Liikenne- ja viestintäviraston kysely 4.8.2020 tunnistus- ja luottamuspalvelumääräyksen 72 ja muun teknisen ohjauksen muutostarpeista

Sisällys

1 Määräyksen päivittämisen syyt, organisointi ja aikataulu

Määräys on annettu vuonna 2016. Tekninen kehitys, ETSI:n standardoinnin edistyminen, markkinoiden kehitys, tunnistus- ja luottamuspalveluntarjoajien soveltamiskokemukset ja viraston kokemus valvonnasta edellyttävät vaatimusten ajantasaisuuden arviointia ja muutoksia tarvittaessa. Määräyksen päivittämisessä on huomioitava määräystoimivallan rajat ja yhteensopivuus EU-sääntelyn kanssa.

Määräyksen 2-5 luvut koskevat vahvan sähköisen tunnistuspalvelun tarjoajia, tunnistuspalvelun vaatimustenmukaisuuden arviointia ja arviointielimien pätevyyttä.

Määräyksen vaatimusten täyttäminen on edellytys vahvan sähköisen tunnistuspalvelun merkitsemiselle Liikenne- ja viestintäviraston rekisteriin, josta säädetään laissa vahvasta sähköisestä tunnistamisesta ja luottamuspalveluista (617/2009, tunnistus- ja luottamuspalvelulaki)

Määräyksen 6-8 luvut koskevat EU:n nk. eIDAS-asetuksen (EU) 910/2014 mukaisten hyväksyttyjen luottamuspalveluiden vaatimustenmukaisuuden arviointia ja hyväksytyn sähköisen allekirjoituksen tai leiman luontivälineen sertifiointilaitosta.

Määräys on annettu vuonna 2016 EU:n eIDAS-asetuksen voimaantulon yhteydessä. Tunnistuspalveluiden sääntelyn vaatimukset sovitettiin yhteen uuden EU-sääntelyn kanssa ja lisäksi määrättiin yhteentoimivuudesta kansallisesti säädetyssä luottamusverkostossa.

Muutettava määräys

Määräys sähköisistä tunnistus- ja luottamuspalveluista (Viestintävirasto 72A/2018 M)

Määräyksen siirtymäaikaa 25 §:ssä jatkettiin määräysmuutoksella 72A/2018 M. Muita vaatimuksia ei tuolloin muutettu, joten ne ovat samat kuin määräyksessä Viestintävirasto 72/2016 M

1.1 Määräystoimivalta

Liikenne- ja viestintäviraston toimivalta antaa määräyksiä säädetään tunnistus- ja luottamuspalvelulaissa. Määräystoimivalta rajoittuu siten lain 42 §:ssä säädettyihin asioihin.

Tunnistuspalveluiden vaatimuksissa virasto huomioi sen, että laissa on pyritty yhdenmukaistamaan vaatimukset EU:n eIDAS-sääntelyn kanssa eli erityisesti komission varmuustasoasetuksen (EU) 2015/1502 kanssa. Varmuustasoasetusta tulkitaan vertaisarvioinneissa, kun tunnistusjärjestelmiä notifioidaan Komissiolle. Virasto osallistuu arviointeihin ja huomioi yhteiset tulkinnat kansallisessa sääntelyssä.

Luottamuspalveluissa määräystoimivalta on kapea. Määräyksellä täydennetään vain välttämättömät asiat, jotta hyväksyttyjen luottamuspalveluiden arviointikehys olisi riittävän täsmällinen ja ennakoitava siltä osin, kun vaatimuksia ei ole tarkennettu EU-sääntelyssä. Määräyksellä tarkennetaan EU-sääntelyä ja tunnistus- ja luottamuspalvelulain sääntelyä siten, että on olemassa oikeudelliset edellytykset luottamuspalveluiden vaatimustenmukaisuuden arviointilaitoksen akkreditoinnille tai sähköisen allekirjoituksen tai leiman luontivälineen sertifiointilaitoksen nimeämiselle, jos tähän ilmenee kiinnostusta.

