöksessä 13 määrätään, että luottamusverkostosta tulisi säilön ylittää solmupisteelle säännöksessä 12 määrätyt tiedot.Rajat ylittävässä tunnistamisessa tunnistautumisen julkisen hallinnon asiointipalveluihin tulee eIDAS-asetuksen mukaan olla ilmaista jäsenvaltioiden välillä, mutta yksityisten asiointipalveluiden tunnistamisesta eIDAS-asetus ja täytäntöönpanosäännökset mahdollistavat korvauksen perimisen tunnistusvälineen käytöstä. Tämän vuoksi tieto siitä, kohdistuuko tunnistustapahtuma julkisen hallinnon asiointipalveluun vai yksityiseen asiointipalveluun, tulee pystyä siirtämään myös tämän rajapinnan yli.

Välityspalvelun tarjoajan ja solmupisteen välistä rajapintaa koskevat säännöksen 10 mukaan samat yleiset vaatimukset kuin tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välistä rajapintaa. Muilta osin välityspalvelun tarjoaja ja solmupisteen toteuttaja sopivat säännöksen 14 mukaisesti rajapinnan ominaisuuksista keskenään. Tarkoituksenmukaista kuitenkin on, että protokollaksi valitaan jokin luottamusverkostossa käytössä oleva protokolla.

Ulkomaisella notifioidulla tunnistusvälineellä tunnistaminen *suomalaiseen julkisen sektorin palveluun* tapahtuu kansallisen solmupisteen ja suomi.fi -tunnistuksen kautta. Sitä ei käsitellä määräyksessä.

4.13.2 Tunnistus yksityisellä sektorilla

Määräyksestä poistetaan aikaisemman määräyksen 13 § 2 momentti, jossa määrättiin attribuuttien käsittelystä siinä tilanteessa, että ulkomaisella eIDAS-asetuksen mukaisesti notifioidulla tunnistusvälineellä tunnistauduttaisiin solmupisteen ja luottamusverkoston kautta yksityisen sektorin asiointipalveluun Suomessa.

Kansallisen solmupisteen käyttämisestä tunnistautumisessa *yksityisiin asiointipalveluihin* ei kuitenkaan ole yhtenäisiä määrittelyjä EU-tasolla eikä kansallisia määrittelyjä Suomessa. Kansallisessa solmupisteessä toteutetaan rajat ylittävä tunnistus julkishallinnon asiointipalveluille, mutta Digi- ja väestötietovirasto ei ole toteuttanut tai suunnitellut ulkomaisen tunnistuksen välitystä yksityisiin asiointipalveluihin. Siten määräyksen säännös on tarpeeton. Asiaa arvioidaan tarvittaessa, jos eIDAS-asetuksen tulevat muutokset sitä edellyttävät.

Ulkomaisia tunnistusvälineitä käyttävien asiakkaiden tunnistaminen suomalaisiin yksityisen sektorin asiointipalveluihin voi tapahtua sopimusperusteisesti, samoin kuin suomalaisella tunnistusvälineellä tunnistautuminen ulkomaisessa yksityisen sektorin palvelussa. Ulkomaisen tunnistuspalvelun luotettavuus voisi olla todettavissa välillisesti notifioinnin perusteella, tunnistuspalvelun kotivaltion mahdollisen sääntelyn ja valvonnan perusteella tai sopimusperusteisesti.

Kun luottamusverkostoon kuuluva tunnistusvälityspalvelu välittää vahvaa tunnistusta myös ulkomaille, tunnistusvälityspalvelun ja ulkomaisen asiointipalvelun rajapintaa ja sopimussuhdetta koskevat samat vaatimukset kuin kotimaisille asiointipalveluille tarjottaessa. Sääntely ja Liikenne- ja viestintäviraston valvonta kattavat tällöin tunnistuslain ja määräyksen vaatimukset tunnistusvälitykselle. eIDAS-asetuksen rajat ylittävän tunnistamisen yhteentoimivuus- ja turvallisuusvaatimukset komission asetuksessa (EU) 2015/1501 koskevat vain kansallista solmupistettä.

4.14 Säännös 14 Tiedonsiirrossa käytettävä protokolla ja muut vaatimukset

4.14.1 Säännös 14.1 Tiedonsiirrossa käytettävä protokolla

Säännöstä on tarkennettu nimeämällä OpenID Connect ja SAML standardeiksi, joista jommankumman mukaista rajapintaa tunnistuspalvelun on vähintään tarjottava tunnistusvälineen tarjoajien välillä eli ensitunnistamisen ketjuttamiseen ja tunnistusvälineen ja tunnistusvälityspalvelun välillä.

Säännöksen tarkoitus on tarkentaa tunnistus- ja luottamuspalvelulain 12 a §:n ja valtioneuvoston luottamusverkostoasetuksen vaatimuksia yhteentoimivuudelle ja rajapintojen ominaisuuksille ja rajoittaa niiden standardien lukumäärää, joiden mukaiset rajapinnat tunnistuspalvelun on oltava valmis ylläpitämään voidakseen osaltaan välittää tai vastaanottaa tunnistetiedot ensitunnistamisessa tai tunnistusvälityksessä luottavia osapuolia varten.

Mahdollistamisella tarkoitetaan säännöksessä sitä, että vaatimusta tarkastellaan ensitunnistamisen tai luottavalle osapuolelle välitettävän tunnistustapahtuman vastaanottajan oikeuden näkökulmasta, mikä tunnistus- ja luottamuspalvelun sääntelyllä on tarkoitus turvata. Tunnistuspalvelu voi täyttää velvoitteensa luottamusverkostossa myös tarjoamalla toiminnon toisen luottamusverkoston tunnistuspalvelun kautta, kunhan säädetyt ja määrätyt vaatimukset tällöinkin täyttyvät.

Liikenne- ja viestintäviraston 2020 määräyksen muutostarpeista tekemään kyselyyn saatujen vastausten perusteella rajapintaprotokollien tekniseen ohjaukseen ei liity suuria muutostarpeita. Kyselyyn saadut vastaukset tukivat viraston ennakkoarviota siitä, että 14 § informatiivinen säännös on hyvä säilyttää. Rajapintojen tarkempi ohjaaminen on tarkoituksenmukaista edelleen tehdä suosituksella. Suositusten tehokkuudesta tai pikemminkin tehottomuudesta yhteentoimivuuden edistämisessä tuli kuitenkin kriittisiä kommentteja.

Liikenne- ja viestintävirasto suosittelee käyttämään SAML 2.0 - tai Open ID Connect -protokollien kansallisesti laadittuja profiileja, jotka virasto on julkaissut erillisinä suosituksina 2018 ja päivittänyt 2021 (212/2021 S ja 213/2021 S). Rajapintatoteutukselle kansallisesti säädetyt ja tai määrätyt erityiset vaatimukset tarkennetaan suosituksissa ja muilta osin standardien noudattamisessa on sovellettava hyviä yleisiä käytäntöjä.

Sopimusvapauteen vaikuttaa tunnistus- ja luottamuspalvelulain ja valtioneuvoston luottamusverkostoasetuksen sääntely. Tunnistus- ja luottamuspalvelulain 12 a.3 §:n mukaan *[t]unnistuspalvelun tarjoajien on tehtävä yhteistyötä sen varmistamiseksi, että luottamusverkoston jäsenten väliset tekniset rajapinnat ovat yhteen toimivia ja että ne mahdollistavat yleisesti tunnettujen standardien mukaisten rajapintojen tarjoamisen luottaville osapuolille.*

Valtioneuvoston asetuksen 169/2016 (muutettu 1212/2018) 1.1 §:n mukaan *tunnistuslain 12 a.2 §:ssä (viittaus on päivittämättä, mutta asiasta säädetään 12 a §:n muutoksen jälkeen 12 a.3 §:ssä) tarkoitettuja teknisiä rajapintoja ovat 1) tunnistusvälineen tarjoajien välinen rajapinta; 2) tunnistusvälineen tarjoajan ja tunnistusväli-*

tyspalvelun tarjoajan välinen rajapinta; 3) tunnistusvälityspalvelun tarjoajan ja tunnistuspalveluun luottavan osapuolen välinen rajapinta. Asetuksen 1.3 §:n mukaan Luottamusverkostoon kuuluvan tunnistuspalvelun tarjoajan on tarjottava 1 momentin 1 ja 2 kohdassa tarkoitetuissa rajapinnoissa kummassakin vähintään yhtä yleisesti käytetyn standardin mukaista teknistä rajapintaa.

