

Perustelut määräykselle sähköisistä tunnistus- ja luottamuspalveluista (M72 B/2022)

1	Määräyksen tausta ja säädösperusta.....	6
1.1	Määräyshistoria ja päivittämisen syyt	6
1.2	Määräystoimivallan säädösperusta.....	6
1.3	Asiaan liittyviä muita määräyksiä ja säädöksiä	6
1.3.1	Sähköinen tunnistaminen	6
1.3.2	Sähköisen allekirjoituksen ja leiman luontiväline.....	7
1.3.3	Henkilötiedot.....	8
2	Määräyksen tavoite	8
2.1	Tavoitteet	8
2.2	Pääasialliset muutokset ja arvio määräyksen vaikutuksista	9
2.3	Muut toteuttamismahdollisuudet	15
3	Määräyksen valmistelu	16
3.1	Sidosryhmävalmistelu	16
3.2	Lausuntopalaute	16
3.2.1	Yleinen palaute ja henkilötietojen suoja	16
3.2.2	Säännös 4.1 Tietoturvallisuuden hallinnan standardi (4 Tunnistuspalvelun tietoturvallisuuden hallintajärjestelmä).....	17
3.2.3	Säännös 5 Tunnistusjärjestelmän tietoturva-vaatimukset.....	18
3.2.4	Säännös 5.5 Tunnistusjärjestelmän tuotantoverkon hallinta- ja etäyhteydet.....	18
3.2.5	Säännös 6.1 Tunnistusmenetelmän ominaispiirteet ja suojauskyky	18
3.2.6	Säännös 6.2.1 Tunnistusmenetelmän erityiset turvatoimenpiteet (session binding)	19
3.2.7	Säännös 6.2.2 (SPname)	20
3.2.8	Säännös 6.2.3 Kertakirjautuminen	20
3.2.9	Säännös 7 Tunnistusjärjestelmän rajapintojen salausvaatimukset ja muut salausasiat.....	20
3.2.10	Säännös 8.1 Tietoliikenneyhteyden osapuolten tunnistaminen	21
3.2.11	Säännös 8.2 varmenteiden ja avainten uusiminen	24
3.2.12	Säännös 9 Tunnistussanomien eheys ja luottamuksellisuus.....	26
3.2.13	Säännös 11.3 Tunnistuspalvelun häiriöilmoitusten ilmoitusmenettely	26
3.2.14	Säännös 12.2 Luottamusverkostossa välitettävät valinnaiset tiedot.....	26
3.2.15	Säännös 15.2 Tunnistuspalvelun arviointikriteeristö	27
3.2.16	Säännös 16 Selvitys tunnistuspalvelun tarjoajan ja julkaistujen tietojen luotettavuudesta	27
4	Yksityiskohtaiset perustelut	28

20.5.2022

Määräyksen luku 1 Yleiset säännökset	28
4.1 Säännös 1 Soveltamisala	28
4.2 Säännös 2 Tarkoitus	28
4.2.1 Tunnistuspalvelut	28
4.2.2 Luottamuspalvelut	29
4.2.3 Arviointitoiminta	29
4.3 Säännös 3 Määritelmät	29
4.3.1 Säännös 3.1 Määräyksen määritelmät	29
4.3.2 Säännös 3.2 Tunnistus- ja luottamuspalvelulain ja eIDAS-asetusten määritelmät	30
Määräyksen luku 2 Tunnistuspalvelun tietoturva vaatimukset	32
4.4 Säännös 4 Tunnistuspalvelun tarjoajan tietoturvallisuuden hallintajärjestelmä	32
4.4.1 Säännös 4.1 Tietoturvallisuuden hallinnan standardi	32
4.4.2 Säännös 4.2 Tietoturvallisuuden hallinnan kattavuus	32
4.4.3 Riskinhallintamalli ja -prosessi	35
4.4.4 Säännös 4.1, harkitut sääntelyvaihtoehdot	36
4.5 Säännös 5 Tunnistusjärjestelmän tietoturva vaatimukset	37
4.5.1 Yleistä	37
4.5.2 Tunnistusjärjestelmän kokonaisuus (arkkitehtuuri ja alihankkijat)	38
4.5.3 Säännös 5.1.1 Tunnistusjärjestelmän suojautumiskyky	39
4.5.4 Säännös 5.1.2 Säännösten 5 ja 7 salausvaatimusten suhde	39
4.5.5 Säännös 5.2 Tietoliikenneturvallisuus	40
4.5.6 Säännös 5.3 Tietojärjestelmäturvallisuus	41
4.5.7 Säännös 5.4 Käyttöturvallisuus	42
4.5.8 Säännös 5.5 Tunnistusjärjestelmän tuotantoverkon hallinta- ja etäyhteydet	44
4.5.9 Säännös 5, harkitut sääntelyvaihtoehdot	45
4.5.9.1 Korkean varmuustason vaatimukset	45
4.5.9.2 Eriyttämisvaatimukset tietoturva toimenpiteenä	46
4.5.10 Tunnistusjärjestelmän kellonajan luotettavuus	46
4.6 Säännös 6 Tunnistusmenetelmän tietoturva vaatimukset	46
4.6.1 Säännös 6.1 Tunnistusmenetelmän ominaispiirteet ja suojautumiskyky	46
4.6.1.1 Säännös 6.1.1 Eritelty riskiarvio	46
4.6.1.2 Riskiarviossa huomioitavia uhkia	48
4.6.1.3 Todentamistekijöiden tyypilliset uhat	49
4.6.1.4 Todentamismekanismi (autentikointi)	50
4.6.1.5 Turvatoimenpiteet	51
4.6.1.6 Riskiarvio ja hyökkäys potentiaali	53
4.6.1.7 Säännös 6.1.2 Todentamistekijöiden riippumattomuus	54

20.5.2022

4.6.1.8	Säännös 6.1.3 Tunnistusmenetelmän ja todentamisen salausvaatimukset	54
4.6.2	Säännös 6.2 Erityiset turvatoimenpiteet	55
4.6.2.1	Säännös 6.2.1 Asiointitapahtuman yksilöintitiedon näyttäminen käyttäjälle (session binding)	55
4.6.2.2	Säännös 6.2.2 Luottavan osapuolen nimen näyttäminen käyttäjälle (SP-name)	55
4.6.2.3	Säännös 6.2.3 Kertakirjautuminen (SSO)	56
4.6.3	Säännös 6.3 Tunnistusvälineen kytkeminen henkilöön	57
4.6.4	Säännös 6.4 Tunnistusmenetelmän haltijakohtaisten tietojen käsittely	58
4.6.5	Harkitut sääntelyvaihtoehdot, säännös 6.1 tunnistusmenetelmän turvallisuusvaatimukset	59
4.6.6	Säännös 6 ja Tunnistus- ja luottamuspalvelulain/varmuustasoasetuksen ja PSD2-sääntelyn yhteensopivuus	60
4.7	Säännös 7 Tunnistusjärjestelmän rajapintojen salausvaatimukset	61
4.7.1	Säännös 7.1 Tietoliikenteen salausmenetelmät	61
4.7.1.1	Yleistä	61
4.7.1.2	Säännös 7.1.1 pakolliset salausmenetelmät	62
4.7.1.3	Suositus säännöksen 7.1.1 tiukennuksista korkean varmuustason tunnistuspalvelussa	63
4.7.1.4	Säännös 7.1.2 sallitut NSCA:n ja SOGIS MRA:n arvioimat salausmenetelmät	64
4.7.1.5	Säännös 7.1.3 asetusten pakottaminen	64
4.7.2	Säännös 7.2. Tietoliikenteen salausprotokolla (TLS)	65
4.7.3	TLS 1.2 ja TLS 1.3 salausprofiilit	65
4.7.4	Lähteet kansallisesti tai kansainvälisesti suositelluista salausratkaisuksista	66
4.8	Säännös 8 Tietoliikenteen osapuolten varmentaminen	67
4.8.1	Yleistä	67
4.8.2	Säännös 8.1 Tietoliikenneyhteyden osapuolten tunnistaminen	68
4.8.3	Säännös 8.2 Varmenteiden ja avainten uusiminen	69
4.8.4	Yhteenveto säännöksen 8.2 teknisestä soveltamisesta	71
4.8.5	Säännöksen 8 tavoitteet ja vaikutusarviointi	72
4.8.5.1	Tavoitteet	72
4.8.5.2	Tiukennus standardien peruskäytäntöihin	72
4.8.5.3	Luottamusverkoston ja luottavien osapuolten ero	73
4.8.5.4	Luottamussuhteen perustaminen ja avaimen toimittaminen	73
4.8.5.5	Luottavan osapuolen eli asiointipalvelun järjestelmien koventamisvaatimukset	74
4.8.6	Säännös 8.2, teknisen soveltamisen vaihtoehtojen arviointi	75
4.9	Säännös 9 Tunnistussanomien eheys ja luottamuksellisuus	76
4.9.1	Säännös 9.1 Sanomien suojaaminen tunnistuspalveluiden ja luottavan osapuolen välillä	76
4.9.2	Säännös 9.1, vaikutukset ja toteutettavuus	77

20.5.2022

4.9.3	Säännös 9.1.2 tunnistussanomien allekirjoitus	77
4.9.4	Säännös 9.2 Sanomien salaaminen käyttäjärajapinnassa	78
4.9.5	Säännös 9.3 Salausalgoritmit ja menettelyt	79
4.10	Säännös 10 Tietoturva-vaatimukset kansallisen solmupisteen rajapinnassa ...	80
4.11	Säännös 11 Tunnistuspalveluntarjoajan häiriöilmoitukset Liikenne- ja viestintävirastolle	80
4.11.1	Säännös 11.1 Merkittävät uhkat tai häiriöt (ilmoituskynnys)	80
4.11.2	Säännös 11.2 Ilmoitettavat tiedot	82
4.11.3	Säännös 11.3 Ilmoitusmenettely	82
4.11.4	Säännös 11, harkitut sääntelyvaihtoehdot ja muut ohjauskeinot	83
	Määräyksen luku 3 Tunnistuspalveluiden yhteentoimivuus	83
4.12	Säännös 12 Luottamusverkostossa välitettävät vähimmäistiedot	83
4.12.1	Säännös 12.1 Pakolliset tiedot (attribuutit)	83
4.12.2	Yleistä	83
4.12.3	Uusi attribuutti: luottavan osapuolen nimi	84
4.12.4	Säännös 12.2 Valinnaiset tiedot	85
4.12.5	Säännös 12.3. Tunnistuksen pseudonymisointi ("köyhdyttäminen")	86
4.12.6	Säännös 12, harkitut sääntelyvaihtoehdot	87
4.12.6.1	Uudet valinnaiset attribuutit	87
4.12.6.2	Ensimmäisen tunnistamisen attribuutit	88
4.13	Säännös 13 Rajat ylittävän tunnistamisen edellyttämät tiedot	90
4.13.1	Tunnistus julkisella sektorilla	90
4.13.2	Tunnistus yksityisellä sektorilla	90
4.14	Säännös 14 Tiedonsiirrossa käytettävä protokolla ja muut vaatimukset	91
4.14.1	Säännös 14.1 Tiedonsiirrossa käytettävä protokolla	91
4.14.2	Säännös 14.2 Rajapinnan muut ominaisuudet	92
4.14.3	Uusien protokollastandardien käyttöönotto luottamusverkostossa	92
	Määräyksen luku 4 Tunnistuspalvelun arviointikriteerit	93
4.15	Säännös 15 Vaatimustenmukaisuuden arviointikriteerit	93
4.15.1	Säännös 15.1 Tunnistusjärjestelmän ja tunnistusmenetelmän arvioitavat toiminnot	93
4.15.2	Säännös 15.2 Arviointikriteeristö	95
4.15.3	Esimerkkejä arviointilähteistä	96
4.15.4	Määräykselle vaihtoehtoiset ohjauskeinot ja viraston arviointiohje	97
4.16	Säännös 16 Selvitys tunnistuspalvelun tarjoajan ja julkaistujen tietojen luotettavuudesta	97
4.16.1	Tunnistuspalvelun ilmoitusvelvollisuuteen liittyvät selvitykset	97
4.16.2	Selvitettävät tiedot	97
4.16.3	Viraston ilmoitusohje	98

20.5.2022

4.17 Säännös 17 Kansallisen solmupisteen arviointiperusteet	98
Määräyksen luku 5 Tunnistuspalvelun arviointielimen pätevyys	98
4.18 Säännös 18 Tunnistuspalvelun ulkoisen arviointielimen vaatimukset	98
4.19 Säännös 19 Tunnistuspalvelun sisäisen tarkastuslaitoksen vaatimukset.....	99
Määräyksen luku 6 Hyväksytyt luottamuspalvelut.....	99
4.20 Säännös 20 Hyväksytyn luottamuspalvelun tarjoajan arviointikriteerit.....	99
4.20.1 Yleistä luottamuspalveluiden sääntelystä ja standardeista	99
4.20.2 Hyväksytyn luottamuspalvelun tarjoajan yleiset ja palvelukohtaiset vaatimukset	100
4.20.2.1 Säännös 20.1.1 Hyväksytyn luottamuspalvelun tarjoajan yleiset vaatimukset.....	100
4.20.2.2 Säännös 20.1.2 Hyväksytyn varmenteen tarjoajan lisävaatimukset	100
4.20.2.3 Säännös 20.1.3 Hyväksytyn aikaleiman tarjoajan lisävaatimukset	101
4.21 Säännös 21 Hyväksytyn luottamuspalvelun arviointikriteerit.....	101
4.21.1 Hyväksytyt luottamuspalvelutyypit.....	101
4.21.2 Standardit	102
Määräyksen luku 7 Luottamuspalvelujen vaatimustenmukaisuuden arviointilaitokset	103
4.22 Säännös 22 Arviointilaitosten pätevyyden arviointi	103
4.22.1 Akkreditointi ja hyväksyntä	103
4.22.2 Standardi.....	104
4.22.3 Arviointikertomus	105
Määräyksen luku 8 Hyväksytyn sähköisen allekirjoituksen ja sähköisen leiman luontivälineen sertifiointi	105
4.23 Säännös 23 Sähköisen allekirjoituksen tai leiman luontivälineen sertifiointilaitos	105
4.23.1 Pätevyysvaatimukset	105
4.23.2 Standardit	106
Määräyksen luku 9 Siirtymäsäännökset ja allekirjoitukset	106
4.24 Säännös 24 Määräyksen voimaantulo ja siirtymäsäännökset	106
4.24.1 Säännöksen 6.2 ja 12.1 siirtymäaika.....	106
4.24.2 Säännöksen 8 siirtymäajat.....	107
4.24.3 Säännöksen 9 siirtymäajat.....	108
5 Liitteet ja viitteet.....	109
5.1 Viiteluettelo	109

1 Määräyksen tausta ja säädösperusta

1.1 Määräyshistoria ja päivittämisen syyt

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

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

Nykyuotoinen tunnistus- ja luottamuspalvelumääräys on annettu alun perin 2.11.2016 EU:n eIDAS-asetuksen (EU) 910/2014 voimaantulon yhteydessä kansallisen ja EU-sääntelyn yhdenmukaistamiseksi ja yhteensovittamiseksi 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 nykyuotoisen 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. Laatuvarmenteille (eIDAS-asetuksen termi on hyväksytty varmenteet) 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]

1.3 Asiaan liittyviä muita määräyksiä ja säädöksiä

1.3.1 Sähköinen tunnistaminen

Valtioneuvoston asetus vahvan sähköisen tunnistuspalvelun tarjoajien luottamusverkostosta 169/2016, muutettu 1212/2018 (nk. luottamusverkostoasetus) [2]

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) [3]

Sähköisten luottamuspalveluiden, akkreditoitujen vaatimustenmukaisuuden 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.

20.5.2022

*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 [4]*

EU:n varmuustasoasetuksessa säädetään tunnistusmenetelmien varmuustasojen vaatimukset. Asetusta sovelletaan niihin tunnistusvälineisiin, jotka notifioidaan EU:n komissiolle. Tunnistus- ja luottamuspalvelulaissa viitataan monissa 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 [5]*

EU:n yhteentoimivuusasetus koskee ensisijaisesti Digi- ja väestötietoviraston 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 [6]*

EU:n notifiointimenettelypäätöksessä määritellään notifiointinissa ilmoitettavat tiedot ja menettely. Tunnistusmenetelmän (tunnistusvälineen) notifiointin komissiolle ja muille jäsenvaltioille tekee Liikenne- ja 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 [7]*

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

1.3.2 Sähköisen allekirjoituksen ja leiman luontiväline

*Komission täytäntöönpanopäätös (EU) 2016/650, annettu 25 päivänä huhtikuuta 2016, **hyväksytyjen allekirjoituksen ja leiman luontivälineiden tietoturva-arviointia** 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 [8]*

20.5.2022

Komission täytäntöönpanopäätöksessä säädetään sähköisen allekirjoituksen ja leiman luontivälineen sertifiointin vaatimuksista. Säädös liittyy määräyksen säännökseen 23.

1.3.3 Henkilötiedot

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) [9]

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) [10] 29 §:n 4 momentissa käsitellään henkilötunnuksen esittämistä:

*Henkilötunnusta ei tule merkitä tarpeettomasti henkilörekisterin perusteella tu-
lostettuihin 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.

20.5.2022

Tunnistus- ja luottamuspalveluiden asiakkaiden kannalta sääntelyllä huolehditaan tietoturvasta ja yksityisyyden suojaamisesta oletusarvoisesti. 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. Vaiikutuksia 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 siirtymäaika.

Säännös 5 Tunnistusjärjestelmän tietoturva-vaatimukset

Säännös 5.1 Tunnistusjärjestelmän suojautumiskyky on uusi.

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

Sähköisen tunnistamisen varmuustasoasetuksen 2.4.6 kohdan mukaan edellytettujen turvatoimenpiteiden eli teknisten kontrollien vaatimustaso määritellään varmuustasoasetuksen 2.3.1 kohdan hyökkäyspotentiaaliin 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. Hyvien salauskäytäntöjen vaatimusta ja suhdetta säännöksen 7 salausvaatimuksiin selkeytetään. Tiedon säilyttämisen turvallisuusvaatimus 7 §:stä on siirretty säännökseen 5.4.

Säännöksen 5 muutokset eivät edellytä siirtymäaika.

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 tietoturva-vaatimukset

Säännös 6.1 Tunnistusmenetelmän ominaispiirteet ja suojausominaisuudet on uusi.

Tarkoitus on yhdenmukaistaa ja parantaa tunnistusmenetelmien turvallisuuden vähimmäistasoa ja niihin tehtävien muutosten arviointia. Tunnistusmenetelmät kehittyvät jatkuvasti ja myös tietoturva-vaatimukset 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 ennakkolisesti eikä vasta mahdollisen häiriön tapahduttua.

Määräykseen lisätään tarkennus tunnistusmenetelmän suojausominaisuuksien vaatimustasosta. Tulkinnallisesti vaatimus olisi johdettavissa myös laista, mutta asiaa halutaan selkeyttää määräyksessä. (Vrt. säännöksen 5 vastaava muutos). Suojausominaisuuksien vaatimusta tarkennetaan viittauksella varmuustasoa-asetukseen ja lisätaamalla määräyksessä osatekijöitä, joita riski- ja uhka-arvioinnissa on huomioitava.

Virasto arvioi, että tällainen sääntelymalli on tarpeeksi joustava, jotta tunnistuspalvelut voivat kehittää tunnistusmenetelmiään. Malli 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 suojausominaisuuksien vaatimukset standardiviittauksella. Todentamistekijäkohtaiseen sääntelytapaan liittyisi todentamistekijöiden moninaisuuden ja kehittymisen takia paljon yksityiskohtia, joita ei ole viraston arvion mukaan mahdollista eikä tarkoituksenmukaista pyrkiä kattamaan ennakoivasti säännösten tasolla. Myöskään uhkat tunnistusmenetelmän turvallisuudelle ja turvakeinot uhkilta suojaamiselle eivät ole puhtaasti todentamistekijätyypikohtaisia. Suojausominaisuuksien mittareita tai muunlaisia tarkennuksia määräyksessä voisi ajatella standardien perusteella, mutta tiedossa ei kuitenkaan ole sellaista yleispätevää standardia, jonka perusteella voisi yleispätevästi määrätä pakottavat vaatimukset.

Säännös 6.2 Erityiset turvatoimenpiteet on uusi.

20.5.2022

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 asiointipahtuman ja tunnistuspyynnön ja välttää vahvistamatta oikeudettomat tunnistuspyynnot.

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.

Säännös 6.2.3 kertakirjautumisesta on uusi.

Määräykseen lisätään säännös (6.2.3) **kertakirjautumisen turvallisuusvaatimuksesta**: 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.

Säännösten 6.2.1 ja 6.2.2 vaatimusten toteuttamiselle annetaan siirtymäaika.

Säännös 7 Tunnistusjärjestelmän ja rajapintojen salausvaatimukset

Säännös 7.1 Tietoliikenteen salausmenetelmät

Määräyksen luettelo tietoliikenteen salauksessa kelpaavista salausmenetelmistä ja algoritmeista (7.1.1) täydennetään teknisen kehityksen takia. Säännöstä tarkennetaan siten, että se soveltuu myös säännöksessä 9 määrättävään sanomien salaamiseen. Säännöksestä 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 menetelyjen 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 sidosryhmäpalauteen perusteella on, että siirtymäaika vaatimukselle ei tarvita. TLS 1.2 -versioon on laajalti siirrytty jo edellisen siirtymän yhteydessä ja päätelaitekanta tukee sitä.