1.2 Aikataulu ja organisointi

Seuraava aikataulu on alustava ja sitä voidaan joutua muuttamaan, jos esimerkiksi lainsäädäntöympäristöön (eIDAS, tunnistus- ja luottamuspalvelulaki) tulee muutoksia. Määräyksen EU-notifioinnin aikataulu voi vaikuttaa viimeistelyvaiheen aikatauluun vuoden 2021 loppupuolella.

8-9/2020 Toimialakysely muutostarpeista ja vaikutuksista
9-11/2020 Virkavalmistelu (muutosluonnokset ja vaikutusarviot)
12/2020-6/2021 työryhmätyöskentely (virasto kutsuu aihekohtaisiin työpajoihin luottamusverkoston ja eIDAS teknisen työryhmän jäsenet, alustava arvio 5-8 työpajaa)
6-8/2021 Virkavalmistelu ja käännökset (ruotsi, englanti)
9/2021 lausuntokierros uudesta määräys- ja perustelumuistioehdotuksesta
10/2021- lausuntokooste, mahdolliset muutokset ja niiden käännökset, EU-notifiointi (3 kuukautta)
1-2/2022 uusi määräys voimaan

1.3 Vaihtoehtoiset sääntelytavat

1.3.1 Määräys, ohje vai suositus

Määräyksellä annettavat pakottavat säännökset ovat tarkoituksenmukainen sääntelytyökalu, kun halutaan varmistaa tietoturva, laatu tai yhteentoimivuus. Tasapuolisesti tarkennetut vaatimukset edistävät toimijoiden reilua kilpailua. Määräyksellä on tehokkuusetuja, koska ne kohdistuvat kaikkiin toimijoihin ja määrittelevät vaatimustason ennalta. Määräysten sisältö olisi johdettavissa valvonnassa tulkinnalla laista, mutta määräyksellä tehtävät tarkennukset tekevät sääntelystä ennakoitavampaa kuin tapauskohtaiset valvontapäätökset. Määräysten valmistelu yhdessä toimialan kanssa on välttämätöntä, jotta vaatimukset pystytään määrittelemään toteutuskelpoisiksi. Määräyksen antaminen edellyttää sitä, että määrättävät vaatimukset ovat teknisesti riittävän kypsiä pakottaviin säännöksiin.

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

Määräyksen perustelumuistiossa perustellaan annettu sääntely ja annetaan neuvontaa soveltamisesta ja hyvistä teknisistä käytännöistä erityisesti niissä asioissa, jotka määräysvalmistelun yhteydessä osoittautuvat toimijoille epäselviksi.

Jos asia ei sovellu edellä kuvattujen tavoitteiden valossa määrättäväksi tai määräyksen antaminen ei ole tarkoituksenmukaista, virasto voi antaa teknistä ohjausta ohjeilla tai suosituksilla, joiden tarkoitus on edistää palveluiden turvallisuutta ja yhteentoimivuutta sekä toimialan yhteistyötä ja viranomaisen tiedonsaantia.

Virasto on antanut useita ohjeita (O) ja suosituksia (S) tunnistus- ja luottamuspalveluista.

- 211/2019 O Sähköisen tunnistuspalvelun arviointiohje
- 212/2018 S Finnish Trust Network SAML 2.0 Protocol Profile (päivitys käynnissä 2020)
- 213/2018 S OpenID Connect Protocol Profile for the Finnish Trust Network (päivitys käynnissä 2020)
- 214/2016 O Sähköisten tunnistus- ja luottamuspalveluiden ilmoitukset
- 215/2019 O Hyväksytyn eIDAS-luottamuspalvelun arviointikertomus
- 216/2016 S Luottamusverkoston käytännesäännöt

1.3.2 Yhteissääntely ja itsesääntely

Määräysvalmistelussa arvioidaan myös, olisiko tavoitteet mahdollista saavuttaa toimialan yhteis- tai itsesääntelyllä. Tehokas yhteissääntely edellyttää toimialan valmiutta panostaa sen organisointiin ja ylläpitoon ja sitä voi hyödyntää vain asioissa, joissa ei aiheudu vaaraa kilpailusäännelyn vastaisesta toiminnasta.