Määräysvalmistelussa 2016 arvioitiin seuraavia kysymyksiä: *Millä tarkkuudella rajapintavaatimukset laaditaan määräykseen suhteessa yksittäisiin protokolliin, kuten SAML ja Open ID Connect? Mahdollistetaanko toisin sanoen myös muiden protokollien käyttö? Miten huomioidaan puhtaasti kansallinen TUPAS-protokolla, joka ei kaikilta osin täytä vaatimuksia ja jonka kehityssuunnitelmista tai mahdollisuuksista ei ole ollut määräyksen valmistelussa varmaa tietoa?*

Määräysvalmistelussa 2016 linjattiin, että ei määräyksessä ei *määrätä, mitä protokollia on käytettävä, vaan tämä jää toimijoiden sovittavaksi. Sen sijaan määrätään lopputuloksesta, joka protokollalla on saatava aikaan eli vähimmäistiedoista, jotka protokollan avulla on kyettävä siirtämään ja rajapinnan tietoturvavaatimuksista.*

Vuoden 2016 jälkeen Tupas-protokolla on poistunut käytöstä ainakin vahvassa tunnistamisessa ja mobiilioperaattorit ovat siirtyneet osassa rajapinnoista käyttämään vanhan ETSI mobiilivarmennerajapinnan sijaan OpenIDConnectia. OpenIDConnect on muutenkin vallitseva protokolla, mutta myös SAML on jossain määrin käytössä.

4.14.2 Säännös 14.2 Rajapinnan muut ominaisuudet

Säännös vastaa aikaisemman määräyksen 14 §:ää.

Säännöksen tarkoitus on selventää sitä, että luottamusverkoston osapuolet ja luottavat osapuolet sopivat keskenään protokollasta ja rajapinnan niistä ominaisuuksista, joista ei ole säädetty. Luottamusverkoston sisällä sopimusvapautta on rajattu sääntelyllä attribuuttien ja protokollan osalta. Luottavien osapuolten kanssa sopimusvapautta on rajattu rajapinnan turvallisuusvaatimusten osalta.

4.14.3 Uusien protokollastandardien käyttöönotto luottamusverkostossa

Virasto arvioi määräysvalmistelussa saamiensa tietojen ja toimialaseurannan perusteella, että teknisessä ohjauksessa ei ole tällä hetkellä nähtävillä tarvetta käsitellä tarkemmin tiettyjä uusia protokollia. Luottamusverkoston sisällä OpenID Connect ja SAML vaikuttavat riittävästi mahdollistavan tunnistuspalveluiden kehityksen. ETSI on jossain määrin käytössä mobiilivarmentajien välisissä rajapinnoissa.

Findy -ryhmän esille tuomat rajapinta- tai arkkitehtuuritarpeet itsehallittavan identiteetin mahdollistamiselle (Self Sovereign Identity) eivät ole vielä kansainvälisesti niin selkeät tai vakiintuneita (valtioneuvoston luottamusverkostoasetus " yleisesti käytetyn standardin mukaista"), että niitä olisi mahdollista tai tarkoituksenmukaista huomioida määräyksessä tai teknisessä ohjauksessa. Asiaa arvioidaan tarpeen mukaan uudestaan, jos EU-sääntelyn tai kansallisen sääntelyn muutokset tai tekninen kehitys sitä edellyttää.

Jos syntyy tarvetta ottaa käyttöön uusia protokollia valtioneuvoston luottamusverkostoasetuksen tarkoittamana *yleisesti käytetyn standardin mukaisena teknisenä rajapintana,* valmistelussa vaihdetaan tietoa asetuksen tarkoittamassa luottamusverkoston yhteistoimintaryhmässä ja virasto arvioi teknisen kehityksen kypsyyttä kansallisesti ja kansainvälisesti saatavilla olevan objektiivisen tiedon perusteella.

~~IPv6-suositus (onko tarpeen ja mitä näkökulmia edellyttäisi)~~

~~Traficom on edistänyt IPv6-tuen lisäämistä muilla viraston teknisen ohjauksen tai valvonnan sektoreilla suosituksilla.~~

~~Virasto ei ole valmistellut nimenomaista IPv6-suositusta tunnistuspalveluille, mutta tarvittaessa sellainen voidaan laatia.~~

Commented [LA7]: **10.6.2021: siirretään rajapintasuosituskeskusteluun**

4.14.4 Säännös 14, harkitut sääntelyvaihtoehdot

4.14.4.1 Luottaviin osapuoliin vaikuttavat yhteentoimivuusvaatimukset

Liikenne- ja viestintävirasto on selvittänyt määräysvalmistelussa, liittyykö luottamusverkoston teknisiin määrittelyihin tekijöitä, joilla on vaikutusta tunnistuksen välitysmahdollisuuksiin luottaville osapuolille.

Tunnistus- ja luottamuspalvelulain 12 a § mukaan *luottamusverkoston yhteistyöllä on varmistettava, että tekniset rajapinnat mahdollistavat yleisesti tunnettujen standardien mukaisten rajapintojen tarjoamisen luottaville osapuolille.*

Liikenne- ja viestintävirasto on tässä yhteydessä kiinnittänyt huomiota ainakin tunnistus- ja luottamuspalvelulain 18 §:n mukaisiin tunnistusvälineen käyttörajoituksiin ja tarkastusmahdollisuuteen, joka tunnistusvälineen tarjoajan on järjestettävä luottaville osapuolille.

Määräyksen muutostarpeista 2020 järjestetyssä kyselyssä ja määräysvalmistelussa ei kuitenkaan tullut esille mitään luottaviin osapuoliin liittyviä tarpeita lukuun ottamatta kertakirjautumisen saatavuutta.

Liikenne- ja viestintävirastolla ei ole havaintoja toiminnoista, joiden mahdollistamista olisi tarpeen tai mahdollista edistää määräyksellä yhteentoimivuuden edistämiseksi luottaville osapuolille. Luottavien osapuolten saamiin palveluihin vaikuttavia kertakirjautumisen reunaehtoja ja tietoturvallista toteutusta käsitellään säännöksessä 6.2.3. ja tunnistuksen pseudonymisointia säännöksessä 12.3.

4.15 Säännös 15 Vaatimustenmukaisuuden arviointikriteerit

4.15.1 Säännös 15.1 Tunnistusjärjestelmän ja tunnistusmenetelmän arvioitavat toiminnot

Säännös vastaa aikaisemman määräyksen 15.1 §:ää. Säännöksellä tarkennetaan tunnistus- ja luottamuspalvelulain 29 §:ssä säädettyjä tunnistuspalvelun vaatimuksenmukaisuuden arviointiperusteita.

Toimintojen tai osa-alueiden ryhmittely perustuu EU:n komission varmuustasoasetuksen vaatimusten ryhmittelyyn. Säännökseen lisätään kansalliseen luottamusverkostosääntelyyn liittyvän yhteentoimivuuden arviointi.

Säännöksessä luetellaan ne tunnistuspalvelun toteutuksen ja tarjonnan toiminnot, joiden osalta säädännön vaatimusten täyttyminen täytyy osoittaa joko ulkoisella tai sisäisellä arvioinnilla.

15.1 1a) alakohdan tietoturvallisuuden hallinta tarkoittaa säännöksen 4 mukaista tietoturvallisuuden hallintajärjestelmää.

15.1 1b) tietojen säilyttäminen tarkoittaa säännöksen 5 mukaista tietojen luokittelua ja suojaustoimenpiteitä sekä lokitietoja ja varmuuskopioita, säännöksen 6 haltijakohtaisten tietojen käsittelyä ja myös tunnistus- ja luottamuspalvelulain 24 §:n mukaisten lokitietojen käsittelyä.

15.1 1c) alakohdan tilojen ja henkilökunnan vaatimukset tarkoittavat tilaturvallisuutta ja oman tai alihankittujen palveluiden henkilökunnan osaamisen ja määrän riittävyyttä suhteessa arvioitavaan toimintaan

15.1 1d) alakohdan teknisillä toimenpiteillä tarkoitetaan kattavasti erityisesti määräyksen 2 luvussa tarkennettuja teknisiä määrittelyjä ja turvakontrolleja.

15.1 1e) yhteentoimivuudella tarkoitetaan määräyksen 3 luvun rajapinta- ja attribuuttivaatimuksia.

Commented [LA8]: Täydennetään vielä poiminnoilla arviointiohjeesta 211/2019

Kaikki laissa ja tässä määräyksessä asetetut vaatimukset. Säännöksessä selvennetään sitä, että arvioinnin täytyy kattaa kaikki arvioitaville toiminnoille tunnistus- ja luottamuspalvelulaissa ja määräyksessä asetetut vaatimukset. Tunnistus- ja luottamuspalvelulailla tarkoitetaan myös laissa viitattuja kohtia EU:n komission varmuustasoasetuksessa. Tietoturva- ja yhteentoimivuusvaatimuksia tarkennetaan erityisesti tämän määräyksen 2 ja 3 luvuissa.

Suhde tietoturvallisuuden hallintajärjestelmään. Vaatimuksenmukaisuuden arvioinnissa on huomattava, että säännöksen 4 mukainen tietoturvallisuuden ja riskien hallinta ei riitä täyttämään tunnistusjärjestelmän aineellisia vaatimuksia, vaan tunnistusjärjestelmän on kaikilta osin täytettävä säädetyt ja määrätyt tekniset vaatimukset. Vaatimustenmukaisuuden arvioinnin kannalta tämä tarkoittaa sitä, että pelkkä tietoturvallisuuden hallinnan arviointi ei riitä osoittamaan säädettyjen vaatimusten täyttämistä, vaan on nimenomaisesti arvioitava, täyttääkö järjestelmä esimerkiksi tietoliikenteen salausvaatimukset.