Säännöksen 7 muutokset eivät edellytä siirtymäaika.

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 pakolliseksikaan 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

Säännöksen 8 vaatimusten tarkennukset ja niiden ulottaminen luottaviin osapuoliin on määräyksen suurin ja vaikuttavin muutos.

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 niiden luotettavuudesta riippumatta. Vaatimusten toteuttaminen edellyttää prosessien määrittelyä avainten ja varmenteiden toimittamisessa ja erilaisia asetusten määrittelyä 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 varata siirtymäaika etenkin suhteessa asiointipalveluihin ja muutosten läpivieminen edellyttää yhteistyötä neuvonnassa ja viestinnässä.

Virasto arvioi, että säännöksen 8 muutokset edellyttävät siirtymäaika, 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 -protokollaa 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 ovat sidoksissa säännöksen 8 vaatimuksiin ja siten siirtymäajat vastaavat säännöksen 8 siirtymäaikoja.

Säännös 11 Tunnistuspalvelun tarjoajan 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. Tältä osin arviota ei muuteta vuonna 2016 tehdystä arviosta. On myös huomattava, että tunnistus- ja luottamuspalvelulaissa 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 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 pseudonymistista 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 esimerkiksi häiriötilanteita selvitetäessä.

Säännöksen 12 muutokset eivät pääosin edellytä siirtymäaika. 12.1 mukaisen luottavan osapuolen nimen käsittely liittyy määräyksen säännöksen 6.2.2 toteuttamiseen ja siirtymäaika on siten sama.

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

Säännös 14 Tiedonsiirrossa käytettävä protokolla ja muut vaatimukset

Säännöstä 14.1 Tiedonsiirrossa käytettävä protokolla on tarkennettu nimeämällä OpenID Connect ja SAML standardeiksi, joista jommankumman mukaista rajapintaa tunnistuspalvelun on vähintään tarjottava tunnistus- ja luottamuspalvelulain 17 §:n mukaisen ensitunnistamisen ketjuttamiseen tunnistusvälineen tarjoajien välillä ja tunnistus- ja luottamuspalvelulain 12 a §:n mukaiseen tunnistusvälitykseen tunnistusvälineen 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.

20.5.2022

Mahdollistaminen tarkoittaa säännöksessä sitä, että vaatimusta tulkitaan ensitunnistamisen tai luottavalle osapuolelle välitettävän tunnistustapahtuman vastaanottajan oikeuden näkökulmasta. Tunnistuspalvelu voi täyttää velvoitteensa tarjoamalla toiminnon toisen luottamusverkoston tunnistuspalvelun kautta, kunhan säädetyt ja määrättyt 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 luvussa 3 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 vahvan sähköisen tunnistuspalvelun ilmoitusvelvollisuuteen toiminnan aloittamisesta ja muutoksista tunnistus- ja luottamuspalvelulain 10 §:ssä. Säännöksen tarkoitus on myös selkeyttää niitä tietoja, joita ei koske säännöksen 15 riippumaton ja pätevä säännöllinen vaatimustenmukaisuuden arviointi. Säännöstä on täydennetty ja muokattu valvonta- ja neuvontakäytännön mukaisesti.

Säännöksen 16 muutokset eivät edellytä siirtymäaikaa.

Säännös 21 Hyväksytyn luottamuspalvelun arviointikriteerit

Säännöksellä määrätään hyväksytyjen 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 sähköisen 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 yhteissäntelyllä. 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 tietoturvasuus-, 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 luottamuspalvelun tarjoajia, ICT-toimijoita, viranomaisia ja jonkin verran sähköisten asiointipalveluiden tarjoajia, jotka käyttävät tunnistus- ja luottamuspalveluita. Kaikki valmistelumateriaalit on julkaistu viraston verkkosivulla.

Lausuntopyyntö on toimitettu 10.11.2021 samoilla jakeluilla ja julkaistu valtionhallinnon lausuntopalvelussa. Lausuntopalautteesta pidettiin 9.3.2022 palautetilaisuus, jossa vielä oli mahdollisuus selventää lausunnoissa esitettyä ja kommentoida viraston lausunnoista tekemiä päätelmiä.

Määräys koskee tietoyhteiskunnan palveluja ja se on notifioitu EU:n nk. transparensisidirektiivin (EU) 2015/1535¹ mukaisesti 22.11.2021 (ilmoitus 2021/792/FIN). Notifioinnin odotusaika päättyi 23.2.2022 eikä notifiointiin tullut palautetta.

3.2 Lausuntopalaute

Lausunnon määräysehdotuksesta ja perustelumuistiosta antoivat Digi- ja väestötietovirasto (DVV), Finanssiala ry, Nixu Certification Oy, Signicat AS, S-Pankki Oyj ja Tietosuojavaltuutettu.

Mobiilivarmentajat eivät lausuneet määräysehdotuksesta, mutta virasto toteaa, että niiden edustajat olivat valmistelussa mukana.

3.2.1 Yleinen palaute ja henkilötietojen suoja

Määräyksen päivittämistä pidettiin lausunnoissa tarpeellisena.

¹ EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI (EU) 2015/1535, annettu 9 päivänä syyskuuta 2015, teknisiä määräyksiä ja tietoyhteiskunnan palveluja koskevia määräyksiä koskevien tietojen toimittamisessa noudatettavasta menettelystä

20.5.2022

Finanssiala katsoi, että määräyksen päivittäminen on perusteltua, koska vaatimusten soveltaminen on edellyttänyt jatkuvaa keskustelua työryhmissä. Finanssiala katsoi kuitenkin, että kaikkia toimialan huolia ei ole ymmärretty tai huomioitu ja uusi määräys aiheuttaa kustannuksia, joita on hintasäännellyssä markkinassa vaikeata tai mahdotonta kattaa tunnistuspalveluiden tuloilla.

DVV katsoi, että yleisellä tasolla määräys sisältää hyviä tarkennuksia ja tärkeitä päivityksiä mm. käytettyihin algoritmeihin. DVV piti hyvänä termin asiointipalvelu korvaamista johdonmukaisesti eIDAS-asetuksen 3 artiklan kanssa yhdenmukaisella määritelmällä luottava osapuoli.

Nixu korosti muun ohjauksen ja neuvonnan tärkeyttä erityisesti arviointitoiminnan kannalta ja totesi, että ohjaus on kehittynyt hyvin vuoden 2016 lähtötilanteeseen nähden.

Tietosuojavalvutettu katsoi lausunnossaan, että tunnistusjärjestelmissä ja tunnistuspalveluissa käsiteltävät henkilötiedot sekä ylipäänsä tunnistamiseen liittyvä yksityisyydensuojan tarve ovat luonteeltaan sellaisia, että on hyvin tärkeää, että tietojen ja niiden käsittelyn eheys, luottamuksellisuus ja turvallisuus on varmistettu korkeatasoisesti. Tietosuojavalvutettu piti mahdollisten epäselvyyksien ja aukkojen tarkentamista tärkeänä ja tarpeellisena ja palveluiden tietosuojan tasoa sekä käsittelyn turvallisuutta lisääviä muutoksia kannatettavina.

Tietosuojavalvutettu totesi, että suhteessa PSD2-sääntelyyn olennaista on se, että sääntelyt eivät ole keskenään ristiriidassa, kuten määräyksessä on katsottu. Kumman tahansa sääntelyn kautta tulevat täydentävät vaatimukset suhteessa toiseen sääntelyyn ovat palveluiden tietosuojan kannalta positiivinen asia.

3.2.2 Säännös 4.1 Tietoturvallisuuden hallinnan standardi (4 Tunnistuspalvelun tietoturvallisuuden hallintajärjestelmä)

Nixu katsoo, että säännös tiukentaa ISO 27001:n tai muun standardin noudattamisen velvoitetta ja pitää vaatimusta hyvänä. Nixu katsoo muutoksen lisäävän auditointien työmäärää ja nostavan alalle tulon kynnystä, mutta ei pidä tätä kovin merkittävänä.

Finanssiala katsoo, että perustelujen valossa muutos vaikuttaa sanamuodon muutosta merkittävämmältä. Kun noudatettavaa standardia ei ole määritelty määräyksessä, Finanssiala näkee riskin, että vaatimustenmukaisuutta noudatetaan epäyhdenmukaisesti. Toisaalta Finanssiala pitää epäselvänä, onko jatkossa käytännön edellytys tietoturvallisuuden hallintajärjestelmän sertifiointi, ja arvioi, että edellytys vaikuttaa organisaation tietoturvallisuuden hallintajärjestelmään, ja yhteensovittaminen toimijan nykyiseen kehikkoon aiheuttaa uusia lisäkustannuksia toiminnalle.

Tietosuojavalvutettu katsoo, että tietoturvallisuuden hallintaa koskevien vaatimusten täsmentäminen on tietosuojanäkökulmasta positiivinen kehityssuunta.

Traficomin arvio:

Traficom viittaa soveltamisen osalta perustelumuistion kohtaan 4.1.1.

Traficom toteaa selvyyden vuoksi, että vaatimus tietoturvallisuuden hallintajärjestelmästä ei ole uusi, vaan säädetty laissa jo vuonna 2016 viittauksella varmuustasoasetukseen.

Traficom katsoo, että perusteluissa vastataan lausunnoissa esille nostettuihin kysymyksiin. Sertifiointia ei määrätä pakolliseksi edes korkealla varmuustasolla. Säännöksen sanamuoto vastaa lakia. Tarkoitus on tiukentaa vaatimuksen soveltamista hienoisesti ja korostaa tunnistuspalvelun tarjoajan johdon sitoutumisen merkitystä ja tietoturvallisuuden hallintajärjestelmän ja prosessien ylläpidon merkitystä, mutta sallia edelleen muutkin standardit kuin ISO 27001.

3.2.3 Säännös 5 Tunnistusjärjestelmän tietoturva-vaatimukset

Nixu katsoo, että luvussa 2 tehdyt muutokset, esim. 5.4.d), selkeyttävät myös arviointia.

Nixu katsoo kuitenkin, että säännökseen 5 vain joihinkin kohtiin lisätyt adjektiivit (hyvin, huolellisesti) voivat aiheuttaa vääriä tulkintoja siitä, että huolellisuus ei koskisi kaikkia kohtia. Nixu ehdottaa, että kaikkien vaatimusten täyttämisen edellytyksenä huolellisuutta ja hyvää tapaa tehdä asioita, ei vain niissä, joissa se on mainittu.

Traficom arvio:

Säännökseen 5 on lisätty kohta 5.1.1, joka edellyttää suojautumiskykyä kohtuullisen tai korkean vakavuustason uhkaa ja hyökkäyspotentiaalia vastaan. Suojautumiskyky edellyttää Traficom näkemyksen mukaan huolellisuutta ja hyvien käytäntöjen noudattamista kaikissa vaatimuksissa.

Traficom poistaa sanan "huolellinen" määräyksen säännöksestä 5.4.a) huolellinen muutosten hallinta. Muut määritteet on poistettu jo valmistelun aikana.

Traficom lisää perustelumuistion kohtaan 4.5.3 (Säännös 5.1.1 Tunnistusjärjestelmän suojautumiskyky): Kaikissa toimissa on noudatettava huolellisuutta ja hyviä käytäntöjä.

3.2.4 Säännös 5.5 Tunnistusjärjestelmän tuotantoverkon hallinta- ja etäyhteydet

Säännökseen ei ollut esitetty muutoksia.

DVV katsoo, että tuotantoverkkoa ei ole riittävällä tarkkuudella määritelty ja on epäselvää, ovatko esimerkiksi asiakastietojärjestelmien käyttöön tarkoitetut työasemat osa tuotantoverkkoa vai viittaako tuotantoverkko vain tunnistusvälineen käytön yhteydessä aktiivisiin komponentteihin ja niiden hallintatyöasemiin. Jälkimmäisten tapauksessa DVV pitää vaatimuksia oikein mitoitettuna, mutta asiakastietojärjestelmien osalta korkealla tasolla ylimitoitettuna.

Traficom arvio:

Traficom toteaa, että siltä osin, kun asiakastietojärjestelmillä tarkoitetaan järjestelmiä, joilla rekisteröidään uusia tunnistusvälineitä tai uudelleenaktivoidaan suljettuja välineitä, ne on katsottava tuotantoverkoksi.

Traficom lisää tuotantoverkon määritelmän perustelumuistion kohtaan 4.5.8 (Säännös 5.5 Tunnistusjärjestelmän tuotantoverkon hallinta- ja etäyhteydet).

Traficom toteaa vielä, että vaatimuksessa on jo 2016 eritelty korotettu ja korkea varmuustaso, jotta se olisi suhteellinen. Nyt määräyksen säännöksessä 5.1.1 selvennetään, että vaatimustaso perustuu korkealla varmuustasolla siihen, että järjestelmän tulee kyetä suojautumaan korkean vakavuustason uhkaa ja hyökkäyspotentiaalia vastaan.

3.2.5 Säännös 6.1 Tunnistusmenetelmän ominaispiirteet ja suojautumiskyky

Finanssiala, Nixu ja Tietosuojavaltuutettu lausuivat säännöksestä.

20.5.2022

Tietosuojavaltuutettu kiinnitti huomiota siihen, että on tärkeää, että toimijat arvioivat henkilötietojen käsittelyn riskejä myös tietosuoja-asetuksen 35 artiklan mukaisen vaikutustenarvioinnin tarpeen näkökulmasta. Tunnistuspalveluihin saattaa liittyä esimerkiksi kasvojen- ja sormenjälkitunnistusta ym. biometristen tietojen käsittelyä.

Nixu piti vaadittuja asioita riskiarvioista hyvinä.

Finanssiala piti tunnistusmenetelmän riskiarviovaatimuksessa hyvänä sitä, että se tulisi voimaan samanaikaisesti kaikille ja tarjoaa työvälineitä verkoston toimijoille arvioida omaa toimintaansa ja antaa viranomaisille tukea valvontaan. Finanssiala katsoi kuitenkin, että riskiarviokehikon ollessa uudistuksessa säädellyllä tavalla avoin, vertailu toimijoiden välisten riskiarvioiden ja teknisten kontrollien välillä voi olla auditoijalle ja viranomaisen valvonnalle haastavaa.

Finanssiala katsoi, että vaatimus riskiarviosta tulee lisäämään tunnistuspalvelun tarjoamisessa vaadittavan työn määrää ja kustannuksia ja totesi, että aiemmin käytössä ollut riskiarviokehikko täytyy sijoittaa uusien vaatimusten mukaiseen kehikoon.

Traficomin arvio:

Traficom toteaa, että Tietosuojavaltuutetun muistutus mahdollisesta yleisen tietosuoja-asetuksen vaikutustenarvioinnista on hyvä ja sitä voi soveltuvin osin hyödyntää osana tunnistusmenetelmän riskiarviota.

Traficom toteaa, että Finanssiala tuo hyvin esiin riskiarvion valitun joustavan sääntelytavan hyvät ja huonot puolet. Perustelumuistion kohdassa 4.6.1.1 on todettukin, että määräyksen erityinen vaatimus voi tarkentaa arvioinnin vaatimuksia ja lisätä dokumentointivaatimuksia. Traficom toteaa kuitenkin, että määräyksen sidosryhmävalmistelussa tulleen toimijoiden palautteen perusteella tunnistusmenetelmän riskiarviovaatimukselle ei tarvita siirtymäaikaa ja riskiarviointi on yleisellä tasolla ollut vaatimuksena tähänkin saakka.

3.2.6 Säännös 6.2.1 Tunnistusmenetelmän erityiset turvatoimenpiteet (session binding)

Finanssiala ja Signicat lausuivat säännöksestä.

Finanssiala ehdotti sanamuodon selkeyttämistä, jotta vaatimus on ymmärrettävä ilman perustelujen lukemista ja katsoi lisäksi, että termi yhdistää viittaa liiaksi PSD2-säädökseen. Ehdotettu sanamuoto: "Tunnistuspalvelun on näytettävä tunnistusvälineen käyttäjälle tunnistustapahtumassa tieto, jonka perusteella käyttäjä voi varmistaa tunnistusvälineeseen saamansa tunnistuspyynnön liittyvän käyttäjän omaan asiointitapahtumaan".

Signicat kommentoi, että esitettävä tieto olisi tyypillisesti tekstiä ja että sen esittäminen on tunnistusvälineen tarjoajan tehtävä. Signicat katsoi kuitenkin, että on tilanteita, joissa tunnistusvälityspalvelun olisi tarpeellista näyttää tieto verkkosivulla (web interface). Signicat ehdottaa siksi, että määräyksen säännöksen 12.2 valinnaisiin attribuutteihin lisättäisiin tekstikenttä, jolla tunnistusvälityspalvelu voi toimittaa tiedon tunnistusvälityspalvelulle näytettäväksi käyttäjälle.

Traficomin arvio:

Traficom kiittää tekstiehdotuksesta. Säännös muutetaan muotoon: "Tunnistuspalvelun on näytettävä tunnistusvälineen käyttäjälle tunnistustapahtumassa tieto, jonka perusteella käyttäjä voi varmistaa, että tunnistusvälineeseen käyttäjän saama tunnistuspyyntö liittyy käyttäjän omaan asiointitapahtumaan."

Signicatin kommentista Traficom toteaa, että session binding -tieto voi olla tekstiä, QR-koodi tai jokin muu.

Muusta asiointitapahtumaan liittyvästä tiedosta Traficom arvioi, että uusi valinnainen attribuutti määräyksen säännökseen 12.2, johon liittyy vain tekninen suunnitteluvelvoite, ei välttämättä edistä yhteentoimivien attribuuttitietojen käyttämistä. Traficom katsoo, että asiointitapahtumien sisältöön (pääsynhallintaan, maksuihin, allekirjoitukseen, sopimuksiin jne.) liittyvä informointi ei kuulu Traficomin määräystoimivaltaan ja luottamusverkon sääntelyssä on vältettävä ratkaisuja, joista syntyy käsitys, että sääntely ottaa kantaa asioinnin PSD2-mukaisuuteen. Traficomin rajapintasuosituksissa voidaan kuitenkin tarkastella vapaatekstikenttien lisäämistä ja niiden käyttö on tunnistus- ja luottamuspalvelulakiin ja määräykseen nähden katsottava varsinaiseen tunnistamiseen liittymättömiksi nk. rikastamistiedoiksi. Traficom toteaa myös, että tunnistuspalvelun tarjoajat voivat keskinäisillä sopimuksilla ottaa ylimääräisiä attribuutteja käyttöön ilman Traficomin määräystä ja suositusta.

3.2.7 Säännös 6.2.2 (SPname)

DVV ja Signicat lausuivat säännöksestä. Kumpikin piti sitä tärkeänä parannuksena.

3.2.8 Säännös 6.2.3 Kertakirjautuminen

Finanassiala ja Signicat lausuivat säännöksestä.

Signicat totesi kannattavansa ehdotusta, kunhan kertakirjautumisen tarjoaminen (provisioning) ei ole pakollista.

Finanssiala katsoi, että istunnolle olisi hyvä määritellä enimmäiskesto, jotta määräyksen kohdalla olisi merkitystä palveluita suunniteltaessa.

Traficomin arvio:

Kertakirjautumisen tarjoaminen ei ole pakollista.

Traficom katsoo, että enimmäiskeston määrittely on tarkoituksenmukaisempaa tehdä muulla tavalla kuin määräyksessä.

Kertakirjautumisesta on tehty vuosina 2017–2020 määrittelytyötä luottamusverkon yhteistoimintaryhmän tätä varten toimineessa teknisessä alatyöryhmässä. Selvityksen tulosta ei ole vahvistettu, mutta aikavalvontoja on tarkasteltu. Selvitysluonnoksessa (kohta 4.2) on todettu, että *on hankala määritellä yhtä tiettyä enimmäisai- kaa kertakirjautumisistunnon kestolle (oikeastaan ajalle, jonka kuluttua edellytetään uutta tunnistautumista istunnon virkistämiseksi), koska asiointitapahtumat ovat si- sällöltään ja kestoiltaan erilaisia. Virkistämättömän kertakirjautumisistunnon enim- mäiskesto on mahdollista mukauttaa tilanteeseen, jossa kertakirjautumista käyte- tään. ...Lähtökohtaisesti hyvänä käytäntönä pidetään, että välityspalvelu pitää virkis- tämätöntä kertakirjautumisistuntoa voimassa pisimmillään enintään 30 minuuttia tunnistusvälineen käyttämisestä eli asiakkaan tunnistamisesta lukien.*

3.2.9 Säännös 7 Tunnistusjärjestelmän rajapintojen salausvaatimukset ja muut salausasiat

Määräyksen säännöksen 7.1.1 algoritmilistan päivitystä kommentoivat DVV ja Nixu. Kumpikin kannatti sitä, joskin Nixu toisti valmisteluvaiheessa esittämänsä näkemyk- sen, että sallittujen algoritmien listaaminen määräyksessä ei ole tarkoituksenmukai- nen ratkaisu.

20.5.2022

Nixu toi lisäksi esiin, että säännökseen 7.1.2 ehdotettu lisäys kryptoviranomaisten listojen huomioimisesta on hyvä ja jopa välttämätön. Nixu ehdottaa kyseisten listojen määrittelyä ensisijaiseksi.