Voimassaolevan määräyksen perustelumuistion vaikutusarvioinneissa on arvioitu yhteis- tai itsesääntelyn mahdollisuudet ja vastaava arviointi tehdään myös käynnistyvässä määräyksen päivittämisessä.

Virasto on hankkinut vuonna 2012 Asianajotoimisto Krogerukselta oikeudellisen selvityksen yhteissääntelyn kilpailuoikeudellisista edellytyksistä. Lisätietoja löytyy verkkosivulta otsikon *Yhteissääntelyn edellytykset* alta https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/saantelyn-toimintatavat

Selvityksen perusteella kilpailuoikeudellisesti keskeistä on, millaisia vaikutuksia sääntely-yhteistyöstä seuraisi. Yhteistyön potentiaalisia kilpailuoikeudellisia ongelmakohtia voisivat olla a) kilpailijayhteistyön kautta syntyvät koordinaatiovaikutukset sekä b) kilpailijayhteistyön, sääntelyyn osallistuvien yhteisen määräävän markkina-aseman tai sääntelyorgaanin määräävän markkina-aseman kautta syntyvät poissuljentavaikutukset.

1.4 Säädökset

Muutettava määräys

Määräys sähköisistä tunnistus- ja luottamuspalveluista (Viestintävirasto 72A/2018 M)

Tässä asiakirjassa viitatut säädökset

Laki vahvasta sähköisestä tunnistamisesta ja luottamuspalveluista (617/2009, nk. **tunnistuslaki tai tunnistus- ja luottamuspalvelulaki**)

Valtioneuvoston asetus vahvan sähköisen tunnistuspalveluntarjoajien luottamusverkostosta 169/2016

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**)

EU:n komission täytäntöönpanoasetus (EU) 2015/1502 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 (nk**. varmuustasoasetus**)

EU:n 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 (nk. **yhteentoimivuusasetus**)

EU:n komission täytäntöönpanopäätös (EU) 2015/296 menettelyä koskevien järjestelyjen vahvistamisesta sähköiseen tunnistamiseen liittyvää jäsenvaltioiden välistä yhteistyötä varten säh-

köisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 12 artiklan 7 kohdan mukaisesti (nk. **yhteistyöverkostopäätös**)

Tiedoksi komission eIDAS-kuulemiset:

EU:n komissiolla on käynnissä eIDAS-asetuksen arviointi. Komissio on käynnistänyt 24.7.2020 julkisen kuulemisen.

Linkki: Komission lausuntopyynnöt 24.7.2020 - 3.9.2020 Digitaalista identiteettiä koskeva EU:n järjestelmästä (EUid)

Linkki: Komission lausuntopyyntö 24.7.2020-2.10.2020 eIDAS-asetuksesta (kyselyssä on omat osiot eID:stä)

PSD2-vertailussa viitattu säädös

KOMISSION DELEGOITU ASETUS (EU) 2018/389, annettu 27 päivänä marraskuuta 2017, 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**)