Esimerkiksi ISO 27001 standardin näkökulma on oleellisesti erilainen kuin tunnistus- ja luottamuspalvelulain ja tämän määräyksen mukaiset arviointiperusteet. ISO-standardien avulla sertifioitu tai muutoin määritelty tietoturvallisuuden hallintajärjestelmä luo hallinnollista kerrosta ja pikemminkin välineitä tietojen käsittelyn ja palveluiden hallintaan eikä sertifiointi itsessään osoita organisaation yksittäisten tai kaikkien palveluiden tietoturvallisuuden ja tietosuojan tason riittävyyttä tai teknisten tietoturvatoimenpiteiden olemassaoloa.

Vrt. EU:n varmuustasoasetuksen soveltamisohje, LOA guidance

> *Riskienhallinnassa yleisenä periaatteena on, että organisaation on itsensä valittava, minkä tasoista riskiä se pitää hyväksyttävänä. Kohdan 2.4 vaatimuksella muutetaan tätä yleistä periaatetta, sillä sen mukaan organisaation turvatoimenpiteiden on oltava suhteutettuja riskeihin kulloisellakin tasolla.*

4.15.2 Säännös 15.2 Arviointikriteeristö

Säännöstä selkeytetään, jotta se kuvaa paremmin tarkoitusta ja vakiintunutta valvontakäytäntöä.

Tunnistus- ja luottamuspalvelulain 29 §:n mukaan *Liikenne- ja viestintävirasto voi määrätä arviointiperusteeksi edellä 1 ja 2 momenteissa tarkoitettujen säädösten lisäksi Euroopan unionin tai muun kansainvälisen toimielimen antamia säännöksiä tai ohjeita, julkaistuja ja yleisesti tai alueellisesti sovellettuja tietoturvallisuutta koskevia ohjeita ja yleisesti käytettyjä tietoturvallisuusstandardeja tai menettelyjä.*

Virasto ei määrää perusteeksi tiettyjä lähteitä, vaan määräyksessä määritellään reunaehdot vaatimuksenmukaisuuden arvioinnissa käytettäville kriteeristöille. Säännökseen lisätään viittaus Liikenne- ja viestintäviraston arviointiohjeeseen, jonka ajantasainen versio on määräyksen valmistelun ajankohtana 211/2019. Ohje on päivitetty 2019 perusteellisesti huomioimaan kaikki säädetyt vaatimukset ja siihen on lisätty mobiilisovelluksia koskeva erityiskriteeristö. Ohjeesta on syytä käyttää ajantasaisinta versiota, jotta kaikki vaatimukset tulevat huomioiduksi.

Arvioinnissa voidaan lisäksi ottaa huomioon myös muita lähteitä, kuten tietoturvallisuusstandardeja, jotka tarkentavat hyviä tietoturvakäytäntöjä ja konkretisoivat arvioinnissa huomionarvoisia yksityiskohtia. Esimerkkejä näistä luetellaan jäljempänä.

Tunnistuspalveluntarjoaja voi täyttää säännöksessä määrätyt arvioinnin vaatimukset yhdellä tai useammalla valitsemallaan arvioinnilla. Myös arviointielimiä voi olla useita. Arviointielimen riippumattomuus- ja pätevyysvaatimuksista säädetään tunnistus- ja luottamuspalvelulain 33 §:ssä ja vaatimuksia tarkennetaan tämän määräyksen säännöksessä 18 ja 19.

Arvioinnin hankkivan tunnistuspalveluntarjoajan on huolehdittava sitä, että arvioinnissa otetaan huomioon myös nimenomaisesti tunnistusjärjestelmään ja tunnistusmenetelmään kohdistuvat vaatimukset, vaikka palvelun tuotanto- ja hallintaympäristö usein on vain osa muuta tuotanto- ja hallintaympäristöä ja vaikka arviointi kohdistuisi kokonaisuutena tähän laajempaan kokonaisuuteen.

Tavoitteena on, että toimijat voisivat hyödyntää joustavasti arviointikriteeristöjä, joita ne muutoinkin jo käyttävät. Toisaalta toimijoiden täytyy arvioida ja varmistaa, että niiden käyttämät eri standardeihin perustuvat kriteeristöt todella kattavat kaikki vaaditut tunnistusjärjestelmän arvioinnin osa-alueet ja niiden vaatimukset.

4.15.3 Esimerkkejä arviointilähteistä [viitteet]

Commented [LA9]: Jätetään tähän oma kohta, kaikki myös lopun koottuun viiteluetteloon

Standardeja tai lähteitä, jotka voivat soveltua myös tunnistusjärjestelmän arviointiin osana arviointia.

- ISO 27001
- Katakri
- PiTuKri
- PCI DSS, PCI/QSA
- Webtrustin Trust Services Principles and Criteria for Certification Authorities ja Webtrust for Certification Authorities - SSL Baseline Requirements Audit Criteria
- Information Security Forumin (ISF) "Standard of Good Practice"
- ISF:n IRAM-kriteeristö (Information Risk Analysis Methodology)
- ETSI TS 101456 (CA policy) - jos palveluntarjoaja tarjoaa luottamuspalveluita, esimerkiksi tähän liittyvään ETSI-kriteeristön arviointiin on mahdollista viitata
- ISRS 4400 ja ISAE 3000
- Vahti-ohjeet
- Tietohallintalautakunnan suositukset https://vm.fi/suositukset
- Euroopan keskuspankin tai FIVA:n määräykset tai ohjeet
- FIVA:n määräys ja ohje 2.4 "Asiakkaan tunteminen - rahanpesun ja terrorismin rahoittamisen estäminen"
- Euroopan keskuspankin SREP cyber risk questionnaire, https://www.eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2/guidelines-on-ict-risk-assessment-under-the-srep
- BISin (Bank for International Settlements) ohje External audits of banks ja supplemental note to External audits of banks - audit of expected credit loss
- Ruotsin Finansinspektionin (FFFS) ja Suomen Finanssivalvonnan määräyksiä ja ohjeita koskien sisäisen tarkastuksen organisointia ja toimintaa (mm Fiva)

- kansainvälisen kattojärjestön IIA:n ohjeita, sääntöjä ja tarkastusperiaatteita (The Institute of Internal Auditors, www.theiia.fi).

4.15.4 Määräykselle vaihtoehtoiset ohjauskeinot ja viraston arviointiohje 211/2019

Suositus/ohje. Liikenne- ja viestintäviraston arviointiohje 211/2019 on päivitetty vuonna 2019 perusteellisesti huomioimaan kaikki säädetyt vaatimukset ja siihen on lisätty mobiilisovelluksia koskeva erityiskriteeristö. Ohjetta on tarkoitus ylläpitää siten, että sen ajantasaisen version käyttäminen kattaa kaikki säädetyt vaatimukset.

Yhteissääntely. Alalle tulon kynnyksen ja mahdollisten kilpailuoikeudellisten kysymysten kannalta on parempi, että viranomainen vastaa vähimmäisvaatimusten asettamisesta. Tiedonvaihto erilaisten kriteeristöjen hyödyntämisestä ja tulkintakysymyksistä soveltuu yhteissääntelyn piiriin.

Informaatio-ohjaus. Ei huomioita.

4.16 Säännös 16 Selvitys tunnistuspalvelun tarjoajan ja julkaistujen tietojen luotettavuudesta

4.16.1 Tunnistuspalvelun ilmoitusvelvollisuuteen liittyvät selvitykset

Säännökseen on koottu selvyyden vuoksi ne tunnistuspalveluntarjoajan ja sen lakisääteisesti julkaisemien tietojen luotettavuutta koskevat osa-alueet, joista ei edellytetä säännöksen 15 tavoin riippumatonta ja pätevää vaatimuksenmukaisuuden arviointia.

Säännös liittyy tunnistuspalvelun tunnistus- ja luottamuspalvelulain 10 §:ssä säädettyyn ilmoitusvelvollisuuteen Liikenne- ja viestintävirastolle. Virastolla on tunnistus- ja luottamuspalvelulain 42 §:n perusteella toimivalta määrätä *tunnistuspalvelun aloitus- tai muutosilmoituksessa ilmoitettavien tietojen sisällöstä ja toimittamisesta virastolle.*

Tunnistuspalveluntarjoajan on siis annettava tiedot ja selvitykset Liikenne- ja viestintävirastolle aloitus- tai muutosilmoituksen yhteydessä tai jos virasto muutoin pyytää niitä valvoessaan tunnistuspalveluita.

Säännöksessä ei määrätä ilmoitettavista tiedoista ja selvitysten muodoista tyhjentävästi. Säännöksessä määrätään yleisellä tasolla, että näiden vaatimusten täyttämisen voi osoittaa yrityksen omalla selvityksellä tai soveltuvalla muulla selvityksellä tai arvioinnilla.