Nixu huomautti lisäksi, että ehdotuksessa määrätään salausvaatimuksista monessa säännöksessä ja osassa viitataan määräyksen säännöksen 7 vaatimuksiin ja osassa suositeltaviin salausratkaisuihin. Nixu kiinnitti huomiota siihen, että ei pitäisi syntyä tilannetta, jossa sallitaan säännöstä 7 heikompi ratkaisu.

Traficomin arvio:

Traficom pitäytyy arviossa, että tarkka listaus on sääntelyn tehokkuuden takia edelleen tarpeellinen ja kryptoviranomaisten listat laaditaan eri tarkoituksiin, mistä syystä niitä ei ole sellaisenaan perusteltua asettaa ensisijaisiksi vaatimuksiksi tunnistuspalveluille. Traficom viittaa perustelumuistion kohdan 4.7.1.1 kappaleeseen *Vaihtoehtoiset sääntelytavat, 7.1 tietoliikenteen salaus*.

Traficom toteaa selvyyden vuoksi, että määräyksen säännöksissä, joissa ei viitata salausvaatimuksissa säännökseen 7, on nimenomaan arvioitu, ettei ole tarpeellista vaatia ehdottomasti säännöksen 7 menettelyä. Muutkin mahdollisesti heikommat salausmenettelyt voivat olla riittäviä, jos muut kontrollit kokonaisuutena takaavat riittävän turvallisuuden. Ks. esim. säännös 5.1.2 *...ellei suojautumiskyky kokonaisuutena arvioiden toteudu muilla turvatoimenpiteillä*.

3.2.10 Säännös 8.1 Tietoliikenneyhteyden osapuolten tunnistaminen

DVV, Finanssiala, Nixu ja Signicat lausuivat ehdotuksesta.

Nixu oli ainoa, joka kannatti säännöstä 8 varauksetta ja totesi, että avaintenhallinnan heikkoudet saattavat murentaa luottamuksen koko tunnistuspalveluun yhdellä kertaa. Nixu totesi, että vaatimuksen auditointi lisää hieman auditointien kokoa nykyisestä.

Finanssiala katsoo, että yksikään luottamusverkoston jäsen ei täytä tällä hetkellä ehdotetun määräyksen uusia vaatimuksia, asiointipalveluista puhumattakaan.

Säännöksen 8.1 avainten suhde säännöksen 9 avaimiin

Finanssiala piti epäselvänä, mitä kaikkia avaimia 8.1 koskee ja ehdottaa selvennyksenä, että jos käytössä on säännöksen 8.1 mukaiset avaimet säännöksen 9 sanomatason salauksessa, TLS-varmenteiden suhteen riittäisi yleisesti hyväksytty varmenne.

Traficomin arvio:

Traficom toteaa, että määräysehdotus on Finanssialan ehdotuksen mukainen.

Säännöksen 8.1 sääntely koskee luottamussuhteen perustamista ja sanamuodon mukaisesti vaatimus koskee joko *tietoliikenteen* (eli TLS) tai *sanomien salaamisessa käytettäviä* varmenteita ja avaimia.

Osapuolen hyväksytty sähköinen allekirjoitus tai leima (QES, QeSeal)

DVV katsoi, että eIDAS-asetuksen mukaisen hyväksytyn sähköisen allekirjoituksen ja leiman huomioiminen on hyvä kehityssuunta.

Signicat huomautti, että niiden käyttö on käytännössä vähäistä ja saatavilla olevat sertifioidut allekirjoituksen tai leiman luontivälineet (QSCD) ovat kalliita. Signicat piti

20.5.2022

vaatimusta liian tiukkana ja arvioi, että suora kahdenvälinen menettely on todennäköisempi käytännössä.

Traficomin arvio:

Traficom yhtyy arvioon, että hyväksytyjen sähköisten allekirjoitusten ja leimojen käyttö on vähäistä ja on huomattava, että sähköisen leiman varmenne olisi hankittava joltain ulkomaiselta hyväksytyn leimavarmenteen tarjoajalta. Traficom toteaa, että menettely on määräysehdotuksessa vaihtoehto ja koska se on suoraan eIDAS-asetuksen nojalla hyväksyttävissä, Traficom katsoo asianmukaiseksi todeta sen määräyksessä eikä pelkästään perusteluissa.

Traficom selventää, että määräyksessä ei rinnasteta suoran kahdenvälisen menettelyn vaatimustasoa hyväksytyyn sähköiseen allekirjoitukseen tai leimaan. Perustelumuistion kohdassa 8.4.2 käsitellään suoran kahdenvälisen menettelyn soveltamista. Menettelyjä ja mahdollisia yhteisiä käytäntöjä voidaan käsitellä luottamusverkoston yhteistoimintaryhmässä.

Osapuolen hyväksytty varmenne

DVV kritisoi sitä, että hyväksytyjä verkkosivuvarmenteita (QWAC) ei yksistään katsota riittäväksi. QWAC-varmenteita tarjoavana organisaationa DVV korosti, että hyväksytyn tason varmenteiden myöntöprosessissa määritetään erittäin yksityiskohtaisesti, kuinka varmenteen hakija tulee tunnistaa varmenteen myöntämiseksi. DVV huomautti, että luottamusverkoston toimijoita valvotaan kuten PSD2-sääntelyn toimijoita.

Signicat katsoi samansuuntaisesti, että ainakin eIDAS-asetuksen mukainen hyväksytyn varmenteen (sähköisen leiman varmenteen) tulisi yksinään olla hyväksyttävä ja tämä olisi linjassa PSD2-sääntelyn kanssa. eIDAS hyväksytyn varmenteen vaatimustakin Signicat piti tiukkana, mutta myönsi, että on vaikea määritellä muulla tavalla varmenteen hyväksyttävä luotettavuustaso. Signicat ehdottaa harkittavaksi, että sovellettaisiin standardin ETSI EN 319 411-1 NCP menettelyä eli perustasoa.

Finanssiala puolestaan katsoi, että Suomessa ei ole toistaiseksi yhtäkään oikeushenkilöitä vahvasti tunnistavaa menetelmää ja määräys vaatisi käytännössä oikeushenkilön lukuun toimivien työntekijöiden tai alihankkijoiden työntekijöiden henkilökoh- taista tunnistamista.

Traficomin arvio:

Traficom toteaa, että esitetyt näkökohdat on arvioitu valmistelussa ja harkittu, että jotkin varmenteet voitaisiin sellaisenaan hyväksyä menettelyksi todentaa toinen osapuoli ja tämän avaimet.

Traficom viittaa perustelumuistion kohtaan 4.8.2:

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

Traficom toteaa vielä, että PSD2-sääntelyssä valvotut osapuolet (nk. TPP-toimijat) vastaisivat luottamusverkoston sääntelyssä luottavia osapuolia ja luottavia osapuolia

20.5.2022

ei tunnistus- ja luottamuspalvelulain sääntelyssä valvota siten kuin PSD2-sääntelyssä TPP-toimijoita. Luottamusverkoston toimijat ovat valvonnan piirissä, mutta Traficom on arvioinut valmistelussa, että tietoliikenneyhteyden turvallisuus luottaviin osapuoliin on tunnistamisen kannalta olennainen osa.

Traficom viittaa perustelumuistion kohtaan 4.8.5.3:

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.

Traficom katsoo, että viitattu ETSI EN 319 411-1 menettelyn taso ei olisi riittävä ilman erillisiä tarkempia luottamusverkostolle laadittuja vaatimuksia, jotka toteuttaisivat saman luotettavuuden kuin määräysehdotus.

Suora kahdenvälinen menettely ja "haltija"

Finanssiala toivoo selvennystä *haltijasta* määräykseen tai perusteluihin ja katsoo, että selkein olisi se taho, joka on tehnyt sopimuksen tunnistamisesta, eli esimerkiksi luottamusverkoston jäsen tai luottavaa osapuolta operoiva yritys, tai näiden lukuun toimiva alihankkija tai yksittäinen vastuuhenkilö.

Finanssiala toivoo, että *haltijan* merkitystä ei ainakaan laajennettaisi siihen, että täytyisi tunnistaa kaikki ne henkilöt, jotka esimerkiksi palvelua operoivan tahon työntekijöinä voivat päästä käsittelemään avainta jossain sen elinkaaren vaiheessa.

Traficom arvio:

Traficom selventää perusteluihin, että haltijan todentaminen tarkoittaa sopimusosapuolena olevan organisaation todentamista ja määräyksessä ei määritellä tarkemmin, miten organisaation edustamisoikeus sopimusta tehtäessä varmistetaan.

Perustelumuistion kohdassa 4.8.2 todetaan seuraavaa:

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

Määräyksessä ei oteta tyhjentävästi kantaa menettelyn yksityiskohtiin ja siihen, mikä on riittävä tapa tunnistaa toinen osapuoli. Esimerkiksi vahvan sähköisen tunnistamisen käyttäminen on hyvä käytäntö. Osapuolten 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 kuulumisen tietoliikenteen osapuolelle.

Vaikutusarviointi asiointipalveluihin ja protokollien menettelyt

Finanssiala toteaa, että Luottamusverkostossa käytetyille protokollille ole vielä olemassa yleisesti hyväksyttyä vakiintunutta ratkaisumallia todennettuun avainten vaihtamiseen. Finanssiala katsoo, että tällä hetkellä ei ole tarjolla sellaisia menetelmiä eikä käytäntöjä, joilla ehdotetun määräyksen vaatimukset voitaisiin täyttää ilman, että vahvan sähköisen tunnistamisen käyttäminen vaikeutuu tai jopa vaarantuu kokonaan.

20.5.2022

Finanssiala katsoo, että määräysehdotus edellyttäisi tarkempaa vaikutusarviointia asiointipalveluihin eli luottaviin osapuoliin ja että ehdotettua muutosta ei tulisi tehdä näin lyhyellä aikataululla, vaan tarvitaan lisäaikaa ja lisäselvityksiä ennen määräyksen antamista.

Signicat toteaa, että säännöksen 8 suomalaisen sääntelyn erityisvaatimukset luottavalle osapuolelle ovat haastavia yrityksille, jotka harjoittavat toimintaa monessa valtiossa. Ne haluaisivat käyttää tunnistamisessa yhtä turvallisuusvaatimuskiltaan yhdenmukaista välitysrapiintaa maasta riippumatta. Signicat arvioi myös, että vaatimukset voivat olla vaikeita pienille yrityksille ja huomauttaa, että vaatimusten luottaville osapuolille tulisi olla taloudellisesti suhteessa riskiin.

Traficomin arvio:

Traficom yhtyy Finanssialan arvioon protokollien menettelyistä ja toteaa, että OpenID Connect- tai SAML-protokollien perusmenettelyjä ei siten voi käyttää sellaiseen luottamussuhteen perustamisessa. Avainrotaation kannalta Traficom viittaa jäljempänä kohdan 8.2 lausuntojen tarkasteluun.

Traficom yhtyy Finanssialan ja Signicatin lausuntoon vaikutusarvioinnin tärkeydestä. Traficom on laatinut perustelumuistioon vaikutusarvion luottaviin osapuoliin, erityisesti kohta 4.8.5.5 *Luottavan osapuolen eli asiointipalvelun järjestelmien koventamisvaatimukset*. Siinä arvioidaan mahdollisimman yksityiskohtaisesti, mitä vaatimukset edellyttäisivät luottavalta osapuolelta. Vaikutusarviointi perustuu 2020 ennakkokyselyyn, 2021 valmistelutyöpajoihin ja valmistelutyöpajoissa saatuun tietoon ja virkätynä tehtyyn arvioon konkreettisista koventamistarpeista.

Traficom ei saanut lausuntoja luottavilta osapuolilta tai näitä edustavilta tahoilta. Finanssialan ja Signicatin lausunnossa on kommentoitu varmenteiden saatavuutta ja ehdotettujen vaatimusten soveltamiskysymyksiä, mutta ei ole otettu kantaa perustelumuistiossa esitettyyn vaikutusarvioon. Traficom katsoo, että virastolla ei ole esitettyä vaikutusarviointia ja lausuntopyyntöjä tehokkaampaa objektiivista keinoa arvioida vaikutuksia luottaviin osapuoliin tarkemmin kuin on jo tehty.

Traficom yhtyy siihen lausuntoon, että muutos vaatii viestintää viranomaisen ja tunnistuspalveluiden yhteistyönä ja **tarkentaa perustelumuistion kohtaa 4.8.5.5muutosten läpivieminen edellyttää luottamusverkon yhteistoimintaryhmän ja Liikenne- ja viestintäviraston yhteistyötä neuvonnassa ja viestinnässä.**

Traficom viittaa lisäksi perustelumuistion kohtaan 4.8.5.4:

Tunnistusvälityspalvelun kannalta vaatimukset vaikuttavat siihen, että sen on sopimussuhteissaan luottavien osapuolten kanssa huolehdittava teknisten vaatimusten informoinnista, sillä ei ole todennäköistä, että nämä olisivat niistä selvillä.

3.2.11 Säännös 8.2 varmenteiden ja avainten uusiminen

Finanssiala lausui ainoana ehdotuksesta.

Lähtötilanne ja vaatimusten riskiarvio

Finanssiala toteaa, että TUPAS-aikaan avaimia ei pääsääntöisesti päivitetty ja vaikka periaatteellisella tasolla nykyiset standardit edellyttävät säännöllistä avaintenvaihtoa, käytännössä luottamusverkostossakaan kaikki toimijat eivät ole vielä vaihtaneet OIIC-protokollan sanomatasolla käytettäviä avaimia, eikä siihen ole kaikilla toimijoilla palvelukuvauksissa määriteltyä prosessia.

Finanssiala kritisoi avainten päivittämiseen liittyviä vaatimusmuutoksia, koska ei pidä riskiarviota oikeaan osuneena. Määräysehdotus vaikeuttaa sitä, että hyökkääjä harhauttaa osapuolen luottamaan itse luomaansa avaimeen. Määräysehdotus ei torju

20.5.2022

sitä, että hyökkääjä varastaa avaimen ja tekeytyy sen avulla oikeaksi osapuoleksi. Avainten vuotoriskiä aiheuttavat esimerkiksi tietomurrot tai poistuvat työntekijät.

Finanssivalvonta toteaa, että manuaalinen avaintenvaihtoprosessi on osoittautunut käytännössä työlääksi ja herkäksi virheille. Finanssiala pitää riskinä, että manuaalipyörittäminen ja viestintää prosesseissa luottamusverkoston jäsenten sekä asiointipalveluiden välillä joudutaan lisäämään ja että tämä ei paranna tunnistuspalvelun tai verkoston turvallisuutta kokonaisuutena. Finanssiala arvioi, että muuttuva prosessi johtaa kokonaisuutena arvioiden jopa aiempaa heikompaan avaintenhallintaan, etenkin asiointipalveluissa, koska niillä ei ole samanlaisia teknisiä valmiuksia kuin luottamusverkoston jäsenillä.

Finanssiala katsoo myös, että kokemusten mukaan tiheä avaintenvaihto ja riittävä automaatio vähentävät oleellisesti sekä inhimillisten virheiden että hyökkäysten aiheuttamaa riskiä. Finanssiala ehdottaa, että viranomaisen rohkaisisi markkinoita entistä lyhytikäisempien avainten käyttöön, jotta avainten mahdollisista vuotamisista syntyviä riskejä voitaisiin minimoida.

Traficomin arvio:

Traficom pitää Finanssialan arviota säännöksen 8 suhteesta avainten vuotamiseen oikeana. Traficom toteaa kuitenkin, avainten varastamisen tai vuotamisen estäminen on luottamusverkoston toimijoilla keskeinen osa säännöksen 5 mukaista tunnistusjärjestelmän turvallisuutta ja mm. säännöksen 5.4.b) tiedon luokitteluun perustuvan salassa pidettävän aineiston käsittely-ympäristön ja säilytyksen suojautumiskykyä. Luottavien osapuolten osalta asiaan voidaan vaikuttaa lähinnä neuvonnalla sopimus-suhteissa.

Traficom toteaa, että säännöksessä 8.2 on nimenomaan pyritty löytämään vaihtoehto, jossa vallitsevan protokollan OpenID Connectin käytössä voidaan automatisoida avainten päivittäminen.

Avainten päivitys, certificate tai key pinning tai mTLS (8.2.b)

Finanssiala huomauttaa, että Let's Encryptin varmenteita uusittaessa vaihdetaan myös niihin kytkeytyvä salainen avain, mikä tekee TLS-varmenteiden sitomisesta (certificate pinning) äärimmäisen työlästä ja häiriöaltista.

Traficomin arvio:

Traficom on arvioinut perustelumuistion kohdassa 4.8.3 säännöksen 8.2.b) menettelyn soveltamista siitä lähtökohdasta, että varmennetta uusittaessa voidaan säilyttää aikaisemmat avaimet.

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.

Avainten päivitys, ketjutus (8.2.c)

Finanssiala arvioi, että avainten vaihtoon, hallintaan ja elinkaareen on kehitteillä useita erilaisia ratkaisuja, esimerkiksi erilaiset lohkoketjuratkaisut tai SSI-menetelmät. Finanssiala ehdottaa, että määräyksen säännöstä 8.2.c) muutetaan sallimaan avainten ketjutus esimerkiksi seuraavalla muotoilulla: c) allekirjoittamalla uudet avaimet 8.1 kohdan mukaisesti toimitetuilla avaimilla tai niistä ketjutetuilla avaimilla.

Traficomin arvio:

Traficom kiittää kommentista ja korjaa säännöksen sanamuotoa, sillä tarkoitus on, että säännöksen 8.1 luottamussuhteen perustamisen jälkeen avaimia voi ketjuttaa.

3.2.12 Säännös 9 Tunnistussanomien eheys ja luottamuksellisuus

Sanomien salausavaimet ja säännös 7 TLS-salauksen DHE-avaintenvaihto

Finanssiala toteaa säännöksen 8 yhteydessä, että jo voimassa oleva määräys M72 edellytti perustellusti DHE-avaintenvaihtoa luottamusverkostossa. Käytännössä tämä tarkoittaa, että TLS-yhteyksien sisällä siirrettävä data salataan tilapäisillä lyhytikäisillä avaimilla eikä useita vuosia voimassa olleilla sivustojen varmenteiden avaimilla, kuten aiemmin oli laajalti käytäntönä.

Finanssiala arvioi, että pyrkimällä minimoimaan sanomien allekirjoittamisessa ja salaamisessa käytettävien avainten elinkaarta kyetään oleellisesti leikkaamaan ajallisesti sitä riskiä mikä syntyy, mikäli ne vuotavat väärin käsiin. Finanssiala kannustaa viranomaista rohkaisemaan markkinoita entistä lyhytikäisempien avainten käyttöön, jotta avainten mahdollisista vuotamisista syntyviä riskejä voitaisiin minimoida.

Traficomin arvio:

Traficom yhtyy Finanssialan lausumaan ja viittaa tässä säännöksessä 8.2.b) käsitelyihin avainten vaihtoon ja turvalliseen tietoliikenneyhteyteen liittyviin käytänteisiin.

3.2.13 Säännös 11.3 Tunnistuspalvelun häiriöilmoitusten ilmoitusmenettely

Tietosuojaavaltuutettu kiinnittää huomiota yleisen tietosuoja-asetuksen tietoturvaloukkauksen ilmoittamista koskeviin 33–34 artikloihin. Toimijoiden on tärkeää tunnistaa, että osa tunnistusjärjestelmien ja tunnistuspalveluiden häiriötilanteista saat-
taa täyttää myös tietosuoja-asetuksen mukaisen henkilötietojen tietoturvaloukkauksen määritelmän.

Traficomin arvio:

Traficom toteaa huomion oikeaksi. Virasto arvioi, että yleisen tietosuoja-asetuksen velvoitteet ovat hyvin tunnettuja ja ei lisää asiasta informaatiota perustelumuistioon. Tunnistuspalvelun tarjoajiin kohdistuu myös kuluttajansuojan ja saavutettavuuden sekä osaan myös finanssialan sääntelyä ja valvontaa.

3.2.14 Säännös 12.2 Luottamusverkostossa välitettävät valinnaiset tiedot

S-Pankki pyysi tarkennusta siihen, mitä tarkoittaa teknisesti suunniteltu ja täytyykö attribuuttien olla teknisesti tehtynä.

Signicatin ehdotusta valinnaisesta vapaatekstikentästä käsitellään säännöksen 6 kohdalla.

Traficomin arvio:

Traficom viittaa perustelumuistion kohtaan 4.12.4:

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 tunnistussanomien sisältävät valinnaiset attribuutit haittaa tunnistustapahtumia silloinkaan, kun niiden käytöstä ei ole sovittu.

3.2.15 Säännös 15.2 Tunnistuspäalvelun arviointikriteeristö

Nixu kannatti sitä, että säännöksessä mainitaan Liikenne- ja viestintäviraston arviointiohje ja ehdotti säännöksen tiukentamista siten, että ohjetta olisi oletusarvoisesti käytettävä. Nixu toteaa käsityksensä, että suurin osa auditoinneista tehdään ohjeen perusteella ja tiukempi velvoittavuus edistäisi auditointien kilpailuttamista ja yhteismitallisuutta.