2 Määräyksen rakenne ja muut yleiset kysymykset

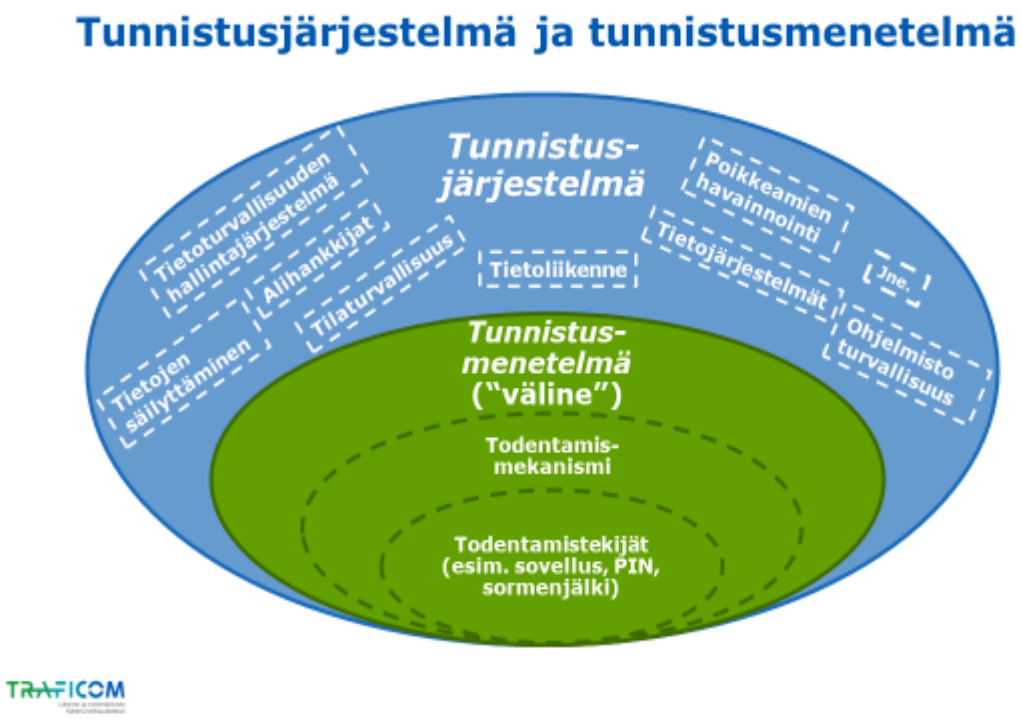
Määräykseen on yhdistetty vahvaa sähköistä tunnistamista ja eIDAS-asetuksen mukaisia hyväksyttyjä luottamuspalveluja koskevat arviointivaatimukset. Lisäksi määräys koskee eIDAS-asetuksen mukaisia hyväksytyn sähköisen allekirjoituksen tai leiman luontivälineen sertifiointilaitosta. Yhdistävä tekijä näille asioille on se, että niistä säädetään EU-tasolla ja Suomessa lain tasolla samassa säädöksessä.

2.1 Yleiset kysymykset

1) **Määräyksen asiakokonaisuus.** Onko tunnistuspalvelu- ja luottamuspalveluasioiden yhdistäminen samaan määräykseen mielestänne tarkoituksenmukaista?
2) **Lukujaottelu.** Onko määräyksen lukujaottelu riittävän selkeä ja toimiva?
3) **Muu tekninen ohjaus.** Puuttuuko tunnistus- ja luottamuspalveluista mielestänne viranomaisohjausta, joka edistäisi niiden tarjontaa tai hankintaa? Mistä tällaisesta asiasta kaipaisitte määrittelyä määräys-, ohje- tai suositustasolla?
4) **Yleistä.** Muita yleisiä kommentteja koko määräyksestä?

3 Vahvan sähköisen tunnistuspalvelun tietoturvavaatimukset

3.1 Mikä on tunnistusjärjestelmä ja tunnistusmenetelmä



Kuva: Termit tunnistusjärjestelmä ja tunnistusmenetelmä

Tunnistusjärjestelmä tarkoittaa järjestelmää, jonka puitteissa sähköisen tunnistamisen menetelmiä myönnetään ja tuotetaan käyttäjille. Tunnistusjärjestelmä kattaa tunnistuspalvelun tarjoajan tekniset järjestelmät, tietoturvallisuuden hallinnan ja muut säädetyt luotettavuusvaatimukset. Tunnistusjärjestelmä kattaa myös kaikki alihankitut osat ja toiminnot, jotka liittyvät tunnistuspalvelun tuottamiseen.