Ilmoituksista ja selvityksistä ohjataan ja neuvotaan ilmoituslomakkeilla ja ilmoitusohjeella sekä tarvittaessa toimijakohtaisella neuvonnalla.

4.16.2 Selvitettävät tiedot

Säännöksen ilmaisut osittain lähtöisin sähköisen tunnistamisen varmuustasoasetuksen kohdista 2.4 hallinto ja organisointi ja erityisesti 2.4.1 yleiset säännökset ja 2.4.2 julkaistut ilmoitukset ja käyttäjätiedot. Vastaavat vaatimukset säädetään tunnistus- ja luottamuspalvelulaissa. Säännöksen otsikkoa ja sanamuotoa on selkeytetty, kohtien järjestystä vaihdettu ja sisältöön on tehty joitakin tarkennuksia ottaen huomioon tunnistuspalvelun tarjoajan ilmoitusvelvollisuudet.

1) *tunnistuspalvelusta vastaava vakiintunut oikeushenkilö ja vastuuhenkilöiden toimintakelpoisuus ja luotettavuus.* Kohdan vaatimukset liittyvät tunnistus- ja luottamuspalvelulain 9 §:n vaatimuksiin. Esimerkiksi oikeushenkilöllisyys voidaan osoittaa rekisteriotteella ja vastuuhenkilöiden luotettavuus selvitetään esimerkiksi henkilöiden antamalla kirjallisella vakuutuksella tai soveltuvilla lähteillä.

2) *julkaistut ilmoitukset ja käyttäjätiedot, kuten tunnistusperiaatteet, tietosuojaperiaatteet, käyttörajoitukset, sopimusehdot ja hinnastot.* Kohdan vaatimukset liittyvät tunnistus- ja luottamuspalvelulain 12 b, 14, 15 ja 18 §§:ien vaatimuksiin. Julkaistujen tietojen luotettavuus selvitetään esittämällä julkaisupaikat ja julkaistut tiedot.

3) *riittävät taloudelliset voimavarat ja valmius ottaa vahinkovastuuriski*. Kohdan vaatimukset liittyvät tunnistus ja luottamuspalvelulain 13 §:n vaatimuksiin. Taloudelliset voimavarat ja vahinkoriskin kantokyky selvitetään tilinpäätöksellä, taseella ja tilintarkastuskertomuksella ja mahdollisella selvityksellä vastuuvakuutuksesta.

4) kohdan vaatimus liittyy tunnistus- ja luottamuspalvelulain 13 §:n vaatimukseen. Vastuu alihankkijoista ilmenee myös määräyksen 15 kohdan vaatimustenmukaisuuden arvioinnissa, mutta on myös osa tunnistuspalvelun hallinnon vaatimustenmukaisuutta. Keskeiset alihankkijat tulisi mainita myös lain 14 §:n mukaisissa tunnistusperiaatteissa.

5) kohta liittyy tunnistus- ja luottamuspalvelulain 13 §:n vaatimukseen. Suunnitelman tarkoitusta ja sisältöä kuvaa sähköisen tunnistamisen varmuustasoasetuksen kohta 2.4.1 5: *Sähköisen tunnistamisen järjestelmille, jotka eivät perustu kansalliseen lakiin, on oltava tehokas suunnitelma järjestelmän päättämisen varalta. Tällaisen suunnitelman on sisällettävä palvelun hallittu lopettaminen tai siirto toiselle palveluntarjoajalle, tapa ilmoittaa tästä asiaankuuluville viranomaisille ja loppukäyttäjille sekä tiedot siitä, miten järjestelmään kirjatut tiedot suojataan, säilytetään ja hävitetään järjestelmän toimintaperiaatteiden mukaisesti.*

4.16.3 Viraston ilmoitusohje 214/2016 O

Viestintäviraston ohjeessa 214/2016 O tunnistus- ja luottamuspalveluiden ilmoituksista käsitellään joiltain osin tietoja tai liitteitä, joita Liikenne- ja viestintävirastolle on toimitettava. Tiedoista ei kuitenkaan ole laadittu yksityiskohtaisia soveltamisohjeita, vaan tarvittavia tietosisältöjä arvioidaan mm. tunnistus- ja luottamuspalvelulain perustelujen avulla.

4.17 Säännös 17 Kansallisen solmupisteen arviointiperusteet

Säännös on lähinnä informatiivinen. Komission täytäntöönpanoasetuksessa (EU) 2015/1501 [XX] mainitaan oletuksena standardiin ISO/IEC 27001 perustuva tietoturvallisuuden hallinta. Määräyksessä vahvistetaan tämä olettama, koska tämä on myös käytännössä Digi- ja väestötietoviraston toimintaan soveltuva ratkaisu. Komission täytäntöönpanopäätöksessä säädetään joitain vaatimuksia solmupisteen toiminnalle.

4.18 Säännös 18 Tunnistuspalvelun ulkoisen arviointielimen vaatimukset

Liikenne- ja viestintävirastolle tunnistus- ja luottamuspalvelulain 10 §:n mukaisesti annettavassa aloitus- tai muutosilmoituksessa ja sen liitteissä annetaan valvovalle viranomaiselle tiedot riippumattomasta arvioinnista. Lisäksi on annettava selvitys, jonka perusteella voidaan arvioida, että arvioinnin tekijä täyttää tunnistus- ja luottamuspalvelulain 33 §:n vaatimukset arviointielimen riippumattomuudelle ja pätevyydelle.

Auditoinnin tekevä arviointielin voi tunnistus- ja luottamuspalvelulain 29 §:n mukaisesti olla joko sisäinen tarkastuslaitos, muu ulkoinen arviointilaitos tai akkreditoitu vaatimustenmukaisuuden arviointilaitos.

Säännöksen tarkoitus on selkeyttää arviointielimen riippumattomuuden ja pätevyyden määrittelyn perusteita ennakoitavasti. Tarkoitus on selkeyttää myös sitä, että arviointielimen riippumattomuus ja pätevyys eivät voi perustua toimijan omiin säännöstöihin tai omaan arvioon, vaan niiden on oltava objektiivisesti perusteluja.

Säännöksessä 18.1 luetellaan esimerkkejä sellaisista kansainvälisistä standardeista tai sääntely- tai itsesääntelykehyksistä, joihin arviointielimen riippumattomuus ja pätevyys voi perustua. Luettelo ei ole tyhjentävä ja 5 kohdassa todetaan yleisesti edellytykset sille riippumattomuuden ja pätevyyden osoittamiselle. Tarkoitus on, että toimijat voisivat tukeutua mahdollisimman joustavasti erilaisiin jo muutoinkin käyttämiinsä arviointeihin.

Esimerkkejä mahdollisista arviointielimistä ovat akkreditoitu ISO 27001 tarkastuslaitos, muu ulkoinen ISO 27001-auditoija tai vastaavat muihin relevantteihin standardeihin perustuvat arvioijat.

Säännöksestä 18.2 ilmenee, että edellytyksenä eri standardien tai säännöstöjen käyttämiselle riippumattomaan ja pätevään tunnistusjärjestelmän arviointiin on se, että arviointi todella kohdistuu tunnistusjärjestelmän vaatimuksiin. On tunnistuspalvelun tarjoajan vastuulla huolehtia siitä, että näin todella on ja että arviointi kattaa kaikki tässä määräyksessä määritellyt osa-alueet.

Tarkastuskertomuksesta on ilmettävä selkeästi auditoinnin kohdistuminen tosiasiassa tunnistusjärjestelmän vaatimuksiin.

4.19 Säännös 19 Tunnistuspalvelun sisäisen tarkastuslaitoksen vaatimukset

Säännöksen perustelut ovat samat kuin säännöksen 18 perustelut. Myöskään sisäisen tarkastuslaitoksen riippumattomuus ja pätevyys eivät voi perustua toimijan omiin säännöstöihin tai omaan arvioon, vaan niiden on oltava objektiivisesti perusteltuja ja sovelluttava perustellusti tunnistusjärjestelmän vaatimusten arviointiin.

Luku 6 Hyväksytyt luottamuspalvelut

4.20 Säännös 20 Hyväksytyn luottamuspalvelun tarjoajan arviointikriteerit

4.20.1 Yleistä luottamuspalveluiden sääntelystä ja standardeista

Yleisesti luottamuspalveluiden sääntelyn tavoitteena on tietoyhteiskunta-kehitys ja luottamuksen lisääminen sähköiseen asiointiin. Luottamuspalveluiden sääntelyllä autetaan sähköisten palveluiden toteuttajia ja käyttäjiä tunnistamaan ne palvelut, joiden avulla on mahdollista toteuttaa sähköisten asiointipalveluiden eri toiminnot mahdollisimman tietoturvallisesti.

eIDAS-asetuksessa määritellään vaatimukset, jotka hyväksytyn luottamuspalvelun tarjoajan ja luottamuspalveluiden tulee täyttää. Vaatimusten sisältöä tarkentamaan Euroopan telestandardointi-instituutti ETSI on laatinut komission mandaatilla luottamuspalveluiden tarjoajia koskevia standardeja. Standardeihin on koottu yksityiskohtaiset konkreettiset vaatimukset, joiden täyttyminen varmistaa sen, että luottamuspalvelun tarjoaja on eIDAS-asetuksen mukainen.