Traficomin arvio:

Traficom yhtyy siihen käsitykseen, että ohjeen käyttäminen edistää auditointien yhdenmukaisuutta ja helpottaa kilpailuttamista. Traficom arvioi kuitenkin, että ohjeen muuttaminen oletusarvoisesti pakolliseksi ei ole perusteltua oikeudellisesti. Ohjeen käytön vaatimus muuttaisi sen määräyksen luonteiseksi ja muutos edellyttäisi perusteellista vaikutusarviointia. On välttämätöntä säilyttää mahdollisuus tukeutua muihin relevantteihin arviointikehyksiin. Myös ennakoitavat ja tasapuoliset poikkeamisperusteet uudesta vaatimuksesta edellyttäisivät sääntelyä ja vaikutusarviota.

3.2.16 Säännös 16 Selvitys tunnistuspäalvelun tarjoajan ja julkaistujen tietojen luotettavuudesta

Finanssiala kiinnitti huomiota siihen, että tunnistus- ja luottamuspalvelulaissa käytetään termiä yhteistyökumppanit ja määräyksen säännöksessä 16 alihankkijat, eikä lain esitöissä, määräyksessä tai määräyksen perusteluissa tarkenneta, minkä ta-soista tietoa yhteistyökumppaneista odotetaan.

Traficomin arvio:

Traficom toteaa, että terminologiassa näkyy kansallisen ja EU-säätelyn yhdistäminen ja se, että yhteistyökumppaneihin tai alihankkijoihin kohdistuu vaatimuksia eri näkökulmista.

Määräys liittyy tunnistus- ja luottamuspalvelulain 13 §:n tarkoittamaan alihankintaan.

Traficom on tulkinut valvonnassa, että myös tunnistus- ja luottamuspalvelulain 14 §:n tunnistusperiaatteissa edellytetyt tiedot palveluntarjoajan tärkeimmistä yhteistyökumppaneista koskevat alihankkijoita, koska kysymys on lain 14 §:n mukaan tiedoista, joissa määritellään tarkemmin, kuinka palveluntarjoaja täyttää tässä laissa säädettyt velvollisuutensa.

Traficom on kuvannut säännösten suhdetta perustelumuistion kohdassa 4.16.2:

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. ...

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

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 tunnistustapah-
tumien välittämistä luottaville osapuolille eli asiointipalveluille.

Sama oikeushenkilö voi toimia halutessaan sekä tunnistusvälineen tarjoajana että tun-
nistusvälityspalveluna.

Määräystä sovelletaan myös eIDAS-asetuksen mukaisiin hyväksyttyihin luottamuspal-
veluihin, 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 luottamus-
palveluita, jos virastolle ilmoitetaan, että ei-hyväksytty luottamuspalvelun tarjoajat tai
niiden tarjoamat luottamuspalvelut eivät väitetyt täytä asetuksessa säädetyjä vaa-
timuksia. Virasto arvioi, että valvontatilanteessa toimintaa voitaisiin verrata lähinnä
eIDAS-asetuksen täytäntöönpanon tueksi laadittuihin standardeihin.

Täsmälliset viittaukset EU-säädäntöön ovat tarpeen selkeyttävänä informaationa mää-
röksessä 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 in-
formatiivinen eikä esimerkiksi määrittele tarkemmin vaatimusten soveltamisalaa.

Säännökseen ei tehdä muutoksia määräyksessä 2022.

4.2.1 Tunnistuspalvelut

Tunnistus- ja luottamuspalvelulain mukaan myös kansallisesti edellytetään, että tun-
nistuspalvelujen 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 eril-
listä tunnistusratkaisua rajat ylittäviä tilanteita ja kansallista tunnistamista varten.

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

4.2.2 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 hyväksytyjen luottamuspalvelujen eIDAS-asetuksessa säädettyjä vaatimuksia viittaamalla EU:n valmistelutyössä viitoitamiin kansainvälisiin standardeihin siltä osin, kun niihin ei ole ainakaan toistaiseksi tehty viitauksia komission täytäntöönpanosäädöksillä, vaikka siihen olisi eIDAS-asetuksessa toimivalta.

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

4.2.3 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 arviointielimet ovat päteviä tekemään tunnistusjärjestelmän arviointeja. Tunnistuspalveluntarjoajan arviointielimen ei tarvitse hakea erikseen hyväksyntää, ellei se ole akkreditoitu 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 §:n 8) *varmenteella sähköistä todistusta, joka todentaa henkilöllisyyden tai todentaa henkilöllisyyden ja liittyy luottamuspalvelun todentamistiedot luottamuspalvelun käyttäjään ja jota voidaan käyttää vahvassa sähköisessä tunnistamisessa ja luottamuspalveluissa*

20.5.2022

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 *EU:n sähköisen tunnistamisen yhteentoimivuusjärjestelmään liittyvää kansallista rajapintaa*. Komission täytäntöönpanoasetuksen (EU) 2015/1501 [5] 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 muihin solmupisteisiin tarjoamalla yhden jäsenvaltion kansalliselle sähköisen tunnistamisen infrastruktuurille rajapinnan muiden jäsenvaltioiden sähköisen tunnistamisen infrastruktuureihin*.

Termiä kansallinen solmupiste käytetään säännöksissä 10, 13 ja 17.

4.3.2 Säännös 3.2 Tunnistus- ja luottamuspalvelulain 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 [1] 2 §

1) **vahvalla sähköisellä tunnistamisella** sellaista henkilön, oikeushenkilön tai oikeushenkilöä edustavan luonnollisen henkilön yksilöimistä ja tunnusteen 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 tunnistusvälinettä tunnistusvälityspalvelun tarjoajalle välitettäväksi luottamusverkostossa;

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

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

11) **vaatimustenmukaisuuden arviointilaitoksella** Liikenne- ja 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

20.5.2022

eIDAS-asetuksen [3] 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 säädetty sovellettavat vaatimukset;

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

EU:n komission sähköisen tunnistamisen varmuustasoasetuksen [4] 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 fyysisesti 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.

Tunnistus- ja luottamuspalvelulain 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 [11] 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 [12].

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 varmuustasolla 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 ylätasoa 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 säännös 15 ja sen perustelut.

20.5.2022

Seuraavassa kuvaillaan alakohtien sisältöä ja arvioidaan niiden liityntä ISO/IEC 27001-standardin [11] kohtiin. Taulukkoon on tehty täydennyksiä 2016 perusteluihin nähden.

Määräys 4.2 kohta ja soveltaminen	ISO/IEC 27001
1) <i>tunnistuspalveluntarjoajan toimintaympäristö kokonaisuutena</i> - Tietoturvallisuuden hallintajärjestelmä kattaa tunnistusjärjestelmään vaikuttavat olennaiset sisäiset ja ulkoiset tekniset, oikeudelliset ja hallinnolliset vaatimukset ja tarpeet. - Tunnistuspalvelussa tulee mm. noudattaa ajantasaisia lainsäädäntöjä ja määräyksiä, kuten tunnistus- ja luottamuspalvelulakia, määräystä 72 ja yleistä tietosuoja-asetusta.	4 organisaation toimintaympäristö
2) <i>tietoturvallisuuden hallinnan johtaminen, organisointi ja ylläpito</i> - Tietoturvallisuuden hallintajärjestelmä kattaa hallinnan johtamisen, organisoinnin ja ylläpidon, joka dokumentoidaan tietoturvapoliitikassa tai vastaavissa ohjausasiakirjoissa. - Käytössä on ajantasainen ja johdon hyväksymä tietoturvapoliittika tai vastaavat ohjausasiakirjat. Turvallisuusperiaatteet ja politiikat ovat organisaation ja suojattavien kohteiden kannalta kattavat ja taroituksenmukaiset. - Henkilökunnan ja alihankkijoiden tietoturvallisuuteen liittyvät vastuut on kuvattu.	5 johtajuus 9.2 sisäinen auditointi 9.3 johdon katselmus 10 hallintajärjestelmän parantaminen A.5.1.1 Tietoturvapoliittikat A.6.1.1 Tietoturvaroolit ja -vastuut A.15.1.1 toimittajasuhteiden tietoturvapoliittika
3) <i>tunnistuspalvelun tarjontaan liittyvien tietoturvallisuusriskien hallinta</i> - 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.	6 suunnittelu

- Riskienhallintaprosessia ja sen tuloksia hyödynnetään tunnistuspalvelun/tunnistusjärjestelmän turvatoimien suunnittelussa. - Vrt. eIDAS varmuustasoasetuksen soveltamisohje: <i>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.</i> - Määräyksen säännöksessä 6.1 määrätään tarkemmat vaatimukset tunnistusmenetelmän riskien arvioimiselle	
4) <i>tietoturvallisuuden resursointi, pätevyys, henkilöstön tietoisuus tietoturvallisuudesta, viestintä ja dokumentointi sekä dokumentoidun tiedon hallinta</i> - 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. - 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.	7 tukitoiminnot
5) <i>tunnistuspalvelun tarjonnan suunnittelu ja ohjaus tietoturvavaatimusten täyttämiseksi</i> - Tietoturvallisuuden hallintajärjestelmässä huolehditaan tunnistuspalvelun tarjonnan suunnittelusta ja ohjauksesta siten, että tunnistuspalvelulle säädetyt tietoturvavaatimukset täyttyvät. - Tunnistuspalvelun vaatimukset (Tunnistus- ja luotamuspalvelulaki, EU:n sähköisen tunnistamisen varmuustasoasetus ja viraston määräys 72) on huomioitu hallintajärjestelmässä	8 toiminta A.18.1.1 vaatimustenmukaisuus/lainsäädäntöön ja sopimukseen sisältyvien vaatimusten noudattaminen: sovellettavien lakisäätteiden ja sopimuksellisten vaatimusten yksilöiminen

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 arvioissa on vähintään otettava huomioon.

Määräyksessä ei oteta kantaa riskinhallinnassa käytettävään malliin tai siinä noudatettavaan standardiin. Sekä koko tunnistusjärjestelmän että erityisesti säännöksen 6 tunnistusmenetelmän 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 [13]
- ISO/TR 31004, Risk management – Guidance for the implementation of ISO 31000, and International Standard/ISO/TR 31004:fi [14]
- SFS-EN IEC 31010:2019, ISO/IEC 31010, Risk management – Risk assessment techniques, developed jointly with the International Electrotechnical Commission/ [15]
- ISO 27005 [16] https://en.wikipedia.org/wiki/ISO/IEC_27005
- VAHTI Ohje riskienhallintaan, Valtiovarainministeriön julkaisuja 22/2017 [17] https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/VM_22_2017.pdf?sequence=1&isAllowed=y
- NIST Risk Management Framework (RMF) [18] <https://csrc.nist.gov/projects/risk-management/about-rmf>
- Erityisesti tunnistusmenetelmien tai salauskäytäntöjen toteutuksen arvioinnissa voi käyttää myös standardeja, kuten FIPS 140-3 Security Requirements for Cryptographic Modules [19] <https://csrc.nist.gov/publications/detail/fips/140/3/final>

Riskinhallintamallin tarkistuslistana voidaan pitää myös seuraavaa, lähteenä KATAKRI 2020 [12], T-03:

20.5.2022

- 1) *Tietoturvallisuusriskien hallinta on osa organisaation toimintaa ja muuta riskienhallintaa.*
- 2) *Tietoturvallisuusriskien hallinnan avulla varmistetaan riittävien tietoturvaluustoimenpiteiden 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 tietoturvaluustoimenpiteiden suunnittelussa ja toteuttamisessa, turvallisuuspoikkeamien vaikutusten arvioinnissa sekä muutoksenhallinnassa ja soveltuville osin hankintamenetelyissä.*
- 7) *Tietoturvaluustoimenpiteet 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) [13]

- 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. Tuoloin päädyttiin siihen, että ISO 27001 on ainoa riittävän kattava standardi. Arvioinneissa on käytännössä tullut esille ainakin finanssialan standardeihin (kuten PCI-standardit, PCI DSS [20]) tukeutuminen osana tietoturvallisuuden hallintaa.

Virasto arvioi, että edelleenkin 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 tietoturva-vaatimukset

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 [4] 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 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 tietoturvatoinenpitenä. Henkilöstön työtehtävien eriyttäminen, fyysisten työtilojen ja -välineiden eriyttäminen tai teknisen palveluympäristön ja palvelinympiiristön 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.

20.5.2022

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.

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 turvallisuushkista ja -toimenpiteistä.

Informaatiolla ohjaaminen. Ei huomioita.

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 säädetty luotettavuusvaatimukset. Tunnistusjärjestelmä kattaa myös kaikki alihankitut osat ja toiminnot, jotka liittyvät tunnistuspalvelun tuottamiseen. Tunnistus- ja luottamuspalvelulain 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 tunnistusmenetelmän toteuttamisessa käytetään tyypillisesti alihankintaa. Vaatimustenmukaisuuden arvioinnin kannalta alihankintaa käsitellään Liikenne- ja viestintäviraston sähköisen tunnistuspalvelun arviointiohjeessa 211/2019 O [21].

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

20.5.2022

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 hyökkäys-potentiaalista suojautumiskyvyn perusteella. Vaatimus koskee koko tunnistusjärjestelmän suojautumiskykyä ja siten säännöksissä 5.2–5.4 tarkennettuja tietoliikenne-, tietojärjestelmä- ja käyttöturvallisuuden osatekijöitä. Kaikissa toimissa on noudatettava huolellisuutta ja hyviä käytäntöjä.

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, LOA Guidance [22], kohta 2.3.1

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" [23] ja ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation" [24]. 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 [25] mainitaan esimerkiksi seuraavat: verkossa ja verkon ulkopuolella tapahtuva arvaaminen, tunnistetietojen toisintaminen, tietojen kalastelu, sala-kuuntelu, replay-hyökkäys, istuntokaappaus, mies välissä -hyökkäys, tunnistetietojen varastaminen, spoofing-hyökkäys ja toisena esiintyminen.

4.5.4 Säännös 5.1.2 Säännösten 5 ja 7 salausvaatimusten suhde

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 säädettyiltä 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.

20.5.2022

Määräyksen säännöksessä 7 määrätään tiettyjen tietoliikenneyhteyksien ja sanomien erityiset salausta- tai suojausvaatimukset. Määräyksen säännöksen 5 vaatimus koskee yleisesti muita yhteyksiä ja elementtejä eli esimerkiksi tunnistusjärjestelmän sisäisiä elementtejä, säilytettäviä tietoja sekä yhteyksiä alihankkijoiden järjestelmiin. Vaatimus ulottuu sekä säännöksen 5.2 tietoliikenteeseen että säännöksen 5.3 tietojärjestelmiin sekä säännöksen 5.4 operointiin. Näissäkin on suositeltavaa käyttää teknisesti soveltuvien osien 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 turvatason 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.

5.2.e) turvalliset hallintayhteydet

Säännökseen on lisätty tarkennus "turvalliset".

20.5.2022

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

Ks. myös määräyksen säännös 5.5.

5.2.f) kansainvälisesti tai kansallisesti suositellut salausratkaisut

Suositteluvien salausratkaisujen lähteistä ks. tämän perustelumuistion kohta 4.7.5.

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.

Pääkäyttäjaoikeuksien 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

20.5.2022

Tunnistusjärjestelmässä täytyy huolehtia haittaohjelmien 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 määriteltä menetelmä, jota noudatetaan mahdollisen turvallisuuspoikkeaman jäljittämiseksi 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 aikälähdettä 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 käyttöönnottoon liittyviä lokitietoja.

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

5.3.g) kansainvälisesti tai kansallisesti suositellut salausratkaisut

Suosittelavien salausratkaisujen lähteistä ks. tämän perustelumuistion kohta 4.7.5.

4.5.7 Säännös 5.4 Käyttöturvallisuus

5.4.a) muutosten hallinta

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

20.5.2022

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 §:n 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 tiiviste-funktioiden 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 säännös 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.

20.5.2022

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

Vrt. PiTuKri, kohta KT-04 Haavoittuvuuksien hallinta, [26] Traficom 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 salausten menetelmät. Määräyksen säännöksen 7 sidosryhmävalmistelussa on nostettu esille kysymys siitä, miten määräyksessä hyväksytyksi listattujen algoritmien tai menetelmien mahdollinen muuttuminen haavoittuviksi ja siitä aiheutuva tarve luopua niiden käytöstä vaikuttaa säännöksen 7 soveltamiseen.

Säännöksen 5.4.d) 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

Suosittelavien 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 §:n 2 momenttia.

20.5.2022

Tuotantoverkolla tarkoitetaan kokonaisuutta, joka koostuu kaikista tietojärjestelmistä ja resursseista, jotka osallistuvat tunnistusmenetelmän linkaaren hallintaan tai tunnistusjärjestelmän hallintaan. 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 käytetään muuta kuin edellä kuvattua kovennettua työasemaa, otetaan toteutuksessa huomioon tuotantojärjestelmän eriyttäminen ja muut järjestelyt, joilla tietoturvaohjeet 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-proxyä.

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

4.5.9 Säännös 5, harkitut sääntelyvaihtoehdot

4.5.9.1 Korkean varmuustason vaatimukset

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

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

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

4.5.9.2 Eriyttämisvaatimukset tietoturvatöimenpiteenä

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

Eriyttäminen tietoturvatöimenpiteenä. Määräyksen valmistelussa arvioitiin vuonna 2016, onko tietoturva-vaatimusten 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 yksityiskohdillaan 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.

4.5.10 Tunnistusjärjestelmän kellonajan luotettavuus

Määräyksen 72 perustelumuistiossa on ollut suositus tunnistusjärjestelmän kellonajan luotettavuudesta (määräyksen perustelumuistio 2016/2018 C-osa kohta 1).

Määräysvalmistelussa on harkittu tunnistusjärjestelmän aikälähteen 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

Suosittelaa, että tunnistuspalveluntarjoaja hankkii luotettavan aikälähteen, 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 [27].

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

4.6 Säännös 6 Tunnistusmenetelmän tietoturva-vaatimukset

4.6.1 Säännös 6.1 Tunnistusmenetelmän ominaispiirteet ja suojausominaisuudet

4.6.1.1 Säännös 6.1.1 Eritelty riskiarvio

Säännös on uusi.

20.5.2022

Säännöksessä 6.1.1 tarkennetaan tunnistusmenetelmän todentamistekijöiden ja todentamismekanismin muodostaman kokonaisuuden turvallisuusvaatimuksia. Määräykseen lisätään 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.

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

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

Vaikutukset. Virasto arvioi, että vaatimus riskiarvion tekemisestä on luonteva osa tunnistuspalvelun tyypillisen 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.

Vaihtoehtoiset sääntelytavat. Virasto on arvioinut säännöksen 6.1.1 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 säännösten tasolla. Myöskään uhkat tunnistusmenetelmän turvallisuudelle ja turvakeinot uhkilta suojaamiselle eivät ole puhtaasti todentamistekijätyyppikohtaisia. Suojautumiskyvyn mittareita tai muunlaisia tarkennuksia määräyksessä voisi harkita.

Muut ohjauskeinot.

Tunnistuspalvelun arviointiohjeessa huomioidaan muutetut vaatimukset.

Yhteissääntelystä virasto katsoo, että luottamusverkoston yhteistoimintaryhmän tiedonvaihdoissa voidaan tunnistus- ja luottamuspalvelulain 16 §:n perusteella käsitellä yhteisiä tietoturvallisuushakia. Lain 12 a §:ssä säädetään luottamusverkostossa kielto käyttää kilpailijoista saatuja tietoja muuhun kuin siihen tarkoitukseen, jota varten ne on tunnistuspalvelun tarjoajalle annettu.

Suositus tai informaatio-ohjaus. Ei huomioita.

Valvonta. Tunnistusjärjestelmän ja sen osana tunnistusmenetelmän riskiarvio on jo ennestään voimassa oleva vaatimus, joten siirtymäaika ei ole tarpeen. Riskiarvioita ei kuitenkaan ole välttämättä laadittu ja dokumentoitu tällä tarkkuudella. Virasto arvioi erikseen, valvotaanko arvion tekemistä ja tuloksia määräyksen voimaan tullessa esi-

20.5.2022

merkiksi valvontakyselyllä vuoden 2022 aikana vai vasta osana säännöllistä vaatimusten mukaisuuden määräaikaisarviointia eli vuoden 2023 kaksivuotisarvioinnissa, jolloin valvonta tapahtuisi käytännössä vuonna 2024. Erityinen arviointivaatimus koskee joka tapauksessa määräyksen voimaantulon jälkeen virastolle ilmoitettavia muutoksia tunnistusmenetelmissä. Se voi tulla valvottavaksi myös tapauskohtaisesti häiriötilanteissa.

4.6.1.2 Riskiarviossa huomioitavia uhkia

Uhka-arviossa huomioon otettavat uhkat perustuvat hyvään toimialaosaamiseen, tunnistuspalvelun ylläpidossa kertyvään tietoon, luottamusverkoston yhteistoimintaryhmässä saatavaan luottamukselliseen tietoon ja yleisesti saatavilla olevaan tietoon tietoturva-uhkista ja haavoittuvuuksista.

Varmuustasoasetuksen soveltamisohje, LOA Guidance [22], kohta 2.3.1:

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 ja ohjeessa NIST 800-63B Digital Identity Guidelines, Authentication and Lifecycle Management mainitut, <https://pages.nist.gov/800-63-3/sp800-63b.html>

ISO 29115 Information technology — Security techniques — Entity authentication assurance framework [25]

- 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 Digital Identity Guidelines, Authentication and Lifecycle Management [28]

- Assertion Manufacture or Modification/assertion/väärän vakuutuksen muodostamisen 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.