Tunnistusväline ja tunnistusmenetelmä tarkoittavat sääntelyssä samaa asiaa: aineellista ja/tai aineetonta kokonaisuutta, joka sisältää henkilön tunnistetietoja ja jota käytetään verkkopalveluun liittyvään todentamiseen. Tunnistusmenetelmä perustuu **todentamistekijöihin,** jotka liittyvät käyttäjän tietoon, ominaisuuteen tai hallussapitoon sekä **dynaamiseen todentamismekanismiin**, jolla taataan jokaisen tunnistustapahtuman ainutkertaisuus.

3.2 Tunnistusjärjestelmän ja tunnistusmenetelmän/tunnistusvälineen vaatimukset ja kysymykset

3.2.1 Tietoturvallisuuden hallinta (4 §)

Määräyksen 4 §:ssä määrätään yleisellä tasolla siitä, mitä tunnistusjärjestelmän tietoturvallisuuden hallinnassa täytyy ottaa huomioon. Tunnistuspalvelun tarjonnalla tarkoitetaan koko tunnistusjärjestelmää, joka kattaa koko tunnistuspalvelun kokonaisuuden.

EU:n varmuustasoasetuksen liitteen 1 kohdassa 2.4.3 edellytetään, että *tietoturvallisuuden hallintajärjestelmässä noudatetaan vakiintuneita standardeja tietoturvaan liittyviä riskien hallintaa*

ja valvontaa varten. Tunnistuslain 8.1 §:n 5 alakohdassa säädetään tietoturvallisuuden hallinnasta ja viitataan mm. varmuustasoasetuksen kohtaan 2.4.3.

Pykälän 1 momentissa tarkennetaan tunnistus- ja luottamuspalvelulain ja EU:n varmuustasoasetuksen vaatimusta. Ainakin ISO/IEC 27001 -standardi 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.

Pykälän 2 momentissa luetellaan toiminnan osa-alueet, jotka tietoturvallisuuden hallinnan täytyy kattaa. Vaatimuksissa on hyödynnetty standardin ISO/IEC 27001 ylätason ryhmittelyä.

Virasto on havainnut käytännön valvontatyössä, että tietoturvallisuuden hallinnan arvioinnin on varsinkin määräyksen soveltamisen alkuaikoina virheellisesti luultu riittävän vaatimustenmukaisuuden arviointiin. Näin ei ole, sillä tietoturvallisuuden hallinta on yksi arvioitava asia ja säännöksissä määriteltyjen teknisten vaatimusten täyttyminen on myös arvioitava. Tätä on selvennetty arviointiohjeessa 211/2019.

5) **Tietoturvallisuuden hallinta.** Virasto arvioi, että ainakin määräyksen perusteluja pitää täydentää ja selventää tietoturvallisuuden hallinnan suhde teknisiin vaatimuksiin. Oletteko samaa mieltä?
6) **Tietoturvallisuuden hallinta.** Olisiko tietoturvallisuuden hallinnan vaatimuksia mielestänne muutettava, lisättävä tai vähennettävä jollain tavalla ja millä perusteella?

3.2.2 Tunnistusjärjestelmän tekniset vaatimukset, varmuustasot ja häiriönhallinta (5 § - 11 §)

Tietojärjestelmä-, tietoliikenne- ja käyttöturvallisuus. Tunnistusjärjestelmän vaatimukset 5.1 §:ssä pohjautuvat tietojärjestelmien turvallisuuden yleisesti käytettyyn eri osa-alueiden jäsentelyyn tietojärjestelmä- tietoliikenne- ja käyttöturvallisuuteen. 5.2 §:ssä tarkennetaan etähallinnassa käytettävän päätelaitteen vaatimukset korotetulla ja korkealla varmuustasolla. Järjestelmän toteutus ja kontrollit täytyy suhteuttaa tavoitellun varmuustason mukaan joko kohtuullisen tai vakavan tason tietoturvauhkaan.