Määräyksen tavoitteena on selkeyttää hyväksyttyjen luottamuspalvelujen eIDAS-asetuksessa säädettyjä vaatimuksia viittaamalla EU:n valmistelutyössä viitoittamiin kansainvälisiin standardeihin **siltä osin, kun niihin ei ole ainakaan toistaiseksi tehty viittauksia komission täytäntöönpanosäädöksillä, vaikka siihen olisi eIDAS-asetuksessa toimivalta.**

Standardiviittaukset määräyksessä tukevat myös sitä, mitä ainakin tulee huomioida mahdollisten vaatimustenmukaisuuden arviointilaitosten pätevyysvaatimuksena, kun niitä akkreditoidaan.

Standardit eivät ole pakollisia, vaan toiminnot voi toteuttaa muullakin tavalla. Standardit osoittavat kuitenkin sen, millaista luotettavuustasoa eIDAS-asetus edellyttää.

Jos käytetään muuta vastaavat vaatimukset sisältävää standardia, palvelun toteuttajan on erikseen osoitettava, että toiminta täyttää eIDAS-asetuksen vaatimukset. Määräyksessä viitataan niihin standardeihin, jotka ovat määräyksen antamisen ajankohdalla valmiita.

Määräykseen täydennetään edellisen määräyksen antamisen jälkeen valmistuneiden standardien viittaukset.

ETSI standardit on saatettu sellaisenaan voimaan Suomessa ja ne löytyvät myös SFS-standardeina. Tällöin merkitsemistapa on esimerkiksi SFS-EN 319 401.

Enisa on laatinut arvion eIDAS-standardeista: Enisa Assessment of Standards related to eIDAS (December 14, 2018)[VIITE] https://www.enisa.europa.eu/publications/assessment-of-standards-related-to-eidas

4.20.2 Hyväksytyn luottamuspalvelun tarjoajan yleiset ja palvelukohtaiset vaatimukset

4.20.2.1 Säännös 2.1.1 Hyväksytyn luottamuspalvelun tarjoajan yleiset vaatimukset

ETSI EN 319 401 V2.2.1 (2018-04) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [VIITE]

Standardi sisältää yleiset palveluriippumattomat vaatimukset hyväksytyn luottamuspalvelun tarjoajalle. Se sisältää vaatimuksia mm. riskien arvioinnille, tietoturvapolitiikalle ja -käytännölle sekä toiminnan johtamiselle.

4.20.2.2 Säännös 20.1.2 Hyväksytyn varmenteen tarjoajan lisävaatimukset

Varmenteita myöntävän hyväksytyn luottamuspalvelun tarjoajan standardiviittaukset on yhdistetty samaan säännökseen, joka koskee hyväksyttyjen varmenteiden myöntämistä.

ETSI EN 319 411-1 V1.2.2 (2018-04) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [VIITE]

Seuraava versio ETSI EN 319 411-1 V1.3.0 (2021-02) on hyväksyntämenettelyssä.

Standardi sisältää yleiset vaatimukset varmenteita tarjoavalle luottamuspalvelun tarjoajalle. Se täydentää ja tarkentaa standardissa EN 319 401 esitettyjä vaatimuksia. Standardi sisältää yksityiskohtaisia vaatimuksia mm. varmennepolitiikalle ja varmennuskäytännölle. Standardiin liittyy informatiivinen liite C (Conformity Assessment Check list), johon on koottu standardin vaatimukset tarkistuslistan muodossa. Tarkistuslistaa voi hyödyntää esimerkiksi luottamuspalvelun tarjoajan auditoinnissa.

ETSI EN 319 411-2 V2.2.2 (2018-04) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates [VIITE]

Seuraava versio ETSI EN 319 411-2 V2.3.0 (2021-02) on hyväksyntäkierroksella.

Standardi sisältää vaatimukset eIDAS-asetuksen mukaisia hyväksyttyjä varmenteita tarjoavalle luottamuspalvelun tarjoajalle. Se täydentää standardissa EN 319 411-1 esitettyjä vaatimuksia vastaamaan eIDAS-asetuksen erityisvaatimuksia. Lisävaatimukset kohdistuvat mm. varmennepolitiikkaan ja varmennuskäytäntöön.

Standardiin liittyy informatiivinen liite B (Conformity Assessment Check list), johon on koottu standardin vaatimukset tarkistuslistan muodossa. Tarkistuslistaa voi hyödyntää esimerkiksi luottamuspalvelun tarjoajan auditoinnissa.

4.20.2.3 Säännös 20.1.3 Hyväksytyn aikaleiman tarjoajan lisävaatimukset

ETSI EN 319 421 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps [VIITE]

Standardi sisältää tietoturvapolitiikka- ja tietoturvavaatimukset sähköisiä aikaleimoja tarjoavalle luottamuspalvelun tarjoajalle. Standardi viittaa pääsääntöisesti standardin EN 319 401 vaatimuksiin, mutta tarkentaa niitä joiltain osin. Standardi sisältää yksityiskohtaiset vaatimukset aikaleiman allekirjoitusavaimen sisältävän yksikön TSU (Time-Stamping Unit) hallinnalle. Standardiin liittyy informatiivinen liite H (Conformity Assessment Check list), johon on koottu standardin vaatimukset tarkistuslistan muodossa. Tarkistuslistaa voi hyödyntää esimerkiksi luottamuspalvelun tarjoajan auditoinnissa.

4.21 Säännös 21 Hyväksytyn luottamuspalvelun arviointikriteerit

4.21.1 Hyväksytyt luottamuspalvelutyypit

eIDAS-asetuksen mukaiset hyväksytyt (qualified) luottamuspalvelut voivat olla seuraavia palvelutyyppejä:

1) hyväksytty sähköisen allekirjoituksen varmenne (28 artikla) (Qualified certificate for electronic signature)
2) Hyväksytyn sähköisen allekirjoituksen hyväksytty validointipalvelu (33 artikla)(Qualified validation Service for qualified electronic signature)
3) Hyväksytyn sähköisen allekirjoituksen hyväksytty säilyttämispalvelu (34 artikla) (Qualified preservation Service for qualified electronic signature)
4) Hyväksytty sähköisen leiman varmenne (38 artikla) (Qualified certificate for electronic seal)
5) Hyväksytyn sähköisen leiman hyväksytty validointipalvelu (40 art.) (Qualified preservation Service for qualified electronic signature)
6) Hyväksytyn sähköisen leiman hyväksytty säilyttämispalvelu (40 art.) (Qualified preservation Service for qualified electronic seal)
7) hyväksytty sähköinen aikaleima (42 artikla)(Qualified time stamp)
8) hyväksytty sähköinen rekisteröity jakelupalvelu (44 artikla) (Qualified electronic registrered delivery Service, "eDelivery"/QERDS)
9) verkkosivujen todentamisen hyväksytty varmenne (45 artikla) (Qualified certificate for website authentication, QWAC)

Hyväksyntä hankitaan eIDAS-asetuksen 20 ja 21 artiklan mukaisesti.

4.21.2 Standardit

Säännöksessä tarkennetaan hyväksyttyjen luottamuspalveluiden arviointikriteerit.

eIDAS-asetuksen liitteissä I, III ja IV määritellään sähköisten allekirjoitusten, sähköisten leimojen ja verkkosivustojen todentamisen hyväksyttyjä varmenteita koskevat vaatimukset.

Vaatimusten sisältöä tarkentamaan Euroopan telestandardointi-instituutti ETSI on laatinut komission mandaatilla määräystekstissä luetellut standardit. Standardeihin on koottu yksityiskohtaiset konkreettiset vaatimukset, joiden täyttyminen varmistaa sen, että luottamuspalvelu on eIDAS-asetuksen mukainen.

Standardit eivät ole pakollisia, vaan palvelut voi toteuttaa muullakin tavalla. Standardit osoittavat kuitenkin sen, millaista luotettavuustasoa eIDAS-asetus edellyttää palveluissa. Jos palvelun toteuttaa viitatun standardin mukaisesti, eIDAS-asetuksen vaatimukset tulevat huomioiduksi. Jos käytetään muuta vastaavat vaatimukset sisältävää standardia, palvelun toteuttajan on erikseen osoitettava, että palvelu täyttää eIDAS-asetuksen vaatimukset.

Määräyksessä lueteltuihin varmenneprofiileihin sisältyvät yleiset vaatimukset sisältävä standardi (EN 319 412-1), varmenteen tarkoitetun sovelluksen mukaisia standardeja (EN 319 osat 2-4) sekä hyväksyttyjen varmenteiden sisällön (statements) määrittelevä standardi (EN 319 412-5).

Siltä osin kuin standardeissa on eritelty EU-säädännön vaatimusten täyttymistä koskevat ja muita vaatimuksia koskevat osat, tämän määräyksen kannalta soveltuvina osina pidetään EU-säädännön täyttymiseen liittyviä vaatimuksia.