Hallussapitoon perustuva todentamistekijä. Varmuustasoasetuksen soveltamisohje, LOA Guidance [22], kohta 1(2)(a):

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, puhelinelukituksen 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.

Tietoon perustuva todentamistekijä. Varmuustasoasetuksen soveltamisohje, LOA Guidance, kohta 1(2)(b):

Tyypillisiä tiedossa oloon perustuviin todentamistekijöihin kohdistuvia hyökkäyksiä ovat arvaaminen, tietojen kalastelu (phishing), salakuuntelu tai toisintaminen. Tiedossa oloon perustuvilla todentamistekijöillä 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 kopioituneet 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.

Ominaisuuteen perustuva todentamistekijä. Varmuustasoasetuksen soveltamisohje, LOA guidance, kohta 1(2)(c):

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.

20.5.2022

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.

Varmuustasoasetuksen soveltamisohje, LOA Guidance [22], kohta 1(3):

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 yhtäaikaista 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 Diffie-Hellman-avaimiin, jos luottava osapuoli antaa tilapäisen avaimen (esimerkiksi laajennettu pääsynvalvonta)*

20.5.2022

- 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.

Varmuustasoasetuksen soveltamisohje, LOA Guidance, kohta 2.3.1:

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 tunnisteiden vahvuus ja suojatun kanavan vahvuus.
- Aikaperusteiselle kertakäyttösalasanojen muodostajalle hallussapidon todentamismekanismi on muodostetun kertakäyttösalasanan lähettäminen varmentajalle. Tämän mekanismin vahvuutta rajoittaa muun muassa kertakäyttösalasanan pituus, salasanan voimassaoloaika sekä toimitustavan luottamuksellisuus.

4.6.1.5 Turvatoimenpiteet

Hallussapitoon perustuva todentamistekijä. Varmuustasoasetuksen soveltamisohje, LOA guidance [22], kohta 1(2)(a):

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, yksilöivät 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.

20.5.2022

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.

Tietoon perustuva todentamistekijä. Varmuustasoasetuksen soveltamisohje, LOA guidance, kohta 1(2)(b):

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, väärin yritysten määrän rajoittaminen.

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

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

Ominaisuuteen perustuva todentamistekijä. Varmuustasoasetuksen soveltamisohje, LOA guidance, kohta 1(2)(c):

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 mobiilisovelluksen 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 mitta-reita. 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. NISTin Face Recognition Vendor Test (FRVT) projektin [29] sivuilla, <https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt>

20.5.2022

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
- Tunnistusvälineen haltijan informointi

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 hyväksyttävyyys on suhteutettava suojautumiskyvyn vaatimukseen tietyntasoista hyökkäyspotentiaalia vastaan.

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

Varmuustasoasetuksen soveltamisohje, LOA guidance [22], kohta 2.3.1:

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" [23] ja ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation" [24]. 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

Säännökseen 6.1.2 lisätään tarkennettu vaatimus tunnistusmenetelmän ominaispiirteistä ja turvatoimenpiteistä todentamistekijöiden riippumattomuuden varmistamiseksi.

Tekijöiden riippumattomuus on välttämätön turvatoimenpide etenkin, jos eri tekijöitä käytetään samalla päätelaitteella kuten älypuhelimella. Eriyttäminen 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 säännöksen 6.1.1 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 mahdollisia osia. 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.

Säännöksen 7 mukaiset tietoliikenteen salausvaatimukset säännöksessä 6 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.
- Esimerkki arviointiohjeesta 211/2019 [21], Liite C Mobiilitunnistusratkaisun erityiskriteeristö: hard fail certificate pinning 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

20.5.2022

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)

Vaatus 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 tunnistuspyynnot.

Vaatus koskee luonnollisesti vain sellaista tunnistusmenetelmää, jossa on oma näyttö. Esimerkiksi tunnuslukulaitteessa näyttäminen ei yleensä ole teknisesti mahdollista. Sähköisen 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.

Tapahtumatunnisteen esittämisessä on syytä huomioida digitaalisten palvelujen tarjoamisesta annetun lain (306/2019) [30] saavutettavuusvaatimukset.

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

Siirtymäajasta ks. säännös 24.

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

Vaatus on uusi.

Tieto luottavasta osapuolesta tarkoittaa asiointipalvelua, jolle vahvistus tunnistamisesta ollaan toimittamassa. Määräyksen tarkoitus on, että kun käyttäjälle näytetään sen asiointipalvelun nimi, joka on esittänyt tunnistuspyynnön, käyttäjällä on mahdollisuus havaita ja jättää vahvistamatta mahdollinen väärä tai petollinen tunnistuspyyntö. Asiointipalvelusta näytettävän nimen on tarkoitus olla käyttäjän helposti tunnistama nimi palvelusta, jonka kanssa hän asioi. 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

20.5.2022

ja käyttöliittymät, joissa käyttäjältä vaaditaan toimenpiteitä, esim. tunnistusmenetelmän valintaikkuna, mahdollinen tunnistusvälityspalvelun esittäminen käyttöliittymä, tunnistusvälineen tarjoajan selainkäyttöliittymä tai tunnistussovellus tai muu näyttämisen mahdollistava tunnistusvälineen tai todentamisen osa.

Asiointipalvelun nimen esittämisessä on syytä huomioida digitaalisten palvelujen tarjoamisesta annetun lain (306/2019) [30] saavutettavuusvaatimukset.

Tieto määrätään pakolliseksi attribuutiksi tunnistusvälineen ja tunnistusvälityspalvelun välisessä rajapinnassa säännöksessä 12.1. Tiedon tuottaa tunnistusvälityspalvelu. Attribuutti on ollut määriteltynä luottamusverkoston SAML- ja OpenID Connect -rajapintasuosituksiin [31, 32] (*ftn_spname*) jo aikaisemmin vapaaehtoisena ja 2021 pakollisena, joten valmius voi olla osalla tunnistuspalveluista jo määriteltynä rajapinnoissa.

Siirtymäajasta 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 työstyetty yhdessä

20.5.2022

tunnistuspalveluiden kanssa. Tämä työ jatkuu ja virasto harkitsee työn edetessä tarkoituksenmukaiset ohjauskeinot. Tunnistuspalveluiden toistaiseksi eriävien näkemysten takia lähinnä viraston *ohje, suositus tai tulkintalinjaukset* näyttäivät 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.

Soveltaminen. 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 kiello 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.

20.5.2022

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 tiedotamalla käyttäjää toisen kanavan kautta ja käyttämällä varmistettuja yhteystietoja.

4.6.4 Säännös 6.4 Tunnistusmenetelmän haltijakohtaisten tietojen käsittely

Vaatuimuksilla 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 §:ssä.

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 [4]

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 todentamismekanismeja, 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.

20.5.2022

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 perustuvan 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 todentamistekijätyypikohtaisia.

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 lisätekiällä, 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 tunnistus- ja luottamuspalvelulaissa ja sähköisen tunnistamisen varmuustasoasetuksessa. Varmuustasoasetuksessa mainitaan myös säännöksen tasolla uhkatyyppiä.

Suojautumiskyvykyys 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"* [23] ja *ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation"* [24]

20.5.2022

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 todentamismekanismien 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 mahdollista. 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.

4.6.6 Säännös 6 ja Tunnistus- ja luottamuspalvelulain/varmuustasoasetuksen ja PSD2-säätelyn yhteensopivuus

Pankki- ja maksupalveluissa käytettävää vahvaa tunnistusta säännellään PSD2-direktiivissä [33] ja sen nojalla annetussa komission täytäntöönpanosäädöksessä (EU) [34]. Kansallisesti maksupalveluista säädetään maksupalvelulaissa [35].

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

Sääntelyjä ei ole toistaiseksi yhteensovitettu EU-tasolla.

Monia tunnistus- ja luottamuspalvelulain mukaan rekisteröityjä vahvoja sähköisiä tunnistusmenetelmiä käytetään Suomessa myös maksupalvelusäätelyn 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 [36] lausuntoja toimialalta Finanssivalvonnan PSD2-yhteistyöryhmältä ja Viestintäviraston eIDAS-työryhmältä. **Arvion ja lausuntojen perusteella saman tunnistusmenetelmän käyttämiselle molempien sääntelyjen puitteissa ei havaittu**

vuonna 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.

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

4.7 Säännös 7 Tunnistusjärjestelmän rajapintojen salausvaatimukset

4.7.1 Säännös 7.1 Tietoliikenteen salausmenetelmät

4.7.1.1 Yleistä

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 ja turvattu.

Vaatimusten soveltamisesta tiedon siirtämiseen tunnistusjärjestelmän alihankkijalle määrätään säännöksessä 5.

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.

Vaihtoehtoiset sääntelytavat, 7.1 tietoliikenteen salaus. Virasto on arvioinut säännöksen 7.1 valmistelussa toimialapalautteessa ehdotettua vaihtoehtoa, että määräyksen luettelo korvattaisiin kokonaan viittauksella NCSA:n [37] ohjeeseen. Virasto katsoo ensinnäkin valvontakokemuksen perusteella, että vähimmäisvaatimukset on edelleen tarpeellista määrätä yksiselitteisesti. Toiseksi virasto katsoo, että NCSA:n ja SOGIS MRA:n [38] 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 vaatimuksia sidota kansallisen tai kansainvälisen turvaluokitellun tiedon vaatimustasoon.

4.7.1.2 Säännös 7.1.1 pakolliset salausmenetelmät

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 *Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset suojaustasot (ohje 28.11.2018, dnro 190/651/2015)* salaustuoteratkaisujen turvallisuuden arviointia varten niissä tilanteissa, joissa tietoa siirretään ei-luotetussa verkossa. [39]

Tavoitteena on korotetulla varmuustasolla 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 hyväksynnit. Tehtävä perustuu EU:n neuvoston turvallisuussäännöstöön (2013/488/EU) ja lakiin kansainvälisistä tietoturallisuusvelvoitteista (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 [40]

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. Säännökseen lisätään EdDSA. Säännökseen lisätään soveltuminen epäsymmetriseen salaukseen, koska käytettäessä RSA:ta määräyksen säännöksen 9 mukaiseen sanomien salaamiseen on kysymys epäsymmetrisestä salauksesta.

20.5.2022

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.

4.7.1.3 Suositus säännöksen 7.1.1 tiukennuksista korkean varmuustason tunnistuspalvelussa

Vuoden 2016 määräyksen perustelujen suositus 7 §:n 1 momentin eli muutetun määräyksen säännöksen 7.1 soveltamisesta päivitetään. Suosituksessa jätetään pois eräitä määräyksessä lueteltuja kevyimpiä menettelyjä ja arvoja. Suositus vastaa salaustuotteiden hyväksyntäviranomaisen CAA:n arviointiohjeen määrittelyä turvaluokalle TL IV [39].

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 tapahtumakohteisesti. Virasto katsoo kuitenkin, että vaikutus korkean varmuustason tunnistusta käyttäviin luottaviin osapuoliin on vaikeampi arvioida.

Suositus

Huom. Korkean varmuustason vaatimukset on tekstissä **lihavoitu** ja korotetun varmuustason vaatimukset, jotka eivät riitä korkealla varmuustasolla, on **yliviivattu**.

Korkealla varmuustasolla tunnistusjärjestelmässä suositellaan sovellettavaksi määräyksessä säännöksessä 7.1 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-määrittelysten mukaiset DH-ryhmät ~~14~~ - 21, ~~23~~, ~~24~~ ja ~~26~~ (korkealla varmuustasolla **1615 - 21**) toteuttavat edellä mainitut edellytykset.*

20.5.2022

- 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) [39], 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 Scheme Agreed Cryptographic Mechanisms [41].

4.7.1.4 Säännös 7.1.2 sallitut NSCA:n ja SOGIS MRA:n arvioimat salausmenetelmät

Säännös 7.1.2 on uusi.

Sen mukaan säännöksen 7.1.1 1–4 alakohdissa lueteltujen algoritmien ja menetelmien lisäksi voidaan käyttää NSCA:n tai SOGIS MRA:n turvallisiksi arvioimia algoritmeja ja arvoja, jotka ilmenevät määräyksessä viitatuista lähteistä. Lähteistä on käytettävä ajantasaista tuoreinta asiakirjaa.

Virasto pitää NSCA: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.

4.7.1.5 Säännös 7.1.3 asetusten pakottaminen

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.

20.5.2022

Ohjelmistojen ja laitteiden oletustoiminnot perustuvat usein toimivuuden tukemiseen joustavasti mahdollisimman monilla vaihtoehtoisilla määrittäyksillä, 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 päätelaitetekanta tukee hyvin kattavasti vähintään TLS 1.2 -versiota. Käytössä on jo myös versio TLS 1.3.

Virasto arvioi sidosryhmäpalautteen perusteella, että siirtymäaika 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 TLS 1.2 ja TLS 1.3 salausprofiilit

Tässä kohdassa neuvotaan, mitkä ovat säännöksen 7.1 vaatimukset täyttäviä cipher-suiteja.

Kaikkia säännöksessä 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
- 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 [42] 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 [43] listatut TLS 1.3 ciphersuitet

<https://datatracker.ietf.org/doc/html/rfc8446>

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

4.7.4 Lähteet kansallisesti tai kansainvälisesti suositelluista salausratkaisuista

- Liikenne- ja viestintäviraston NCSA-toiminnon (National Communications Security Authority, NCSA-FI) Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset suojaustasot (ohje 28.11.2018 dnro 190/651/2015) [39]
 - o <https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf>
 - o NCSA-toiminnon hyväksymät salausratkaisut (1.7.2020 dnro 1240/651/2017) [44] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/NCSA_salausratkaisut.pdf
 - o yleistä NCSA-FI tietoa: <https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/ncsa>
- SOGIS-MRA SOGIS Agreed Cryptographic Mechanisms (version 1.2 January 2020) [41]
 - o <https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf>
 - o Tällä hetkellä tuoreempi kuin NCSA-FI:n lista ja sisältää enemmän algoritmeja, joita ei vielä hyväksytty/listattu Suomessa. Päivitetään joka toinen vuosi.
 - o Yleistä SOGIS MRA tietoa: https://www.sogis.eu/uk/supporting_doc_en.html#:~:text=The%20document%20%20%20SOG%20DIS%20Crypto,by%20all%20SOG%20DIS%20participants
- IANA (Internet Assigned Numbers Authority)
 - o IKEv2-määrittelyt [40]: <http://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml>
 - o IANA:n ciphersuitet [40]: <http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4>
- RFC 7905 ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS) [42]
 - o <https://tools.ietf.org/html/rfc7905>

- RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3 [43]
 - o <https://datatracker.ietf.org/doc/html/rfc8446>
- eIDAS yhteistyöverkoston (Cooperation Network) [45] tekninen spesifikaatio eIDAS Cryptographic Requirements for the Interoperability Framework, TLS and SAML, Version 1.2, 31 August 2019 [46]
 - o <https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20Cryptographic%20Requirement%20v.1.2%20Final.pdf?version=2&modificationDate=1571068651805&api=v2>
 - o Yleistä eIDAS Cooperation Network -tietoa: <https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Cooperation+Network+Resources>
- ETSIn standardit tai spesifikaatiot
 - o Feb 2019 - ETSI TS 119 312 V1.3.1 (2019-02) "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites" [47]
 - o <https://ec.europa.eu/cefdigital/wiki/display/EIDTECHSUB/Security+Profile+v1.3>
- NIST SP 800-52 Rev. 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations [48]
 - o <https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final>

4.8 Säännös 8 Tietoliikenteen osapuolten varmentaminen

4.8.1 Yleistä

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.

Säännöksessä 8.2 määrätään tietoliikenneyhteyden luottamussuhteen ylläpidosta.

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

Siirtymäajoista ks. säännös 24.

Muut ohjauskeinot

Ohje. Osapuolten varmentamisen ja avaintenvaihdon käytännöistä on tähän asti puuttunut viranomaisen ohje.

20.5.2022

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.

4.8.2 Säännös 8.1 Tietoliikenneyhteyden osapuolten tunnistaminen

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.

Suora kahdenvälinen menettely määräyksessä tarkoittaa sitä, että osapuolen varmenne ja salausavaimet on toimitettava siten, että haltijasta voidaan nimenomaisesti varmistua. Haltijan todentaminen tarkoittaa sopimusosapuolena olevan organisaation todentamista. Määräyksessä ei oteta tyhjentävästi kantaa menettelyn yksityiskohtiin ja siihen, mikä on riittävä tapa tunnistaa toinen osapuoli. Esimerkiksi vahvan sähköisen tunnistamisen käyttäminen on hyvä käytäntö. Osapuolten välillä tehdään aina sopimus, joten käytännön toimet on mahdollista yhdistää sopimusprosessiin. Määräyksessä ei oteta kantaa siihen, miten organisaation edustamisoikeus sopimusta tehtäessä varmistetaan.

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, Qualified Signature/Seal Creation Device) ja tämä turvaa sen, että allekirjoituksen tai leiman luomisessa käytettävät avaimet ovat oikean henkilön hallinnassa.

Ks. eIDAS-asetus [3]

20.5.2022

Art. 35.2: 2. Hyväksyttyyn sähköiseen leimaan liitetään oletettava 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 reaali maailman 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 [32] käytettäessä *jwtks_uri* -osoite ei yksistään riitä luotettavaan osapuolen varmentamiseen, vaan on käytettävä myös muita menettelyjä. *Jwtks_uri* -osoitteen varmistaminen myöskään kiinteän IP-osoitteen perusteella ei ole riittävä varmistus toisesta osapuolesta. Niin ikään SAML-protokolla käytettäessä on todennettava metadatan allekirjoittaja.

4.8.3 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.

8.2.a) 8.1 kohdan mukaisella menettelyllä

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

Alakohtien b ja c menettelyissä nojataan perustamisvaiheessa rakennettuun luottamukseen.

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

20.5.2022

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 b alakohdan mukaisesti varmistettuja tietoliikenneyhteyksiä käytetään jo jossain määrin luottamusverkoston sisällä ja vaihtoehton voi olettaa olevan tarkoituksenmukaisesti toteutettavissa tunnistuspalveluiden välillä. Tämä vaihtoehto mahdollistaa sanomien suojaamisessa käytettävien avainten uusimisen automatisoinnin.

Luottavien osapuolten tietoliikenteen varmentamisessa *certificate pinning* voi olla epä-tarkoituksenmukainen. 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. Kiinnityksissä yhteyksissä osapuolet normaalisti hankkivat itse omat varmenteensa, mutta tyypillisesti mTLS-käyttötapauksessa toinen osapuoli toimittaa varmenteen (client certificate) omalle asiakkaalleen.

8.2.c) allekirjoittamalla uudet avaimet 8.1 kohdan mukaisesti toimitetulla avaimella tai sellaisesta ketjutetulla avaimella

20.5.2022

8.2.c) alakohdan menettely perustuu siihen, että luotetaan perustamismenettelyllä aikaisemmin toimitettuun avaimen ja varmenteeseen. Uusi avain allekirjoitetaan aikaisemmin toimitetulla avaimella. OSI-mallin kannalta 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 tai sellaisesta ketjutetulla avaimella. Virasto katsoo, että hyvän tietoturvakäytännön mukaisesti säännöksen 8.1 mukainen menettely on hyvä tehdä vähintään kahden vuoden välein.

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) alakohdan mukainen uusien jwks-avainten (OpenID Connect -protokollaa käytettäessä) allekirjoittaminen ja salaaminen luotetuilla avaimilla. Tämä ei niinkään ole kovenusvaatimus ohjelmistoihin, vaan edellyttäisi kokonaan uuden toiminnon rakentamista luottavien osapuolten järjestelmiin. Määrittelyyn liittyvät osat sinänsä olisivat olemassa, mutta yhteensopiva toteutus edellyttäisi koordinoitua ja yhteistä kehittämistä.

Viraston käsityksen mukaan uusimista ei siis välttämättä voida toteuttaa automaattisesti siten, että allekirjoituksen varmentaminen sidottaisiin nimenomaisesti säännöksen 8.1 mukaisesti toimitettuun varmenteeseen/avain-kokonaisuuteen. Jos kuitenkin pystytään varmistumaan siitä, että tarkistus sidotaan nimenomaisesti säännöksen 8.1 mukaisesti toimitettuun varmenteeseen ja avaimen, 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 määrittääkseen menettelyn, jota ei ole standardissa valmiina eli kehitystyö olisi tehtävä luottamusverkostossa. Jos menettely ei olisi kaikille yhdenmukainen, yhteensopivuus tunnistusvälityspalveluiden ja luottavien osapuolten välillä ei olisi mahdollista. Epäyhteensopivuudet ja virheet aiheuttavaisivat korjaus- ja neuvontaprosessitarvetta.

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

Virasto ei ole tarkistanut, onko SAML-standardissa [31] valmis määrittely metadatan allekirjoittamiselle manuaalisesti toimitetuilla avaimilla.

4.8.4 Yhteenvedo säännöksen 8.2 teknisestä soveltamisesta

Virasto arvioi, että ainakin seuraavat standardin mukaiset vaihtoehdot ovat käytettävissä:

- sanomatason salausvaatimus ja säännöksen 8.1 mukainen salausavainten vaihto, jos käytössä on TLS suojattu yhteys, jossa ei ole käytössä certificate tai key pinning,

20.5.2022

- käytössä on päästä päähän suojattu TLS yhteys, jossa säännöksen 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.