Varmuustasot. Korotetun ja korkean varmuustason vaatimuksia ei pääsääntöisesti ole määritelty määräyksessä erikseen. Järjestelmän toteutus ja kontrollit täytyy suhteuttaa tavoitellun varmuustason mukaan joko kohtuullisen tai vakavan tason tietoturvauhkaan.

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

Vaikutusarvioinnissa päädyttiin siihen, että jätettiin eriyttäminen yksityiskohdiltaan pääosin yleisen tietoturvallisuuden hallinnan, suunnittelun ja auditoinnin varaan. Hallintaverkossa ja toimistoverkossa käytettävien työasemien turvallisuusvaatimusten määrittely herätti valmistelussa niin paljon kysymyksiä, että vaatimukset selkeytettiin määräyksessä 5 §:n 2 momentilla ja perustelumuistion soveltamisohjeilla.

Määräyksen 5 §:n 2 momentissa tarkennetaan 1 momentin yleisiä vaatimuksia hallintayhteyksien ja myös niiden etäkäytön osalta. 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.

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 ennakoitavuutta tunnistuspalveluiden toiminnan helpottamiseksi. Selkeät vaatimukset luovat viraston arvion mukaan myös keskinäistä luottamusta luottamusverkoston nykyisten ja tulevien tunnistuspalveluiden tietoturvallisuuteen.

Alihankkijat. Määräyksessä ei käsitellä erikseen alihankkijoita. Tunnistuspalvelun tarjoaja vastaa tunnistuslain 13 §:n mukaan siitä, että sen alihankintana käyttämät palvelut täyttävät vaatimukset. Tunnistusjärjestelmän ja tunnistusmenetelmän toteuttamisessa käytetään tyypillisesti alihankintaa. Vaatimustenmukaisuuden arvioinnin kannalta alihankintaa käsitellään tunnistuspalvelun arviointiohjeessa 211/2019.

Tunnistusmenetelmän ominaispiirteet ja todentamistekijät. Tunnistusmenetelmällä tarkoitetaan käyttäjän tunnistusvälinettä todentamistekijöineen ja todentamismekanismia, jolla autentikointi tunnistustapahtumassa toteutetaan. Tunnistusmenetelmässä täytyy käyttää vähintään kahta todentamistekijää eri luokista (tieto, hallussapito, biometrinen ominaisuus). Todentamismekanismin täytyy olla dynaaminen eli jokaisen tunnistustapahtuman täytyy olla uniikki.

Useampi erityyppinen todentamistekijä turvaa sitä, että tunnistusväline on vain oikean haltijan käytettävissä. Dynaaminen todentamismekanismi turvaa sitä, että tunnistus perustuu oikeisiin todentamistekijöihin ja sitä, että tapahtumia ei voi kopioida tai väärentää. Tunnistusmenetelmän ja todentamismekanismin toteutuksen täytyy pystyä suojautumaan tietoturvauhkilta ja varmuustason mukaan kohtuullisen tai korkean kyvykkyystason hyökkäyksiltä.

Todentamistekijöitä ja todentamismekanismia käsitellään tarkemmin kohdan 3.4. vertailussa PSD2-sääntelyyn.

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

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

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

Rajapintaturvallisuus. Tietoliikennerajapintojen turvallisuusvaatimukset koostuvat lähinnä 7 §:n salausvaatimuksista.

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

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

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

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

Poikkeamat ja häiriöilmoitukset. Poikkeamien havainnointikyvystä ja hallinnasta ei ole 5 §:n lisäksi tarkennettuja vaatimuksia. Määräyksen 11 §:ssä määrätään häiriöilmoituksista Liikenne- ja viestintävirastolle. Ilmoituskynnystä ei ole tarkennettu määräyksen, mutta määräyksen perusteluissa on soveltamisohjeita eri häiriötilanteista.