Seuraavassa taulukossa on koottuna hyväksyttyjä luottamuspalveluntarjoajia ja eri luottamuspalveluja koskevat standardit. Tekniset spesifikaatiot (ETSI TS) eivät ole vielä vahvistettuja, joten niihin ei viitata määräyksessä.

Palvelu, eIDAS-artikla	**valmis standardi**	**tekninen spesifikaatio**
hyväksytty luottamuspalveluntarjoaja (kaikki luottamuspalvelutyypit)	ETSI EN 319 401	Suositeltava ETSI TS 119 312 V1.3.1 (2019-02)
varmenteita tarjoava luottamuspalveluntarjoaja (kaikki hyväksytyt varmenteet)	ETSI EN 319 411-1 ETSI EN 319 411-2	
Allekirjoitusvarmenne artikla 28	ETSI EN 319 412-1 ETSI EN 319 412-2 ETSI EN 319 412-5	
Leimavarmenne artikla 38	ETSI EN 319 412-1 ETSI EN 319 412-3 ETSI EN 319 412-5	
verkkosivuvarmenne (QWAC) artikla 45	ETSI EN 319 412-1 ETSI EN 319 412-4 ETSI EN 319 412-5	
Aikaleima artikla 42	ETSI EN 319 421 ETSI EN 319 422	
sähköisen allekirjoituksen validointi	ETSI EN 319 102-1	ETSI TS 119 441 ETSI TS 119 442

art 33		ETSI TS 119 102-2 ETSI TS 119 172-4
sähköisen leiman validointi art 40, viittaus art 33	ETSI EN 319 102-1	ETSI TS 119 441 ETSI TS 119 442 ETSI TS 119 102-2 ETSI TS 119 172-4
sähköisen allekirjoituksen säilyttäminen art 34		ETSI TS 119 511 ETSI TS 119 512
sähköisen leiman säilyttäminen Art 40, viittaus art 34		ETSI TS 119 511 ETSI TS 119 512
sähköinen rekisteröity jakelupalvelu (eDelivery) art 44	ETSI EN 319 521 ETSI EN 319 522 ETSI EN 319 531 ETSI EN 319 532	

Luku 7 Luottamuspalvelujen vaatimustenmukaisuuden arviointilaitokset

4.22 Säännös 22 Arviointilaitosten pätevyyden arviointi

4.22.1 Akkreditointi ja hyväksyntä

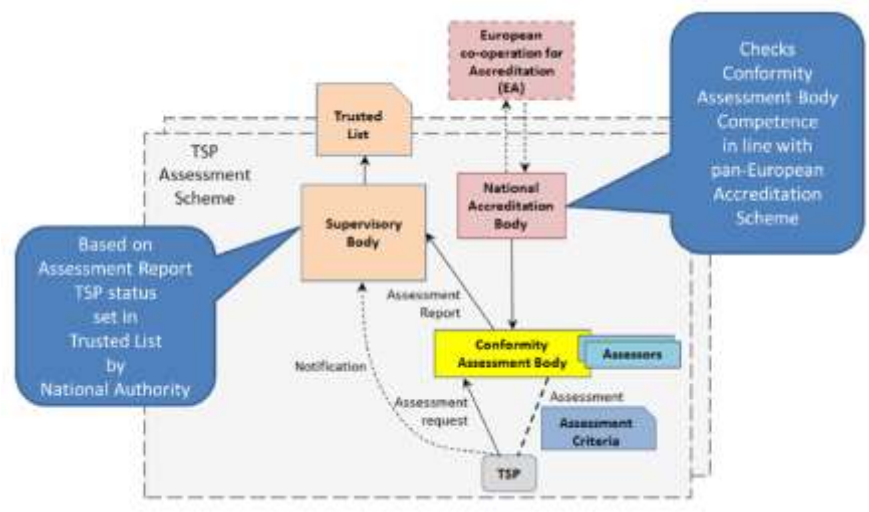
Vaatimustenmukaisuuden arviointilaitoksen aseman saaminen edellyttää tunnistus- ja luottamuspalvelulain 33 §:n mukaisten riippumattomuus- ja pätevyysvaatimusten osoittamista FINASilta [VIITE] haettavalla akkreditoinnilla.

Säännöksellä tarkennetaan tunnistus- ja luottamuspalvelulain 33 §:n pätevyysvaatimuksia vaatimustenmukaisuuden arviointilaitokselle.

Kun FINAS tekee vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta annetun lain (920/2005) tarkoittaman päätöksen arviointilaitoksen akkreditoinnin kriteereistä, se voi huomioida muitakin riippumattomuuden ja pätevyyden arviointiin liittyviä vaatimuksia kuin tässä määräyksessä viitatut standardit.

Lisäksi laitoksen tulee hakea hyväksyntä Liikenne- ja viestintävirastolta. Hyväksynnän edellytyksenä on FINASin akkreditointi ja selvitys tunnistuslain 33.1 §:n 4 kohdan edellyttämistä ohjeista ja niiden seurannasta.

Seuraavassa kuvassa kuvataan yleisen akkreditointisääntelyn ja eIDAS-asetuksen sektorikohtaisen valvonnan suhteita sähköisen luottamuspalvelun vaatimustenmukaisuuden arvioinnissa. Kuvassa ei ole mukana arviointilaitoksen (*conformity assessement body, CAB*) hyväksyntä- ja valvontaroolia, joka on kansallisesti säädetty tunnistus- ja luottamuspalvelulaissa Liikenne- ja viestintäviraston tehtäväksi. Määräyksen tarkennukset liittyvät kuvassa akkreditointivaatimuksiin (*Accreditation Scheme*), josta akkreditointielin päättää (National Accreditation Body, Suomessa FINAS).



Kuva: Luottamuspalvelun tarjoajan arvioinnin kaavio

(Lähde Euroopan tietoturvallisuusviraston ENISAn dokumentti *Auditing Framework for TSPs, Guidelines for Trust Service Providers, Versio 1.0 - December 2014* [VIITE])

Commented [LA10]: Auditing Framework for TSPs — ENISA (europa.eu)

4.22.2 Standardi

Komissio ei ole laatinut täytäntöönpanopäätöstä, jolla tarkennettaisiin eIDAS-asetuksen 20.4 artiklan nojalla vaatimuksenmukaisuuden arviointilaitosta koskevat standardit.

Koska komissio ei ole antanut asiaa koskevaa täytäntöönpanosäädöstä, seuraavassa kappaleessa kuvataan EA:n dokumentissa luetellut standardit toimivat pohjana vaatimustenmukaisuuden arviointilaitosten akkreditoinnissa ja hyväksynnässä. Joissakin jäsenvaltioissa on vahvistettu omia vaatimuksia.

Eurooppalaisten akkreditointiorganisaatioiden yhteistyöelin EA (European Cooperation for Accreditation) on laatinut 2015 dokumentin *EA Certification Committee Reference Paper; ETSI / EA Recommendations regarding; Preparation for Audit under EU Regulation (EU) No 910/2014 Article 20.1*.[VIITE] Siinä määritellään, miten luottamuspalveluiden vaatimustenmukaisuuden arviointilaitosten (Conformity Assessment Bodies, CAB) akkreditoinnissa siirrytään aiemmasta käytännöstä eIDAS-asetuksen mukaiseen käytäntöön ja mitä vaatimuksia akkreditoinnissa edellytetään arviointilaitoksen täyttävän ja minkä asioiden osalta sillä pitää olla pätevyys. Pohjana ovat ETSIn laatimat standardit.

Vaatimustenmukaisuuden arviointilaitoksen vaatimukset on määritelty standardissa ETSI EN 319 403-**1** V2.3.1 (2020-06) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers [VIITE].

Standardi pohjautuu standardiin ISO/IEC 17065, joka määrittelee yleiset vaatimukset arviointilaitoksille. Standardi EN 319 403 täydentää ISO/IEC-standardin vaatimuksia erityisesti luottamuspalveluiden tarjoajia ja niiden tarjoamia palveluita koskevilla vaatimuksilla.

Standardiin on lisätty osa 2, joka koskee varmenteiden myöntäjien arviointia. Osa ei ole vielä vahvistettu, vaan tekninen spesifikaatio (TS). **Standardia ei siten määrätä viitteeksi, mutta sitä voidaan soveltaa.**

*ETSI TS 119 403-**2** V1.2.1 (2019-04) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates*

Tunnistus- ja luottamuspalvelulain mukaisesti arviointilaitoksella tulee olla pätevyys arvioida palveluntarjoajaa ja sen tarjoamia palveluita. Määräyksen säännökset 20 ja 21 tarkentavat arviointivaatimuksia luottamuspalveluiden tarjoajalle ja luottamuspalvelulle, joten arviointilaitokselta tulee edellyttää pätevyyttä pykälissä mainittujen standardien mukaiseen arviointiin.

4.22.3 Arviointikertomus

ETSI:n standardiin 119 403 on myös lisätty osa 3, jossa standardoidaan arviointikertomus. Osa ei ole vielä vahvistettu, vaan tekninen spesifikaatio (TS).