4.8.5 Säännöksen 8 tavoitteet ja vaikutusarviointi

4.8.5.1 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.

4.8.5.2 Tiukennus standardien 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 reaaliaikaisen asiointimenettelyllä sopimuksen tekemisen yhteydessä. Tällä käytännöllä pystyttiin identifioimaan tietoliikenteen toinen osapuoli luotettavasti ja varmistamaan 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 tietoliikennesyhteyksien 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.

20.5.2022

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

Vaihtoehtoon arviointi. Valmistelussa on harkittu vaihtoehtona sitä, että määriteltäisiin varmenteet, joihin voisi luottaa ilman kahdenvälisen toimittamisen menettelyn vaatimusta. Esimerkiksi eIDAS-asetuksen mukaisesti hyväksytty verkkosivun todentamisen varmenne (QWAC) tai leiman (eSeal) varmenteet tai EV-varmenteet olisivat kuitenkin kustannustekijä ja epätodennäköistä, että yritykset hankkivat näitä. Virasto arvioi myös, että avaintenhallinta ei silti ole taattu.

Kuten edellä on todettu, 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.

4.8.5.3 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.

Teknisiltä valmiuksiltaan tunnistuspalvelut ja niitä käyttävät asiointipalvelut voivat erota merkittävästikin. Erityisesti muilla kuin suurilla sähköisten asiointipalveluiden tarjoajilla omat tekniset valmiudet voivat olla vähäiset ja ne voivat olla sähköisen asiointin toteuttamisessa teknisten alihankkijoiden varassa. Seuraavissa kohdissa arvioidaan asiointipalvelulle aiheutuvia teknisiä vaatimuksia.

4.8.5.4 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 kuvatun *jwks-urin* perusteella. Luottavien osapuolten käyttämien varmenteiden laatu vaihtelee paljon sen suhteen, perustuuko varmenteen haltijan todentaminen tämän omaan ilmoitukseen vai todentaako varmenteen myöntäjä haltijan jotenkin.

20.5.2022

Ks. Liikenne- ja viestintäviraston suositus 213/2021 S OpenID Connect Protocol Profile for the Finnish Trust Network [32], kohta 2.3

The use of extended validation (EV) certificates is RECOMMENDED.

Vaatus 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 sopimuksen tekemiseen liittyy käyntiasiointi, samassa yhteydessä on mahdollista vaihtaa tarvittavat avaimet.

Tavallisemmin sopimukset tunnistuspalvelusta luottavan osapuolen kanssa kuitenkin tehtäen sähköisesti ja tällöin joudutaan määrittelemään tarpeeksi **luotettava sähköinen tapa toimittaa osapuolen julkinen avain**. Määräyksessä on esimerkkinä suoraan eIDAS-asetuksessa luotettavaksi säädetty tapa. Muut 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 tarjoaa 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 niistä selvillä. Tunnistus- ja luottamuspalvelulain 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 viraston arvion mukaan sinänsä paikallaan ja hyvä käytäntö.

4.8.5.5 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.

20.5.2022

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 samomasalla. 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 kovenusvaatimus, että TLS-yhteyden säännöksen 7 mukainen salaus on konfiguroitava siten, että siinä käytetään vain tiettyä luotettua avainparia. Tämä edellyttää huolellista, mutta verraten tavanomaista teknistä määrittelyä ohjelmistoissa.

Jos avaimen päivittämisen turvallisuus halutaan perustaa 8.2.b) alakohdan 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 varmenteiden 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 säännösten 8.1 ja 8.2.b) menettelyjen kovennustarpeet ovat viraston käsityksen mukaan sinänsä kohtuullisen helposti luottavan osapuolen tehtävissä, mutta ne edellyttävät sitä, että asiaan liittyvät 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 alihankkija ja tunnistus liittyy johonkin laajempaan ICT-kokonaisuuteen. Muutokset aiheuttavat myös kustannuksia luottaville osapuolille. Osapuolten varmentaminen 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 siirtymäaika etenkin suhteessa asiointipalveluihin ja muutosten läpivieminen edellyttää luottamusverkoston yhteistoimintaryhmän ja Liikenne- ja viestintäviraston yhteistyötä neuvonnassa ja viestinnässä.

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 lii-

20.5.2022

kenteen 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 säännöksen 8.2 menettelyvaihtoehtoihin. (Kovennetuilla määrittelyillä TLS with DNSSEC, JWT Encryption, Rotation of encryption keys (JWKS)).

Vrt. Financial-grade API (FAPI) WG [51] <https://openid.net/wg/fapi/>

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 7–9 §:n vaatimukset tunnistussanomien 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 määritettyä. Pohjaoletuksena on luonnollisesti, että tietoliikenneyhteys ("TLS-putki") on salattu määräyksen säännöksen 7 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, [26] 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 tunnistussanomien suojaamisvelvoitetta**

20.5.2022

sen perusteella, millainen henkilötieto tunnistussanomassa välitetään ("alakäinen" vrt. "121212+999Å, Alma Virtanen"). Henkilötietojen luokittelulle olisi vaikea määrittellä objektiivisia ja kattavia perusteita ja tekniset toteutukset on yksinkertaisinta tehdä kaikille tunnistustapahtumille samalla tavalla.

4.9.2 Säännös 9.1, 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 tunnistussanomien 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 suojaamisen menetelmällä 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 [52] käyttävän mobiilivarmenratkaisun, 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 tavallisesti käytettäne.

4.9.3 Säännös 9.1.2 tunnistussanomien allekirjoitus

Säännös 9.1.2 on uusi.

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

Vaatimus koskee vain luottamusverkoston tunnistusvälityspalvelun ja luottavan osapuolen välisiä tunnistussanomien eli tunnistuspyyntöjä ja vastaussanomien. 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/liikennesetasolla 9.1.a) alakohdan mukaista varmistettua tietoliikenneyhteyttä. Tarkoitus on erityisesti todentaa ne sovellukset, jotka luottavan osapuolen tietojärjestelmistä pyytävät tunnistusta.

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

Vaikutus/toteutettavuus. Luottavan osapuolen tunnistuspyyntöjen allekirjoitus on tullut esille rajapintasuosituksen valmistelussa. Se on valmistelussa saadun palautteen

20.5.2022

perusteella yleisesti toivottu turvallisuutta lisäävä menettely. Menettely on teknisesti tavanomainen.

Vrt. eIDAS Cryptographic Requirements for the Interoperability Framework, version 1.2 [46]

Rajat ylittävän tunnistamisen teknisten vaatimusten määrittelyssä käytetään kansallisten solmupisteiden välillä 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 tunnistussanomien välittämisessä tunnistuspalvelun ja luottavan osapuolen eli asiointipalvelun välillä käytetään käyttäjän selainta, asiointisovellusta tai päätelaitetta muutoin, sanoman salaaminen säännöksen 7 mukaisen TLS-yhteydellä salaamisen lisäksi on edelleen pakollista.

Käyttäjän selain tai asiointisovellus voi olla sähköisen asiointi- ja tunnistustapahtuman aikana yhteydessä asiointipalveluun, tunnistusvälitykseen ja tunnistusvälineen tarjoajaan. 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 salaamisen menetelmistä, mutta virasto toteaa, että RFC 7519 on tarvittaessa hyvä lähde määrittelyssä.

RFC 7519 JSON Web Token (JWT) [53] <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 [32] 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 and MGF1 with SHA-256	OPTIONAL
alg	JWE	ECDH-ES	Elliptic Curve Diffie-Hellman Ephemeral Static key agreement using Concat KDF	OPTIONAL
enc	JWE	A128GCM	AES GCM using 128-bit key	REQUIRED

4.10 Säännös 10 Tietoturva vaatimukset 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 salaustarpeita 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* [46]

<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 (ilmoituskyynnys)

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

Virastolla on tunnistus- ja luottamuspalvelulain 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

20.5.2022

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. Ilmoitus- kynnystä tai ilmoitettavia tietoja ei ole tarkoitus muuttaa, vaan ainoastaan selkeyttää säännöstä.

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

- tunnistusvälineen myöntäminen väärälle henkilölle,
- sellaiset sulkulistojen toimivuuteen liittyvät häiriöt, joissa ajantasaista sulkulista 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 merkittävänä hyvin matalalla kynnyksellä, samoin esimerkiksi haavoittuvuuksia tai virheitä, jotka vaarantavat tunnistamistiedon oikeellisuuden. Sen sijaan käytettävyys- tai laatuongelmien ilmoitus- kynnys 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 välittämisen asiointipalveluille. 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 tietoturvalisempaa kanavaa.

Luottamusverkoston sisällä välitetyn häiriö- ja uhkatiedon käytölle on säädetty tunnistus- ja luottamuspalvelulain 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.

Säännöksessä 11.2 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 ajan kohta ja arvioitu kesto tai toteutunut kesto, jos se on tiedossa.

Teknisestä tapahtumakuvauksesta tulisi käydä ilmi, mihin osaan tunnistusjärjestelmästä 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 säännöksen 11.1 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.

20.5.2022

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 tarkat verkkoturvallisuuteen liittyvät tiedot on syytä toimittaa muulla tavoin kuten turva-postilla. Ilmoituksen voi toimittaa myös sähköpostilla eid@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.

4.11.4 Säännös 11, harkitut sääntelyvaihtoehdot ja muut ohjauskeinot

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 tarpeellisenä 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 tunnistus- ja luottamuspalvelulaissa ei ole nimenomaisia vaatimuksia tunnistuspalveluiden toimintavarmuudesta, varmistamisesta tai varautumisesta eikä siten toimivaltuutta määrätä niistä.

Ohje, suositus. Ei huomioita.

Yhteissääntely. Luottamusverkoston yhteistoimintaryhmässä on laadittu käytäntö häiriöiden ja uhkien tiedonvaihdesta toimijoiden välillä.

Informaatiolla ohjaaminen. Ei huomioita.

Määräyksen luku 3 Tunnistuspalveluiden yhteentoimivuus

4.12 Säännös 12 Luottamusverkostossa välitettävät vähimmäistiedot

4.12.1 Säännös 12.1 Pakolliset tiedot (attribuutit)

4.12.2 Yleistä

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 yhteentoimivuuasetuksessa (EU) 2015/1501 [5] määriteltyjä tietoja.

Määräyksen säännöksen 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.

20.5.2022

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 etunimi, henkilön sukunimi ja organisaation yksilöivä tunniste. Tunnistus- ja luottamuspalvelulain 7 a §:n perusteella tunnistusvälineen tarjoajan on hankittava ja päivitettävä oikeushenkilön tunnistuspalvelun tarjoamiseksi tarvitsemansa tiedot yritys- ja yhteisörekistereistä.

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.

4.12.3 Uusi attribuutti: luottavan osapuolen nimi

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 6.2.2 määrätään velvollisuudesta näyttää tieto tunnistusvälineen käyttäjälle.

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 ongelmaton. 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 työläisiä 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

20.5.2022

jo määriteltynä rajapinnoissa. Tunnistusvälineen tarjoajalta se edellyttää kentän lisäämistä käytössä oleviin rajapintamäärittelyihin ja käyttäjälle annettavan informaation lisäämistä tunnistuspyynnössä.

Tunnistus- ja luottamuspalvelulain 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 tunnistus- ja luottamuspalvelulain 12 b §:n perusteella tunnistustapahtuman enimmäishintasäätelyn piiriin, mutta hintasäätely koskee tunnistusvälineen tarjoajan tuottamia tietoja, joten säätelyllä 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 tunnistusvälityspalveluista 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 [31, 32]. Sen status on muutettu suositusten päivityksessä pakolliseksi 2021.

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

Informaatiolla ohjaaminen. Ei huomioita.

4.12.4 Säännös 12.2 Valinnaiset tiedot

Säännöksessä 12.2 määrätään valinnaiset tiedot. Attribuutit vastaavat EU:n komission yhteentoimivuusasetuksessa (EU) 2015/1501 [5] 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 momen-*

20.5.2022

tin 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 tunnistussanomien sisältävät 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.

4.12.5 Säännös 12.3. Tunnistuksen pseudonymisointi ("köyhdyttäminen")

Säännös on uusi. Sen tarkoitus on selvittää 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 pseudonymistista 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.

20.5.2022

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 luotettavuudelle 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 maksupalveluiden välillä tietyvästi todennetaan vahvasti vain, että maksaja on maksunsaajalle kerrotun maksukortin haltija, eikä maksupalveluiden välillä välitetä henkilö-tietoja.

Käyttäjää olisi informoitava henkilötietojensa käsittelystä luottamusverkostossa ja luotettavalle 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.

4.12.6 Säännös 12, harkitut sääntelyvaihtoehdot

4.12.6.1 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 [5]. 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.

20.5.2022

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.²

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.

Yhteissäätely. 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.

4.12.6.2 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 ensitunnistustahtauma 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 ennakoarvion 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 tar-

² Ks. Traficomien tutkimuksia ja selvityksiä 2/2021 Sähköisen tunnistamisen markkinat, Sähköisen tunnistaminen turvallisen asiointin mahdollistajana, kohta 5.2 Yritysten tarpeet, Sähköisten asiointipalvelujen näkemyksiä tulevaisuuden tarpeista, s. 53 Lähes kaikki eli 98 prosenttia näkemyksensä antaneista vastaajista pitää vahvan sähköisen tunnistamisen yhteydessä saatavia tietoja riittävinä.

20.5.2022

joaja 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 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 ennakoarvion 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 alkupeäinen 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 näkemyksensä 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 vaatisi 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 myönnettyistä tunnistusvälineistä) toteuttaisi turvallisuustavoitteet ja mahdollistaisi kaikkien ketjutettujen tunnistusvälineiden sulkemisen.

Linjaus. Ei määrätä. 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 notifiomia 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 tällöin välittää solmupisteelle säännöksessä 12 määrätty 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 §:n 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.

20.5.2022

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 notifiointin 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 tunnistus- ja luottamuspalvelulain ja määräyksen vaatimukset tunnistusvälitykselle. eIDAS-asetuksen rajat ylittävän tunnistamisen yhteentoimivuus- ja turvallisuusvaatimukset komission asetuksessa (EU) 2015/1501 [5] 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, 17 §: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 tunnistusvälineen tarjoajan tai tunnistusvälityspalvelun oikeuden näkökulmasta, mikä tunnistus- ja luottamuspalvelulailla ja valtioneuvoston asetuksella on tarkoitus turvata. Tunnistuspalvelu voi täyttää veloitteensa 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 ennakoarviota siitä, että 14 §:n 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 OpenID Connect -protokollien kansallisesti laadittuja profiileja, jotka virasto on julkaissut erillisinä suosituksina vuonna 2018 ja päivittänyt ne vuonna 2021 [31, 32]. 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*

20.5.2022

että ne mahdollistavat yleisesti tunnettujen standardien mukaisten rajapintojen tarjoamisen luottaville osapuolille.

Valtioneuvoston asetuksen 169/2016 (muutettu 1212/2018) [2] 1.1 §:n mukaan *tunnistus- ja luottamuspalvelulain 12 a.2 §:ssä (viittaus on päivittämättä, mutta asiasta säädetään lain 12 a §:n muutoksen jälkeen lain 12 a.3 §:ssä) tarkoitettuja teknisiä rajapintoja ovat*

- 1) tunnistusvälineen tarjoajien välinen rajapinta;*
- 2) tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun 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 kummasakin vähintään yhtä yleisesti käytetyn standardin mukaista teknistä rajapintaa.

Määräysvalmistelussa 2016 arvioitiin seuraavia kysymyksiä: *Millä tarkkuudella rajapintavaatimukset laaditaan määräykseen suhteessa yksittäisiin protokolliin, kuten SAML ja OpenID 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 tietoturva vaatimuksista.*

Vuoden 2016 jälkeen Tupas-protokolla on poistunut käytöstä ainakin vahvassa tunnistamisessa ja mobiilioperaattorit ovat siirtyneet osassa rajapinnoista käyttämään vanhan ETSI mobiilivarmennerajapinnan sijaan OpenID Connectia. OpenID Connect 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 säänteilyllä 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 mobiilivarmenintajien välisissä rajapinnoissa.

Jos syntyy tarvetta ottaa käyttöön uusia protokollia valtioneuvoston luottamusverkoston asetusten tarkoittamana *yleisesti käytetyn standardin mukaisena teknisenä rajapintana*, valmistelussa vaihdetaan tietoa asetuksen tarkoittamassa luottamusverkoston

20.5.2022

yhteistoimintaryhmässä ja virasto arvioi teknisen kehityksen kypsyttää kansallisesti ja kansainvälisesti saatavilla olevan objektiivisen tiedon perusteella.

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

4.14.4 Säännös 14, harkitut säätelyvaihtoehdot

4.14.4.1 Luottaviin osapuoliin vaikuttavat yhteentoimivuusvaatimukset

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

Tunnistus- ja luottamuspalvelulain 12 a §:n mukaan *luottamusverkon 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 vuonna 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.

Määräyksen luku 4 Tunnistuspalvelun arviointikriteerit

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.

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 sähköisen tunnistamisen varmuustasoasetuksessa. Tietoturva- ja yhteentoimivuusvaatimuksia tarkennetaan erityisesti tämän määräyksen 2 ja 3 luvuissa.

20.5.2022

Säännöksessä luetellaan ne tunnistuspalvelun toteutuksen ja tarjonnan toiminnot, joiden osalta säädännön vaatimusten täyttyminen täytyy osoittaa joko ulkoisella tai sisäisellä arvioinnilla. Toimintojen tai osa-alueiden ryhmittely perustuu EU:n komission varmuustasoasetuksen vaatimusten ryhmittelyyn. Säännökseen lisätään kansalliseen luottamusverkostosäätelyyn liittyvän yhteentoimivuuden arviointi.

Yksityiskohtainen arvio ja ohje siitä, mitä säädettyjä ja määrättyjä vaatimuksia arviointivaatimus koskee, esitetään Sähköisen tunnistuspalvelun arviointiohjeessa 211/2019. Ohjeen kohdassa 3 luetellaan osa-alueittain relevantit säännökset ja liitteessä B Tunnistuspalvelun yleinen arviointikriteeristö eritellään vaatimukset alueittain.

Säännöksen 15.1 1) alakohdan osa-alueet kattavat seuraavia asioita.

Tietoturvallisuuden hallinta tarkoittaa määräyksen säännöksen 4 vaatimuksia, jotka tarkentavat tunnistus- ja luottamuspalvelulain 8.1 §:n 5 alakohdan ja varmuustasoasetuksen liitteen kohdan 2.4 johdanto-osan ja kohtien 2.4.3 ja 2.4.7 vaatimuksia.

Määräyksessä ja ohjeessa *tietojen säilyttäminen ja muu käsittely* on yhdistetty kokonaisuudeksi.

Tilat ja henkilökunta tarkoittavat tilaturvallisuutta ja henkilökunnan pätevyyttä ja riittävyyttä tunnistus- ja luottamuspalvelulain 8.1 §:n 5 alakohdan ja 13 §:n sekä varmuustasoasetuksen liitteen kohdan 2.4.5 mukaisesti.

Tekniset toimenpiteet (engl. *controls*) pitävät sisällään laajasti tietoturvatyökalut, joilla tunnistusjärjestelmän ja tunnistusmenetelmän eheys ja luottamuksellisuus turvataan. Kokonaisuuteen kuuluvat tietojärjestelmä-, tietoliikenne- ja käyttöturvallisuuden lisäksi salaustekniset ratkaisut ja poikkeamien havainnointi, hallinta ja informointi. Tunnistusjärjestelmän tietoturvallisuudesta säädetään tunnistus- ja luottamuspalvelulain 8.1 §:n 4 kohdassa ja varmuustasoasetuksen liitteen kohdissa 2.2.1, 2.3.1 ja 2.4.6. Häiriöilmoituksista säädetään lain 16 §:ssä. Määräyksessä teknisiä toimenpiteitä koskee luku 2.

Yhteentoimivuus luottamusverkostossa pitää sisällään attribuuttien välittämisen ja rajapinnat. Määräyksessä yhteentoimivuutta koskee luku 3.

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 määrätty 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 olennaisesti erilainen kuin tunnistus- ja luottamuspalvelulain ja tämän määräyksen mukaiset arviointiperusteet. ISO-standardien avulla sertifioitu tai muutoin määritelty tietoturvallisuuden hallintajärjestelmä luo hallinnollista kerrosta ja pikemminkin puitteita tietojen käsittelyn ja palveluiden hallintaan eikä sertifiointi itsessään osoita organisaation yksittäisten tai kaikkien palveluiden tietoturvallisuuden ja tietosuojan tason riittävyyttä tai teknisten tietoturvatyökalujen olemassaoloa.

Vrt. varmuustasoasetuksen soveltamisohje, LOA guidance, kohta 2.4 [22]

20.5.2022

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.

Säännöksen 15.1 2) alakohdan osa-alueet kattavat seuraavia asioita. On hyvä huomata, että tässä kuvataan vaatimuksia yleisellä tasolla ja erilaiset erityistilanteet on arvioitava lain ja sen perustelujen valossa. Eri toimenpiteiden rajanveto ei ole yksiselitteistä esimerkiksi, kun uusitaan vain yksittäinen todentamistekijä.