*ETSI TS 119 403-**3** V1.1.1 (2019-03) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers*

Liikenne- ja viestintävirasto määräysvaltuutus tunnistus- ja luottamuspalvelulain 42 §:ssä ei koske luottamuspalvelun vaatimuksenmukaisuuden arviointikertomusta, vaan ainoastaan arviointikriteerejä. **Standardia ei siten määrätä viitteeksi, mutta arviointilaitos voi soveltaa sitä.**

Liikenne- ja viestintävirasto on antanut ohjeen 215/2019 luottamuspalvelun arviointikertomuksesta. Ohjeen sisältö luottamuspalveluiden arvioinnista on sama kuin ohjeessa 215/2016.

Luku 8 Hyväksytyn sähköisen allekirjoituksen ja sähköisen leiman luontivälineen sertifiointi

4.23 Säännös 23 Sähköisen allekirjoituksen tai leiman luontivälineen sertifiointilaitos

4.23.1 Pätevyysvaatimukset

Aikaisemman määräyksen säännös 23 ja 24 on yhdistetty.

Jos jokin suomalainen sertifioija haluaa hakeutua hyväksytyksi sertifiointilaitokseksi, se voi hakea hyväksyntää Liikenne- ja viestintävirastolta tunnistus- ja luottamuspalvelulain 36 §:n mukaisesti ja pykälässä säädetyillä edellytyksillä.

Säännöksessä 23 määrätään siitä, miten laissa edellytetyn pätevyyden voi osoittaa. Mahdollisia tapoja ovat ainakin akkreditointi, joka tarkoittaa FINASin tekemään pätevyyden arviointia, tai liittyminen SOGIS-MRA -sopimuksen vertaisarviointiin perustuvaan pätevyyden arviointimenettelyyn.

SOGIS-MRA (Senior Officers Group for Information Systems, Mutual Recognition Agreement)[VIITE] on eurooppalainen järjestelmä sertifiointien keskinäiseen tunnustamiseen. Mukana on kahdeksan maata, joilla on omia sertifioijia (*qualified/authorising participant*) ja kaksi maata (*consuming participant*), joilla ei ole omia sertifioijia (mm. Suomi).

Pätevyys sertifiointilaitoksena toimimiseen edellyttää, että toimijalla on kyky todentaa luontivälineen vaatimukset, jotka asetetaan komission täytäntöönpanopäätöksellä (EU) 2016/650 [viite]. Päätöksessä (EU) 2016/650 on viittaukset hallussapitoon perustuvan luontivälineen standardeille. CENin standardit etäluontivälineelle on hyväksytty standardointimenettelyssä, mutta niiden lisääminen komission täytäntöönpanopäätökseen on tämän perustelumuistion valmisteluhetkellä vasta vireillä.

EU:n tai ETA-alueen jäsenvaltioiden komissiolle ilmoittamien jäsenvaltioissa hyväksyttyjen sertifiointilaitosten tekemät sertifioinnit ovat sellaisenaan päteviä myös Suomessa. Tällä hetkellä suuri osa komissiolle ilmoitetuista sertifiointielimistä kuuluu myös SOGIS-MRA -sopimuksen piiriin.

4.23.2 Standardit

Vaatimukset tukeutuvat komission täytäntöönpanopäätökseen (EU) 2016/650 [43].

Komission täytäntöönpanopäätöksen liitteessä vahvistetaan sertifioinnin pohjaksi seuraavat standardit. Niistä yleinen IT-tietoturvallisuuden arvioinnin standardi ISO/IEC 15408 Information technology -- Security techniques -- Evaluation criteria for IT security-standardisarja [VIITE] tunnetaan Common Criteria -vaatimuksina.

Etäallekirjoitusvälineen standardit

Komission täytäntöönpanopäätöksessä ei ole vielä viittauksia standardeihin tai muita tarkennuksia eIDAS-asetuksen vaatimuksiin, mutta komissio valmistelee täytäntöönpanopäätöksen päivittämistä.

Luku 9 Siirtymäsäännökset ja allekirjoitukset

4.24 Säännös 24 Määräyksen voimaantulo ja siirtymäsäännökset

Määräys on tarkoitus saattaa voimaan helmikuussa 2022 Lopullisessa perustelumuistiossa: Määräys tulee voimaan pp.kk.vvvv

Mahdolliset siirtymäsäännökset

1) 6.2 tunnistusmenetelmän erityiset turvatoimenpiteet

- 6.2.1 edellyttää luottavan osapuolen nimen näyttämistä käyttäjälle.
    - Lyhyt siirtymäaika
    - Vaatimus on yhteydessä 12.1. 4) kohdan attribuutin tuottamiseen ja 9.1.2 vaatimukseen, että tunnistussanoma (myös pyyntö) on allekirjoitettava - voi tulla käyttöön jo ennen 8.1. avainten käyttöönottoa, ks. 9.1.2
    - Määritelty rajapintasuosituksiin pakollisena
    - millä aikataululla prosessi toteutettavissa, huomioiden sopimussuhde luottavaan osapuoleen - tekninen toteutus ks. 9.1.2

- 6.2.2 edellyttää session binding -viestin/kuvan/tms. näyttämistä käyttäjälle tunnistuksen vahvistuspyynnössä **ja** tunnistusvälineen sovelluksessa/selaimessa
    - Tunnistuspalveluiden tehtävissä, ei ole samalla tavalla vaikutusta luottavaan osapuoleen kuin kohdalla 6.2.1
    - osalla tunnistuspalveluista ominaisuus on jo käytössä
    - millä aikataululla teknisesti toteutettavissa niillä, joilla ei ole jo käytössä

2) 8.1 tietoliikenteen osapuolten tunnistaminen

- missä ajassa voidaan laatia tekniset menettelyt ja prosessit vanhojen sopimusasiakkaiden/luottavien osapuolten tunnistamiseen
    - vaikuttaa olennaisesti myös luottaviin osapuoliin
    - siirtymäaika uusille asiakkaille voi olla lyhyempi kuin vanhoille
- edellyttääkö siirtymäaikaa luottamusverkoston sisällä
    - rajattu määrä toimijoita ja vahvat kyvykkyydet tai jo valmiina

3) 8.2 avainten ja varmenteiden uusiminen

- missä ajassa voidaan laatia tekniset menettelyt ja prosessit avainten varmenteiden päivittämiselle
    - vaikuttaa olennaisesti myös luottaviin osapuoliin
    - siirtymäaikatarve uusille asiakkaille ja vanhoille asiakkaille sama vai eri
- edellyttääkö siirtymäaikaa luottamusverkoston sisällä
    - rajattu määrä toimijoita ja vahvat kyvykkyydet

9) 9.1.2 tunnistussanomien allekirjoittaminen luottamusverkoston ja luottavan osapuolen välillä

- ei siirtymäaikaa tai erittäin lyhyt siirtymäaika
- liittyy 8.1 avainten/varmenteiden voimaansaattamiseen, mutta jo sitä ennen voidaan allekirjoittaa nyt käytössä olevilla avaimilla

4.25 (Jälkiseuranta)

- Tässä kerrotaan, jos määräyksen toimeenpanoa ja toimivuutta (sille asetettujen tavoitteiden toteutumista) aiotaan seurata jotenkin

5 Liitteet ja viitteet

5.1 Viiteluettelo

[päivitetään, tässä MPS2016 viitteet]

Linkit aihepiiriin liittyviin säädöksiin on koottu Viestintäviraston verkkosivulle ja merkitty viiteluetteloon tähdellä * https://www.viestintavirasto.fi/ohjausjavalvonta/lait-maarayksetpaatokset.html

Viestintäviraston ohjeet ja suositukset löytyvät viraston verkkosivuilta ja ne on merkitty viiteluetteloon kahdella tähdellä **

https://www.viestintavirasto.fi/ohjausjavalvonta/ohjeetjajulkaisut/ohjeidenjulkinto-jensuositustenjaselvitystenasiakirjat.html

ETSIn standardit löytyvät ETSIn verkkosivulta ja ne on merkitty viiteluetteloon kolmella tähdellä ***

https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx

[1] * Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009 muutoksineen, **tunnistus- ja luottamuspalvelulaki**)

[2] * EU:n komission täytäntöönpanoasetus (EU) 2015/1502 (nk. **varmuustasoasetus**) teknisten vähimmäiseritelmien ja -määrittelyjen vahvistamisesta sähköisen tunnistamisen menetelmien varmuustasoja varten sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 8 artiklan 3 kohdan mukaisesti

[3] * EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta (nk. **eIDAS-asetus**)

[4] FINAS (Finnish Accreditation Service) Turvallisuus- ja kemikaaliviraston (Tukes) akkreditointiyksikkö https://www.finas.fi/Sivut/default.aspx

[5] * Valtioneuvoston asetus vahvan sähköisen tunnistuspalvelun tarjoajien luottamusverkostosta 169/2016 (nk. **valtioneuvoston luottamusverkostoasetus**)