Tunnistusmenetelmän *hakeminen ja rekisteröinti* tarkoittavat tunnistusvälineen hakemismenettelyä ja tunnistamisessa edellytettujen henkilötietojen keräämistä ja tarkistamista tunnistus- ja luottamuspalvelulain 6 ja 7 §:n mukaisesti.

Hakijan henkilöllisyyden todistaminen ja varmentaminen tarkoittavat tunnistus- ja luottamuspalvelulain 17 §:n mukaista tunnistusvälineen hakijan ensitunnistamista mukaan lukien mm. luotettujen henkilöllisyystodistusten aitouden tarkistaminen ja voimassaolon varmistaminen lain 7 b §:n mukaisesti.

Tunnistusmenetelmän ominaispiirteet ja laatiminen tarkoittavat tunnistusmenetelmässä käytettävien todentamistekijöiden valintaa sekä todentamistekijöiden ja todentamismekanismin ominaisuuksia eli menetelmän luotettavuuden kokonaisuutena turvaavia ominaisuuksia tunnistus- ja luottamuspalvelulain 8 a §:n ja 8.1 §:n 4 kohdan sekä varmuustasoasetuksen liitteen 2.2.1 ja 2.3.1 kohdan mukaisesti.

Tunnistusmenetelmän *myöntäminen, toimittaminen ja aktivointi* tarkoittavat tunnistus- ja luottamuspalvelulain 20 ja 21 §:n ja varmuustasoasetuksen liitteen 2.2.2 kohdan mukaisia menettelyjä ja toimenpiteitä, joilla tunnistusväline kytketään haltijaan ja saatetaan haltijalle ja otetaan käyttöön.

Voimassaolon keskeyttäminen, peruuttaminen ja uudelleen aktivointi tarkoittavat tunnistus- ja luottamuspalvelulain 25 ja 26 §:n mukaisia sulkupalveluita ja -toimenpiteitä haltijan tai tunnistuspalvelun aloitteesta.

Uusiminen ja korvaaminen tarkoittavat tunnistus- ja luottamuspalvelulain 22 §:n ja varmuustasoasetuksen liitteen 2.2.4 kohdan mukaista uuden tunnistusvälineen toimitamista aikaisemman tilalle. Toimittaminen voi liittyä myös lain 26 §:n soveltamiseen.

Todentamismekanismi tarkoittaa tunnistusvälineen haltijan autentikointimenettelyä tunnistus- ja luottamuspalvelulain 8 a §:n ja varmuustasoasetuksen liitteen 2.3.1 kohdan mukaisella dynaamisella todentamisella. Todentamismekanismin vaatimukset koskevat osaltaan myös tunnistusvälityspalvelua, kun se osallistuu sanomien välittämiseen autentikoinnissa.

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 toimieliimen antamia säännöksiä tai ohjeita, julkaistuja ja yleisesti tai alueellisesti sovellettuja tietoturvallisuutta koskevia ohjeita ja yleisesti käytettyjä tietoturvallisuusstandardeja tai menettelyjä.*

20.5.2022

Virasto ei määrittää 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 [21]. 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 tietoturvasuusstandardeja, 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 siitä, 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

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

- ISO/IEC 27001 [11]
- Katakri [12]
- PiTuKri [26]
- PCI DSS, PCI/QSA [20]
- Webtrust Trust Services Principles and Criteria for Certification Authorities ja Webtrust for Certification Authorities - SSL Baseline Requirements Audit Criteria [54]
- Information Security Forum (ISF) Standard of Good Practice [55]
- ISF:n IRAM-kriteeristö (Information Risk Analysis Methodology) [55]
- ISRS 4400 [56] ja ISAE 3000 [57]
- Vahti-ohjeet [58]
- Tiedonhallintalautakunnan suositukset [59]
- Euroopan keskuspankin ohjeet
- FIVA:n määräykset tai ohjeet [60]
- FIVA:n määräys ja ohje 2.4 "Asiakkaan tunteminen - rahanpesun ja terrorismin rahoittamisen estäminen" [61]
- Euroopan keskuspankin SREP cyber risk questionnaire [62]
- BIS, Bank for International Settlements, ohjeet External audits of banks ja supplemental note to External audits of banks - audit of expected credit loss [63]
- Ruotsin Finansinspektionin (FFFS) ja Suomen Finanssivalvonnan määräyksiä ja ohjeita koskien sisäisen tarkastuksen organisointia ja toimintaa
- IIA, The Institute of Internal Auditors [64] kansainvälisen kattojärjestön ohjeita, sääntöjä ja tarkastusperiaatteita
- ETSIn standardit [66, koottu luottamuspalvelujen linkit]

4.15.4 Määräykselle vaihtoehtoiset ohjauskeinot ja viraston arviointiohje

Suositus/ohje. Liikenne- ja viestintäviraston sähköisen tunnistuspalvelun arviointiohje 211/2019 [21] on päivitetty vuonna 2019 perusteellisesti huomioimaan kaikki säädetty vaatimukset ja siihen on lisätty mobiilisovelluksia koskeva erityiskriteeristö. Ohjetta on tarkoitettu ylläpitää siten, että sen ajantasaisen version käyttäminen kattaa kaikki säädetyt vaatimukset.

Yhteissääntely. Alalle tulon kynnyksen ja mahdollisten kilpailuoikeudellisten kysymysten kannalta on parempi, että viranomaisen 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 ilmaiset ovat osittain lähtöisin sähköisen tunnistamisen varmuustasoaasetuksen 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.

20.5.2022

2) *julkaistut ilmoitukset ja käyttäjätiedot, kuten tunnistusperiaatteet, tietosuojaperiaatteet, käyttörajoitukset, sopimusehdot ja hinnastot.* Kohdan vaatimukset liittyvät tunnistus- ja luottamuspalvelulain 12 b, 14, 15 ja 18 §:n 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 säännöksen 15 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

Viestintäviraston ohjeessa 214/2016 O tunnistus- ja luottamuspalveluiden ilmoituksista [65] 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 [5] mainitaan oletuksena standardiin ISO/IEC 27001 [11] perustuva tietoturvallisuuden hallinta. Määräyksessä vahvistetaan tämä oletama, koska tämä on myös käytännössä Digi- ja väestötietoviraston toimintaan soveltuva ratkaisu. Komission täytäntöönpanopäätöksessä säädetään joitain vaatimuksia solmupisteen toiminnalle.

Määräyksen luku 5 Tunnistuspalvelun arviointielimen pätevyys

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.

20.5.2022

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 perusteltuja.

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 alakohdassa 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 ilmeistä selkeästi auditoinnin kohdistuminen tosiasiasa 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 sovellettava perustellusti tunnistusjärjestelmän vaatimusten arviointiin.

Määräyksen 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 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.

eIDAS-asetuksessa [3] 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 [66]. Standardeihin on koottu yksityiskohtaiset konkreettiset vaatimukset, joiden täyttyminen varmistaa sen, että luottamuspalvelun tarjoaja on eIDAS-asetuksen mukainen.

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

20.5.2022

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) [67] <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 20.1.1 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 [66]

Standardi sisältää yleiset palveluriippumattomat vaatimukset kaikille hyväksytyn luottamuspalvelun tarjoajalle. Se sisältää vaatimuksia mm. riskien arvioinnille, tietoturva-politiikalle 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 hyväksytyjen 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 [66]

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 [66]

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

Standardi sisältää vaatimukset eIDAS-asetuksen mukaisia hyväksytyjä 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 [66]

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 (EU) 910/2014 [3] 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 registered 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 hyväksytyjen luottamuspalveluiden arviointikriteerit.

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

Vaatimusten sisältöä tarkentamaan Euroopan telestandardointi-instituutti ETSI on laatinut komission mandaatilla määräystekstissä luetellut standardit. Standardeihin on koottu yksityiskohtaiset konkreettiset vaatimukset, joiden täytyminen 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 viitatus 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 319 412 osat 2-4) sekä hyväksytyjen 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 hyväksytyjä luottamuspalveluntarjoajia ja eri luottamuspalveluja koskevat standardit. Tekniset spesifikaatiot (ETSI TS) eivät ole vielä vahvistettuja, joten niihin ei viitata määräyksessä.

Taulukko: Hyväksytyjen luottamuspalvelun tarjoajien ja luottamuspalveluiden standardit			
Standardiviitteet löytyvät koottuna viiteluettelosta, valmiit standardit [66] ja tekniset spesifikaatiot [68]			
Palvelu, eIDAS-artikla	valmis standardi	tekninen spesifikaatio	
hyväksytty luottamuspalveluntarjoaja (kaikki luottamuspalvelutyypit)	ETSI EN 319 401	ks. ETSI TS 119 312 V1.3.1 (2019-02)[47]	
varmenteita tarjoava luottamuspalveluntarjoaja (kaikki hyväksytyt varmenteet)	ETSI EN 319 411-1 ETSI EN 319 411-2		
Allekirjoitusvarmenne	ETSI EN 319 412-1		

artikla 28	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 artikla 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 leiman validointi artikla 40, viittaus artiklaan 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 artikla 34		ETSI TS 119 511 ETSI TS 119 512
sähköisen leiman säilyttäminen Artikla 40, viittaus artiklaan 34		ETSI TS 119 511 ETSI TS 119 512
sähköinen rekisteröity jakelupalvelu (eDelivery) artikla 44	ETSI EN 319 521 ETSI EN 319 522 1-4	ETSI TS 119 524

Määräyksen 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 [69] 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 viitattut standardit.

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

The diagram illustrates the TSP Assessment Scheme. It shows the flow of information and assessment between various entities:

- TSP (Trusted Service Provider)** (grey box) sends an **Assessment request** (dashed arrow) to the **Conformity Assessment Body** (yellow box).
- The **Conformity Assessment Body** sends an **Assessment Report** (solid arrow) to the **Supervisory Body** (orange box).
- The **Supervisory Body** sends a **Notification** (dashed arrow) back to the **TSP**.
- The **Supervisory Body** sends information to the **Trusted List** (orange box).
- The **Trusted List** is part of the **TSP Assessment Scheme** (dashed line boundary).
- The **Trusted List** is based on the **Assessment Report** TSP status set in the **Trusted List** by the **National Authority** (blue callout).
- The **Supervisory Body** and **Conformity Assessment Body** are linked by a double-headed arrow.
- The **Conformity Assessment Body** is supported by **Assessors** (light blue box) and **Assessment Criteria** (blue box).
- The **Conformity Assessment Body** is linked to the **National Accreditation Body** (pink box) by a double-headed arrow.
- The **National Accreditation Body** is linked to the **European co-operation for Accreditation (EA)** (pink dashed box) by a double-headed arrow.
- The **National Accreditation Body** checks for **Conformity Assessment Body Competence in line with pan-European Accreditation Scheme** (blue callout).

(Lähde Euroopan tietoturvallisuusviraston ENISAn dokumentti *Auditing Framework for TSPs, Guidelines for Trust Service Providers, Versio 1.0 - December 2014* [70])

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

Koska komissio ei ole antanut asiaa koskevaa täytäntöönpanosäädöstä, seuraavassa kappaleessa kuvatus 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* [71]. 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.

20.5.2022

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* [72].

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. Osaa 2 ei ole vielä vahvistettu, vaan se on tekninen spesifikaatio (TS). Standardia ei siten määrätä viitteeksi, mutta sitä voidaan soveltaa.

https://www.etsi.org/deliver/etsi_ts/119400_119499/11940302/01.02.01_60/ts_11940302v010201p.pdf
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 [73]

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. Osaa 3 ei ole vielä vahvistettu, vaan se on 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 [74]

Liikenne- ja viestintäviraston 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 *eIDAS-luottamuspalvelun arviointikertomuksesta* [75]. Ohjeen sisältö luottamuspalveluiden arvioinnista on sama kuin ohjeessa 215/2016.

Määräyksen 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 nimetyksi sertifiointilaitokseksi, se voi hakea hyväksyntää Liikenne- ja viestintävirastolta tunnistus- ja luottamuspalvelulain 36 §:n mukaisesti ja pykälässä säädettyillä edellytyksillä.

20.5.2022

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) [38] on eurooppalainen järjestelmä sertifiointien keskinäiseen tunnustamiseen. Mukana on kahdeksan maata, joilla on omia sertifioidjia (*qualified/authorising participant*) ja kaksi maata (*consuming participant*), joilla ei ole omia sertifioidjia (mm. Suomi).

Pätevyys sertifiointilaitoksena toimimiseen edellyttää, että toimijalla on kyky todentaa luontivälineen vaatimukset, jotka asetetaan komission täytäntöönpanopäätöksellä (EU) 2016/650 [8].

EU:n tai ETA-alueen jäsenvaltioiden komissiolle ilmoittamien jäsenvaltioissa hyväksyttyjen sertifiointilaitosten tekemät sertifiointit 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 [8].

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.

Komission täytäntöönpanopäätöksen liitteessä vahvistetuista standardeista yleinen IT-tietoturvallisuuden arvioinnin standardi ISO/IEC 15408 Information technology -- Security techniques -- Evaluation criteria for IT security-standardisarja [23] tunnetaan Common Criteria -vaatimuksina.

Määräyksen luku 9 Siirtymäsäännökset ja allekirjoitukset

4.24 Säännös 24 Määräyksen voimaantulo ja siirtymäsäännökset

Määräys tulee voimaan 1.6.2022.

4.24.1 Säännöksen 6.2 ja 12.1 siirtymäaika

Säännöksen kohdan 6.2.1 eli tapahtumatunnisteen näyttämisen siirtymäaika tarkoittaa sitä, että tieto tulee näyttää tunnistusvälineen käyttäjälle tunnistustapahtumissa viimeistään 1.6.2023.

Vaatus on tunnistuspalveluiden tarjoajien tehtävissä eikä edellytä toimenpiteitä luottavilta osapuolilta. Monissa tunnistuspalveluissa toiminto on jo entuudestaan käytössä. Toteutus edellyttää tunnistusvälineen tarjoajalta teknisiä määrittelyjä, joilla luodaan taustajärjestelmässä merkkijono, QR-koodi tai muu näytettävä viesti, joka esitetään asiointin selainistunnossa tai sovelluksessa ja tunnistusvälineessä näytettävässä vahvistuspyynnössä. Virasto arvioi, että vaadittavat tekniset määrittelyt ovat verraten vähäisiä, mutta siirtymäaika on tarpeen, jotta tarvittavat määrittelyt pystytään suunnittelemaan ja toteuttamaan.

Säännöksen kohtien 6.2.2 ja 12.1.4) eli luottavan osapuolen nimen näyttämisen siirtymäaika tarkoittaa sitä, että luottavan osapuolen nimi tulee näyttää käyttäjälle tunnistustapahtumissa viimeistään 1.6.2023.

20.5.2022

Vaatimuksen toteuttaminen edellyttää toimenpiteitä sekä tunnistuspalveluilta että jos-sain määrin luottavilta osapuolilta.

Tunnistusvälityspalvelun ja luottavan osapuolen on sovittava esitettävät nimet. Tätä käsitellään perustelumuistion kohdassa 4.12.3.

Luottavan osapuolen nimen näyttämiseen liittyy myös säännös 9.1.2, jossa edellytetään, että luottava osapuoli allekirjoittaa tunnistuspyynnön. Allekirjoittamisessa käytettävästä avaimesta ja 9.1.2 siirtymäajasta määrätään säännöksessä 24.4.

Vaatimuksen toteuttaminen edellyttää teknisiä määrittelyjä tunnistusvälityspalvelun ja tunnistusvälineen tarjoajan rajapinnassa tiedon välittämiseksi. Attribuutti on ollut määriteltynä rajapintasuosituksissa jo ennestään ja vuoden 2021 suositusten päivityksessä se on muutettu pakolliseksi. Suositus on valmisteltu tiiviissä yhteistyössä toimijoiden kanssa. Yhteentoimivuuden valmiudet ovat siten hyvät.

Vaatimuksen toteuttaminen edellyttää teknisiä määrittelyjä tunnistusvälineessä näytettävässä vahvistuspyynnössä. Tämä koskee ensisijaisesti tunnistusvälineen tarjoajaa, mutta jos tunnistusvälityspalvelu esittää tunnistusvälineen käyttäjälle tietoja tunnistustapahtuman välivaiheissa, tiedon näyttäminen edellyttää toimenpiteitä myös tunnistusvälityspalvelulta.

Virasto arvioi, että vaadittavat tekniset määrittelyt ovat verraten vähäisiä. Osa tunnistuspalveluista on toteuttanut toiminnon jo ennestään. Virasto arvioi, että siirtymäaika on tarpeellinen teknisten määrittelyjen toteuttamiseksi ja jotta tunnistusvälityspalveluilla on mahdollisuus sopia esitettävät nimet luottavien osapuolten kanssa, jos tätä ei ole aikaisemmin tehty.

4.24.2 Säännöksen 8 siirtymäajat

Säännöksen 24.3 a) alakohdan siirtymäaika tarkoittaa sitä, että luottamusverkoston tunnistuspalveluiden välisillä tietoliikenneyhteyksillä on 1.6.2023 mennessä varmistettava, että käytössä on säännöksen 8.1 mukaisesti toimitettu varmenne.

Säännöksen 24.3 b) alakohdan siirtymäaika tarkoittaa sitä, että tunnistusvälityspalvelun on viimeistään 1.6.2023 käytettävä 8.1 mukaista menettelyä liittäessään uusia asiointipalveluasiakkaita tunnistusjärjestelmäänsä.

Samoin tunnistusvälityspalvelun on tunnistettava viimeistään 1.6.2023 ne asiointipalveluasiakkaat, jotka tunnistusvälityspalvelu on liittänyt tunnistusjärjestelmäänsä ilman säännöksen 8.1 mukaista tunnistamista. Varmenne tai avain on vaihdettava säännöksen 8.1 mukaisesti. Siirtymäaika tarkoittaa sitä, että koko vanha sopimus-kanta on saatettava uuden vaatimuksen mukaiseksi viimeistään 1.6.2023 riippumatta siitä, minä ajankohtana sopimus on alun perin tehty.

Vaatus siitä, että säännöksen 8.2 vaatimus on otettava käyttöön viimeistään 1.6.2023 tarkoittaa sitä, että tästä ajankohdasta lähtien varmenteiden ja avainten päivittäminen on aina tehtävä määräyksen vaatimusten mukaisesti.

Vaatimusten toteuttaminen edellyttää menettelyjen ja prosessien määrittelyä tunnistamisessa ja avainten ja varmenteiden toimittamisessa sekä prosessien määrittelyä vaihtosyklin seurannassa. Teknisesti vaatimusten toteuttaminen edellyttää erilaisia asetusten määrittelyjä palvelinohjelmistoissa sekä tunnistuspalveluissa että asiointipalveluissa.

Luottamusverkoston tunnistuspalveluiden lukumäärä on rajallinen ja niillä on tekninen kyvykyys vaatimusten täyttämiseen. Suunnittelu edellyttää kuitenkin jonkin verran

20.5.2022

aikaa ja on tarpeen varata aikaa myös tiedonvaihdon menettelyistä, jotta niitä voidaan haluttaessa yhtenäistää luottamusverkoston sisällä.

Tunnistusvälityspalvelun kannalta vaatimukset vaikuttavat siihen, että sen on sopimussuhteissaan luottavien osapuolten kanssa huolehdittava teknisten vaatimusten informoinnista, sillä ei ole todennäköistä, että nämä olisivat niistä selvillä.

Säännösten 8.1 ja 8.2 teknisiä vaatimuksia asiointipalveluille arvioidaan kohdassa muistion 4.8.5.5. Menettelyjen edellyttämät kovennostarpeet asiointipalveluiden järjestelmissä edellyttävät myös sitä, että asiaan liittyvät prosessit ja ylläpito- ja toteutusvastuut huomioidaan asiointipalvelun teknisessä ylläpidossa ja sen mahdollisessa alihankinnassa. Uusien asiakkaiden kohdalla menettelyt voidaan viraston arvion mukaan ottaa käyttöön heti, kun tunnistusvälityspalvelu ottaa ne käyttöön ja asiointipalvelu hankkii tunnistuspalvelun. Sen sijaan vanhoilla sopimusasiakkaila on jo tuotannossa tunnistuspalvelun käyttötapa, jonka ylläpitoon niiden on tehtävä muutoksia. Otaen huomioon sen, että tunnistusvälityspalvelun on ensin suunniteltava omat prosessinsa ja informoitava asiointipalveluita tulevasta muutoksesta, tähän on varattava pidempi siirtymäaika. ICT-hankkeet suunnitellaan ja hankitaan viraston käsityksen mukaan tyypillisesti sykleissä ja hankkeita yhdistellään.

Virasto arvioi, että koska kysymyksessä ei ole teknisesti vaativa asia, vaan kriittinen tekijä on viestintä ja tietoisuus muutoksista ja niiden sisällöstä, muutokset voidaan saattaa asiointipalveluissa suunnitteluun ja tuotantoon yhdessä vuodessa. Tämä edellyttää luonnollisesti sitä, että tunnistuspalvelut ja viranomaisen viestivät tulevista muutoksista ja niiden sisällöstä aktiivisesti.

4.24.3 Säännöksen 9 siirtymäajat

Säännöksen 9.1.1 a) alakohdan uutta menettelyä koskeva siirtymäsäännös tarkoittaa sitä, että sanomatason salaukselle vaihtoehtoisen menettelyn voi ottaa käyttöön vasta, kun siinä voidaan käyttää säännöksen 8.1 vaatimukset täyttävää varmennetta tai avainta.