[6] ** Viestintäviraston ohje 211/2016 O tunnistuspalveluntarjoajan auditoinnin malliikrteeristö

[7] ** Viestintäviraston ohje 215/2016 O sähköisten tunnistus- ja luottamuspalveluiden tarkastuskertomuksista

[8] ISO/IEC 27001 Information security management

[9] *** ETSI EN 319 401 V2.1.1 Electronic Signatures and Infra-structures (ESI); General Policy Requirements for Trust Service Providers

[10] EU:n varmuustasoasetuksen epävirallinen soveltamisohje (julkaistu Viestintäviraston työryhmäsivulla https://www.viestintavirasto.fi/ohjausjavalvonta/yhteistyo/kansallinenyhteistyo/tyoryhmat/tunnistaminenjaluottamuspalvelut-tyoryhma.html)

[11] ** Viestintäviraston suositus 212/2016 S Finnish Trust Network SAML 2.0 Protocol Profile

[12] ** Viestintäviraston suositus 213/2016 S OpenID Connect Protocol Profile for the Finnish Trust Network

[13] TUPAS, Pankkien Tupas–tunnistuspalvelun tunnistusperiaatteet v2.0b 28.3.2011
http://www.finanssiala.fi/maksujenvalitys/dokumentit/Tupas-tunnistusperiaatteet_v20b.pdf

[14] *** ETSI TS 119 612 v 2.1.1 Trusted lists. Huom. ETSIn sivulta löytyy toistaiseksi uudempi versio, joka ei vastaa eIDAS-asetusta, ks. esim.: https://www.google.fi/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwiExuLyl-fPAhUMnRQKHde8Ax0QFgggMAE&url=https%3A%2F%2Filnas.services-publics.lu%2Fecnor%2FdownloadPreview.action%3FdocumentReference%3D185416&usg=AFQjCNGRVFbAoeD-PMkiuZS8WSH1d03N2lQ&bvm=bv.136499718,d.d24

[15] KATAKRI, Tietoturvallisuuden auditointityökalu viranomaisille, löytyy esim. http://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

[16] 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

[17] Viestintäviraston kyberturvallisuuskeskuksen NCSA (National Com-munications Security Authority, NCSA-FI)

- Yleistä NCSA-FI tietoa https://www.viestintavirasto.fi/kyberturvallisuus/viestintaviraston tietoturvapalvelut/ncsa-fi.html
- Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset suojaustasot (ohje 11.11.2015 dnro 190/651/2015) https://www.viestintavirasto.fi/attachments/tietoturva/Kryptografiset_vahvuusvaatimukset_-_kansalliset_suojaustasot.pdf
- Viestintäviraston NCSA-toiminnon hyväksymät salausratkaisut (27.4.2016 dnro 238/651/2013) https://www.viestintavirasto.fi/attachments/tietoturva/NCSA_salausratkaisut.pdf

[18] NISTin (National Institute of Standards and Technology) FIPS-standardit (Federal Information Processing Standards) www.nist.gov

[19] SANS (The SANS Institute) www.sans.org

[20] eIDAS - Cryptographic requirements for the Interoperability Framework, TLS and SAML, Version 1.0, 6 November 2015 https://joinup.ec.europa.eu/sites/default/files/eidas_-_crypto_requirements_for_the_eidas_interoperability_framework_v1.0.pdf

[21] IANAn (Internet Assigned Numbers Authority) IKEv2-määritykset http://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml

ja IANAn ciphersuitet: http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4

[22] ENISAn ohjeet luottamuspalveluiden eIDAS-artiklan 19 häiriöilmoituksista (viitteet lisätään, kun ohjeet on annettu) www.enisa.europa.eu

[23] * Komission täytäntöönpanoasetus (EU) 2015/1501 **yhteentoimivuusjärjestelmän vahvistamisesta sähköisestä tunnistamisesta** ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 12 artiklan 8 kohdan mukaisesti

[24] VTJkysely-palvelu; Sovelluskyselyiden rajapintakuvaus https://eevertti.vrk.fi/Default.aspx?id=150

[25] *** ETSI TS 101456 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates

[26] BIS, Bank for International Settlements: External audits of banks - http://www.bis.org/publ/bcbs280.htm, The internal audit function in banks http://www.bis.org/publ/bcbs223.htm

[27] Finanssivalvonnan määräys- ja ohjekokoelma http://www.finanssivalvonta.fi/fi/Saantely/Maarayskokoelma/Uusi/Documents/4.1.std5.pdf

[28] *** ETSI EN 319 401 V2.1.1 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

[29] *** ETSI EN 319 411-1 V1.1.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certifi-cates; Part 1: General requirements

[30] *** ETSI EN 319 411-2 V2.1.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certifi-cates; Part 2: Requirements for trust service providers issuing EU qualified certificates

[31] *** ETSI EN 319 421 V1.1.1 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Elec-tronic Time-Stamps

[32] *** ETSI EN 319 412-1 V1.1.0 (2015-12) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures

[33] *** ETSI EN 319 412-2 V2.1.0 (2015-12) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

[34] *** ETSI EN 319 412-3 V1.1.0 (2015-12) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons

[35] *** ETSI EN 319 412-4 V1.1.0 (2015-12) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates

[36] *** ETSI EN 319 412-5 V2.1.0 (2015-12) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

[37] *** ETSI EN 319 422 V1.1.0 (2015-12) Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

[38] *** ETSI EN 319 521 Policy & security requirements for electronic registered delivery service providers

[39] REM (Registered Electronic Mail) TS 102 640-x -spesifikaatiosarja

[40] Eurooppalaisten akkreditointiorganisaatioiden yhteistyöelin EA (European Co-operation for Accreditation): EA Certification Committee Reference Paper; ETSI / EA Recommendations regarding; Preparation for Audit under EU Regulation (EU) No 910/2014 Article 20.1.

[41] *** ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers

[42] ENISA: Auditing Framework for TSPs, Guidelines for Trust Service Providers, Versio 1.0 - December 2014

https://www.enisa.europa.eu/publications/tsp-auditing-framework

[43] * KOMISSION TÄYTÄNTÖÖNPANOPÄÄTÖS (EU) 2016/650, annettu 25 päivänä huhtikuuta 2016, hyväksyttyjen allekirjoituksen ja leiman luontivälineiden tietoturva-arviointia koskevi-en standardien vahvistamisesta sähköisestä tunnistamisesta ja sähköisiin transaktioihin liit-tyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 30 artiklan 3 kohdan ja 39 artiklan 2 kohdan mukaisesti

[44] ISO/IEC 15408 Information technology -- Security techniques -- Evaluation criteria for IT security -standardisarja

[45] ISO/IEC 18045:2008 – Information technology – Security techniques – Methodology for IT security evaluation

[46] *** EN 419 211 – Protection profiles for secure signature creation device, osat 1–6

[47] CEN, the European Committee for Standardization

- **CEN TC 224 / WG 17** https://standards.cen.eu/dyn/www/f?p=204:22:0::::FSP_ORG_ID,FSP_LANG_ID:478566,25&cs=16448244FB7AC1BDE2E621EACB21E71E2
  PP Secure Signature Creation Device (419211) in a user-managed environment; already available
  Server signing (419241) – for a TSP-managed environment; under development
    - Part1: Security requirements for signature generation services
    - Part2: A protection profile for signature activation module to be used in a HSM.
- TSP Cryptographic Modules (419221) – Development of Protection Profiles
    - Part 1 to Part 4 almost published (signing operations, key generations)
    - Part 5 under development: generic crypto module for Trust Service Providers.

[48] *** ETSI (119 432) DTS/ESI-0019432 Protocol for TSPs providing signature generation services, osat 1-4

[49] *** ETSI (119 442) DTS/ESI-0019442 Protocol for TSPs providing signature validation services

[50] SOGIS-MRA (Senior Officers Group for Information Systems, Mutual Re-cognition Agreement), http://www.sogisportal.eu/

[51] ITU-R TF.1876 (03/2010) Trusted time source for time stamp authority

https://www.itu.int/dms_pubrec/itu-r/rec/tf/R-REC-TF.1876-0-201004-I!!PDF-E.pdf

[52] * Komission täytäntöönpanopäätös (EU) 2015/1506 eritelmien vahvistamisesta sellaisia **kehittyneiden sähköisten allekirjoitusten ja kehittyneiden leimojen muotoja** varten, jotka julkisen sektorin elinten on tunnustettava sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 27 artiklan 5 kohdan ja 37 artiklan 5 kohdan mukaisesti.

[53] *** ETSIn tekninen eritelmä 103171 v.2.1.1 (XadES)

[54] *** ETSIn tekninen eritelmä 103173 v.2.2.1 (CAdES)

[55] *** ETSIn tekninen eritelmä 103172 v.2.2.2 (PAdES)

[56] *** ETSIn tekninen eritelmä 103174 v.2.2.1 (Assosioitujen allekirjoitusten säilötiedoston perustason profiili)

5.2 Vaikutusarviointi

5.3 Lausuntoyhteenveto (jos lausunnot eivät sisälly perustelumuistioon)