Säännöksen siirtymäaika sanomien allekirjoittamiselle tarkoittaa sitä, että salaaminen ja allekirjoittaminen on tehtävä säännöksen 8 mukaisilla avaimilla viimeistään silloin, kun niiden on säännöksen 8 siirtymäaikaajan mukaan oltava käytössä. Siirtymäaikana voidaan sanomatason salauksessa edelleen käyttää niitä avaimia, jotka ovat olleet käytössä ennen määräyksen voimaan tuloa. Myös sanomien allekirjoitus voidaan tehdä näillä avaimilla, kunnes uudet avaimet on vaihdettu. Sanomien allekirjoitus ei kuitenkaan ole pakollista ennen kuin siirtymäaika on päättynyt.

5 Liitteet ja viitteet

5.1 Viiteluettelo

Määräykseen liittyvät säädökset löytyvät säädöstietokannoista Finlexistä tai EUR-Lexistä ja ne on merkitty luetteloon tähdellä*

Liikenne- ja viestintäviraston ohjeet ja suositukset löytyvät viraston verkkosivuilta ja ne on merkitty luetteloon kahdella tähdellä **. Sivuille on koottu myös säädösviitteet.

Yleiset linkit

[Sähköinen tunnistaminen | Kyberturvallisuuskeskus - https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoisen-tunnistaminen](https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoisen-tunnistaminen)

[Sähköinen allekirjoitus ja muut eIDAS-palvelut | Kyberturvallisuuskeskus - https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoisen-allekirjoitus-ja-muut-eidas-palvelut](https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoisen-allekirjoitus-ja-muut-eidas-palvelut)

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

- Yleinen linkki haulla Elecetronic Signatures: <https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx>

[1] * Laki vahvasta sähköisestä tunnistamisesta ja sähköistä luottamuspalveluista (617/2009 muutoksineen, **tunnistus- ja luottamuspalvelulaki**) [617/2009 - Säädosmuutosten hakemisto - FINLEX ® - https://www.finlex.fi/fi/laki/smur/2009/20090617](https://www.finlex.fi/fi/laki/smur/2009/20090617)

[2] * Valtioneuvoston asetus vahvan sähköisen tunnistuspalvelun tarjoajien luottamusverkostosta 169/2016, muutettu 1212/2018 (nk. **valtioneuvoston luottamusverkostoasetus**) [169/2016 - Säädosmuutosten hakemisto - FINLEX ® - https://www.finlex.fi/fi/laki/smur/2016/20160169](https://www.finlex.fi/fi/laki/smur/2016/20160169)

[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**) [EUR-Lex - 32014R0910 - FI - EUR-Lex \(europa.eu\) - https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv%3AOJ.L.2014.257.01.0073.01.ENG](https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv%3AOJ.L.2014.257.01.0073.01.ENG)

[4] * KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2015/1502 (nk. **varmuustasoasetus**) teknisten vähimmäiseritelmien ja -menettelyjen vahvistamisesta sähköisen tunnistamisen menetelmien varmuustasoa 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 [EUR-Lex - 32015R1502 - EN - EUR-Lex \(europa.eu\) - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL.2015.235.R.0002](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL.2015.235.R.0002)

[5] * 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 [EUR-Lex - 32015R1501 - FI - EUR-Lex \(europa.eu\) - https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=OJ%3AJOL_2015_235_R_0001](https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=OJ%3AJOL_2015_235_R_0001)

[6] KOMISSION TÄYTÄNTÖÖNPANOPÄÄTÖS (EU) 2015/1984 (nk. EU:n notifiointimenettelypäätös) olosuhteiden, muutoseikkojen 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

[7] * KOMISSION TÄYTÄNTÖÖNPANOPÄÄTÖS (EU) 2015/296 (nk. **EU:n yhteistyö-verkostopäätös**) 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

[8] * KOMISSION TÄYTÄNTÖÖNPANOPÄÄTÖS (EU) 2016/650, annettu 25 päivänä huhtikuuta 2016, hyväksytyjen allekirjoituksen ja leiman **luontivälineiden tietoturva-arviointia** 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 (huom. koskee nk. QSCD:n sertifiointia) [EUR-Lex - 32016D0650 - FI - EUR-Lex \(europa.eu\) - https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32016D0650](https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32016D0650)

[9] * 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 tietosuojalaki**)

[10] * Tietosuojalaki (1050/2018)

[11] ISO/IEC 27001 Information security management

[12] KATAKRI, Tietoturvallisuuden auditointityökalu viranomaisille, Traficom julkaisusarja 232/2020 <https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille> ja [Katakri 2020 \(um.fi\) - https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246](https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246)

[13] SFS-ISO 31000:2018 Riskien hallinta. Ohjeet. [ISO 31000 Riskienhallinta | SFS - https://sfs.fi/standardeista/tutustu-standardeihin/suosittu-standardit/iso-31000-riskienhallinta/](https://sfs.fi/standardeista/tutustu-standardeihin/suosittu-standardit/iso-31000-riskienhallinta/)

- Englanniksi [ISO 31000:2018\(en\), Risk management — Guidelines - https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en](https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en)

[14] ISO/TR 31004, Risk management – Guidance for the implementation of ISO 31000, and International Standard/ISO/TR 31004:fi [14]

- Englanniksi [ISO - ISO/TR 31004:2013 - Risk management — Guidance for the implementation of ISO 31000 - https://www.iso.org/standard/56610.html](https://www.iso.org/standard/56610.html)

[15] ISO/IEC 31010, Risk management – Risk assessment techniques [ISO - IEC 31010:2019 - Risk management — Risk assessment techniques - https://www.iso.org/standard/72140.html](https://www.iso.org/standard/72140.html)

- SFS-ISO/IEC 31010 [Tuote \(sfs.fi\) - https://sales.sfs.fi/fi/index/tuotteet/SFSsahko/CENELEC/ID2/3/805354.html.stx](https://sales.sfs.fi/fi/index/tuotteet/SFSsahko/CENELEC/ID2/3/805354.html.stx)

[16] SFS-ISO/IEC 27005:2018, Information technology — Security techniques — Information security risk management [Tuote \(sfs.fi\) - https://sales.sfs.fi/fi/index/tuotteet/SFS/ISO/ID2/2/731936.html.stx](https://sales.sfs.fi/fi/index/tuotteet/SFS/ISO/ID2/2/731936.html.stx)

- Englanniksi [ISO - ISO/IEC 27005:2018 - Information technology — Security techniques — Information security risk management - https://www.iso.org/standard/75281.html](https://www.iso.org/standard/75281.html)

[17] VAHTI Ohje riskienhallintaan, Valtiovarainministeriön julkaisuja 22/2017, https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/VM_22_2017.pdf?sequence=1&isAllowed=y

[18] NIST Risk Management Framework (RMF) <https://csrc.nist.gov/projects/risk-management/about-rmf>

- NIST, (National Institute of Standards and Technology) www.nist.gov

[19] FIPS 140-3 Security Requirements for Cryptographic Modules, <https://csrc.nist.gov/publications/detail/fips/140/3/final>

- FIPS, FIPS-standardit (Federal Information Processing Standards) www.nist.gov

[20] PCI Security Standards, ml. PA-DSS (Payment Application Data Security Standards) [Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards - https://www.pcisecuritystandards.org/pci_security/standards_overview](https://www.pcisecuritystandards.org/pci_security/standards_overview)

[21] ** Liikenne- ja viestintävirasto 211/2019 O Sähköisen tunnistuspalvelun arviointiohje https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/O211_S%C3%A4hk%C3%B6isen_tunnistuspalvelun_arviointiohje_211_2019_O.pdf

[22] EU:n varmuustasoasetuksen (EU) 2015/1502 soveltamisohje (LOA Guidance 2021) <https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LoA%20guidance%20%282021%29.pdf>

- Vuoden 2016 version käännös https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LOA_Guidance_Final_suomeksi.pdf [käännös 2021 lisätään, kun valmistuu]
- Englanniksi LOA Guidance 2021 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LOA_Guidance.pdf
- Yhteistyöverkosto (cooperation network) <https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Cooperation+Network+Resources>

[23] ISO/IEC 15408 Information technology – Security techniques – Evaluation criteria for IT security (nk. Common Criteria)

- www.commoncriteriaportal.org/cc CCPART1-3 vastaa standardia ISO/IEC 15408

[24] ISO/IEC 18045 Information technology – Security techniques – Methodology for IT security evaluation

- www.commoncriteriaportal.org/cc CEM vastaa standardia ISO/IEC 18045

[25] ISO/IEC 29115 Information technology — Security techniques — Entity authentication assurance framework [ISO - ISO/IEC 29115:2013 - Information technology — Security techniques — Entity authentication assurance framework - https://www.iso.org/standard/45138.html](https://www.iso.org/standard/45138.html)

[26] ** PiTuKri, Pilvipalveluiden turvallisuuden arviointikriteeristö, Traficom julkaisu 13/2020 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

[27] 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

[28] NIST 800-63B, Digital Identity Guidelines, Authentication and Lifecycle Management <https://pages.nist.gov/800-63-3/sp800-63b.html>

[29] NIST, Face Recognition Vendor Test (FRVT) <https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt21>

[30] * Laki digitaalisten palvelujen tarjoamisesta (306/2019) [306/2019 - Säädosmuutosten hakemisto - FINLEX® - https://www.finlex.fi/fi/laki/smur/2019/20190306](https://www.finlex.fi/fi/laki/smur/2019/20190306)

[31] ** Liikenne- ja viestintäviraston suositus 212/2021 S, Finnish Trust Network SAML 2.0 Protocol Profile, Dnro Traficom/6194/09.02.00/2020 7.7.2021 [Suositus 202/2021 S \(SAML\) https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Traficom_S212_2021_SAML_Profile_for_the_Finnish_Trust_Network_EN.pdf](https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Traficom_S212_2021_SAML_Profile_for_the_Finnish_Trust_Network_EN.pdf)

[32] ** Liikenne- ja viestintäviraston suositus 213/2021 S, OpenID Connect Protocol Profile for the Finnish Trust Network, Traficom/6194/09.02.00/2020, 7.7.2021 [Suositus 213/2021 S \(OIDC\) https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Traficom_S213_2021_OIDC_Profile_for_the_Finnish_Trust_Network_EN.pdf](https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Traficom_S213_2021_OIDC_Profile_for_the_Finnish_Trust_Network_EN.pdf)

[33] * EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI (EU) 2015/2366 maksupalveluista sisämarkkinoilla, direktiivien 2002/65/EY, 2009/1001/EY ja 2013/36/EU ja asetuksen (EU) N:o 1093/2010 muuttamisesta sekä direktiivin 2007/64/EY kumoamisesta (nk. **PSD2**, Toinen maksupalveludirektiivi – Payment Services Directive) [EUR-Lex - 32015L2366 - FI - EUR-Lex \(europa.eu\) - https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32015L2366](https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32015L2366)

[34] * KOMISSION DELEGOITU ASETUS (EU) 2018/389 Euroopan parlamentin ja neuvoston direktiivin (EU) 2015/2366 täydentämisestä asiakkaan vahvaa tunnistamista sekä yhteisiä ja turvallisia avoimia viestintästandardeja koskevilla teknisillä sääntelystandardeilla (nk. **RTS SCA & CSC**) [EUR-Lex - 32018R0389 - FI - EUR-Lex \(europa.eu\) - https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32018R0389](https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32018R0389)

[35] * Maksupalvelulaki 290/2010 [290/2010 - Säädosmuutosten hakemisto - FINLEX® - https://www.finlex.fi/fi/laki/smur/2010/20100290](https://www.finlex.fi/fi/laki/smur/2010/20100290)

[36] Arviomateriaali

- Kalvot 2018 eIDAS ja PSD2/RTS -tarkastelu <https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kalvot%2010102018%20PSD2-seurantarayhm%C3%A4%20eIDAS-%20ja%20PSD2-RTS-vaatimusten%20vertailu.pdf>
- Lausuntoversio 10102018 Vivin ja Fivan eIDAS-PSD2-RTS -vaatimusten vertailu (säännöseccel) <https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Lausuntoversio%2010102018%20Vivin%20ja%20Fivan%20eIDAS-PSD2-RTS-vertailu.XLSX>

[37] NCSA, Liikenne- ja viestintäviraston kansallinen tietoturvallisuusviranomainen (National Communications Security Authority, NCSA-FI)

- Yleistä NCSA-FI tietoa <https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/ncsa>

[38] SOGIS-MRA (Senior Officers Group for Information Systems, Mutual Recognition Agreement), <http://www.sogisportal.eu/>

- Yleistä SOGIS MRA tietoa https://www.sogis.eu/uk/supporting_doc_en.html#:~:text=The%20document%20%C2%AB%20SOG%2DIS%20Crypto,by%20all%20SOG%2DIS%20participants

[39] ** 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>

[40] IANAn (Internet Assigned Numbers Authority)

- IKEv2-määrittelyt <http://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml>
- ciphersuorit: <http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4>

[41] SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, (version 1.2 January 2020) <https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf>

[42] RFC 7905 ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS) <https://tools.ietf.org/html/rfc7905>

[43] RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3 <https://datatracker.ietf.org/doc/html/rfc8446>

[44] NCSA-FI -toiminnon hyväksymät salausratkaisut (1.7.2020 dnro 1240/651/2017) https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/NCSA_salausratkaisut.pdf

[45] eIDAS yhteistyöverkosto, Cooperation Network

- Yleistä eIDAS Cooperation Network -tietoa: [Cooperation Network Resources - eID User Community - CEF Digital \(europa.eu\)](https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Cooperation+Network+Resources) - <https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Cooperation+Network+Resources>

[46] 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>

[47] *** ETSI TS 119 312 V1.3.1 (2019-02) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites <https://ec.europa.eu/cefdigital/wiki/display/EIDTECHSUB/Security+Profile+v+1.3>

[48] 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>

[51] Financial-grade API (FAPI) WG [Financial-grade API \(FAPI\) WG | OpenID - https://openid.net/wg/fapi/](https://openid.net/wg/fapi/)

[52] ETSI MSS, ETSI TS 102 204 V1.1.4 (2003-08) Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface

[53] RFC 7519 JSON Web Token (JWT) <https://tools.ietf.org/html/rfc7519>

[54] Webtrust, CA/Browser Forum <https://cabforum.org/webtrust-for-cas/>

- Webtrust Trust Services Principles and Criteria for Certification Authorities ja Webtrust for Certification Authorities - SSL Baseline Requirements Audit Criteria

[55] Information Security Forum (ISF)

- Standard of Good Practice <https://www.securityforum.org/solutions-and-insights/standard-of-good-practice-for-information-security-2020/>
- INFORMATION RISK ASSESSMENT METHODOLOGY 2 (IRAM2) <https://www.securityforum.org/solutions-and-insights/information-risk-assessment-methodology-iram2/>

[56] ISRS 4400, International Standard on Related Services (ISRS) 4400 <https://www.iaasb.org/publications/isrs-4400-uudistettu-toimeksiannot-erikseen-sovittujen-toimenpiteiden-suorittamisesta>

[57] ISAE 3000, International Standard on Assurance Engagements (ISAE) 3000 Revised, Assurance Engagements Other than Audits or Reviews of Historical Financial Information <https://www.iaasb.org/publications/basis-conclusions-international-standard-assurance-engagements-isa-3000-revised-assurance>

[58] Vahti-ohjeet <https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet>

[59] Tiedonhallintalautakunnan suositukset <https://vm.fi/suosituksset>

[60] Finanssivalvonnan määräys- ja ohjekokoelma [Määräys- ja ohjekokoelma - Säätely - https://www.finanssivalvonta.fi/saantely/maarays-ja-ohjekokoelma/](https://www.finanssivalvonta.fi/saantely/maarays-ja-ohjekokoelma/)

[61] Finanssivalvonta, Standardi 2.4, Asiakkaan tunteminen – rahanpesun ja terrorismin rahoittamisen estäminen <https://www.finanssivalvonta.fi/saantely/maarays-ja-ohjekokoelma/valvottavan-toiminnan-jarjestaminen/2.4/>

[62] 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>

[63] BIS, Bank for International Settlements

- External audits of banks [External audits of banks \(bis.org\) - https://www.bis.org/publ/bcbs280.htm](https://www.bis.org/publ/bcbs280.htm)
- Supplemental note to External audits of banks - audit of expected credit loss [Supplemental note to External audits of banks - audit of expected credit loss \(bis.org\) - https://www.bis.org/bcbs/publ/d513.htm](https://www.bis.org/bcbs/publ/d513.htm)
- The internal audit function in banks <http://www.bis.org/publ/bcbs223.htm>

[64] IIA, The Institute of Internal Auditors www.theiia.fi

[65] ** [Liikenne- ja] Viestintäviraston ohje 214/2016 O tunnistus- ja luottamuspalveluiden ilmoituksista https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Ohje_214_2016_O_tunnistus_ja_luottamuspalveluiden_ilmoitukset_0.pdf

[66] ETSIn luottamuspalvelustandardit

- Ajantasaiset versiot ks. (haulla Digital Signatures ja/tai ESI - Electronic Signatures and Infrastructures) [Download ETSI ICT Standards for free - https://www.etsi.org/standards#page=1&search=&title=1&etsi-Number=1&content=0&version=1&onApproval=1&published=1&historical=1&startDate=1988-01-15&endDate=2021-07-14&harmonized=0&keyword=&TB=607&stdType=&frequency=&mandate=&collection=&sort=3](https://www.etsi.org/standards#page=1&search=&title=1&etsi-Number=1&content=0&version=1&onApproval=1&published=1&historical=1&startDate=1988-01-15&endDate=2021-07-14&harmonized=0&keyword=&TB=607&stdType=&frequency=&mandate=&collection=&sort=3)

*** Luottamuspalvelun tarjoaja

- ETSI EN 319 401 ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); **General Policy Requirements** for Trust Service Providers
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers **issuing certificates**; Part 1: General requirements
- ETSI EN 319 411-2 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**
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers **issuing Electronic Time-Stamps**
- ETSI EN 319 521 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for **Electronic Registered Delivery Service Providers**

*** Luottamuspalvelut

- EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: **Overview and common data structures**
- EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to **natural persons**
- EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to **legal persons**

- EN 319 412-4 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for **web site certificates**
- EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
- ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and **time-stamp token profiles**
- ETSI EN 319 102-1 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and **Validation**
- ETSI EN 319 522 Electronic Signatures and Infrastructures (ESI); **Electronic Registered Delivery Services**
 - o ETSI EN 319 522-1 Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 1: **Framework and architecture**
 - o ETSI EN 319 522-2 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: **Semantic contents**
 - o ETSI EN 319 522-3 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 3: **Formats**
 - o ETSI EN 319 522-4-1 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 1: **Message delivery bindings**
 - o ETSI EN 319 522-4-2 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 2: **Evidence and identification bindings**
 - o ETSI EN 319 522-4-3 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 3: **Capability/requirements bindings**

[67] Enisa Assessment of Standards related to eIDAS (December 14, 2018)

<https://www.enisa.europa.eu/publications/assessment-of-standards-related-to-ei-das>

- Yleistä ENISA, The European Union Agency for Network and Information Security, www.enisa.europa.eu

[68] *** ETSIn tekniset spesifikaatiot

- ETSI TS 119 441 Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing **signature validation** services
- ETSI TS 119 442 Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital **signature validation** services
- ETSI TS 119 102-1 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and **Validation**
- ETSI TS 119 102-2 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature **Validation Report**
- ETSI TS 119 172-4 Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals **using trusted lists**

- ETSI TS 119 511 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing **long-term preservation of digital signatures** or general data using digital signature techniques
- ETSI TS 119 512 Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing **long-term data preservation services**
- ETSI TS 119 524 Electronic Signatures and Infrastructures (ESI); Testing Conformance and **Interoperability of Electronic Registered Delivery Services**

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

[70] Auditing Framework for TSPs, Guidelines for Trust Service Providers, Versio 1.0 - December 2014 [Auditing Framework for TSPs — ENISA \(europa.eu\) - https://www.enisa.europa.eu/publications/tsp-auditing-framework](https://www.enisa.europa.eu/publications/tsp-auditing-framework)

[71] Eurooppalaisten akkreditointiorganisaatioiden yhteistyöelin EA (European Cooperation for Accreditation): EA Certification Committee Reference Paper; ETSI / EA Recommendations regarding; Preparation for Audit under EU Regulation (EU) No 910/2014 Article 20.1. (ei ole julkaistu verkossa)

- Yleistä: [European co-operation for Accreditation - European Accreditation \(european-accreditation.org\) - https://european-accreditation.org/](https://european-accreditation.org/)

[72] ***ETSI EN 319 403-1 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for **conformity assessment bodies** assessing Trust Service Providers

[73] ***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 https://www.etsi.org/deliver/etsi_ts/119400_119499/11940302/01.02.01_60/ts_11940302v010201p.pdf

[74] ***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

[75] ** Liikenne- ja viestintäviraston ohje 215/2019 O eIDAS-luottamuspalvelun arviointikertomuksesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/O215_Hyv%C3%A4ksytyn_eIDAS-luottamuspalvelun_arviointikertomus_%289_10_2019%29.pdf