Häiriöilmoitusten toimittaminen virastolle on lisääntynyt kiitettävästi vuonna 2019 ja 2020, kun aikaisemmin ilmoituksia ei käytännössä tehty. Määräyksen kannalta viraston arvio on edelleen, että dataa häiriöistä ei ole niin paljon, että sen perusteella voisi määritellä määräystasolla yksiselitteisiä kynnyksiä. Säädettävien kynnysten edellytys olisi myös, että ne olisivat konfiguroitavissa tunnistuspalveluiden teknisiin järjestelmiin ja niiden tulisi olla kohtuullisen pysyviä, jotta tunnistuspalveluille ei aiheudu sääntelyn muutoksista tarpeettomia järjestelmäkustannuksia. Tällaiset määrittelyt tietoturvallisuusuhkissa ja -loukkauksissa ovat viraston valvontakokemuksen perusteella ylipäätään hankalia ja myös muilla valvontasektoreilla (teletoiminta, verkkotunnusvälitys, NIS-direktiivin mukaiset pilvipalvelut) kynnykset ovat laadullisia ja perustuvat soveltamisohjeisiin.

3.2.3 Yleiset kysymykset teknisten vaatimusten kattavuudesta

7) **Kattavuus.** Kattaako teknisten vaatimusten sääntely mielestänne oikeat asiat? Ovatko 5 §:n luettelon asiat relevantteja?
8) **Tarpeettomat vaatimukset.** Onko määräyksessä teknisiä vaatimuksia, jotka ovat tarpeettomia? Miksi? Miten näette mahdollisesti tarpeettomina pitämänne vaatimukset suhteessa Suomen markkinoille tuleviin kokonaan uusiin tunnistuspalvelun tarjoajiin?
9) **Puuttuvat vaatimukset.** Onko tunnistusjärjestelmän tai tunnistusmenetelmän toteutuksessa osa-alueita, jotka puuttuvat kokonaan määräyksestä ja joista olisi tarpeellista määrätä? Voisiko mahdollisesti puuttuvia asioita edistää ohjeella tai suosituksella?

3.2.4 Kysymykset varmuustasoista ja eriyttämisestä

10) **Varmuustasot.** Pitäisikö määräyksessä määritellä erikseen korkean varmuustason teknisiä vaatimuksia? Miltä osin ja miten?
11) **Varmuustasot.** Voiko eri varmuustasojen vaatimusten soveltamista ennakoida määräyksen sijaan kehittämällä neuvontaa ja tulkintaohjeita tunnistuspalvelun arviointiohjeessa 211/2019 O?
12) **Eriyttäminen.** Onko mielestänne tarpeen tarkentaa järjestelmien tai työtehtävien eriyttämistä joltain osin määräyksellä tai ohjeella?

3.2.5 Kysymykset todentamistekijöistä

13) **Todentamistekijät.** Onko tunnistusmenetelmän ominaispiirteiden suunnittelussa ja todentamistekijöiden turvallisuudessa osa-alueita, joita olisi arvioitava määräysvalmistelussa? Ks. myös kohdan 3.3 kysymykset PSD2-vertailun yhteydessä.

3.2.6 Kysymykset salauksesta

14) **Salaus.** Onko 5 §:n määrittely salausvaatimuksista ja määräyksen perusteluissa olevat referenssit (ENISA, NIST, NCSA-FI, SANS) riittäviä? Olisiko määräystä tai perusteluja tarpeen muuttaa jotenkin? Mikä on mielestänne hyödyllisin referenssi suositelluista salausratkaisuista?
15) **Salaus.** Ovatko tietoliikenneyhteyden salausvaatimukset 7 §:ssä mielestänne ajan tasalla? Mitä muutoksia salausmenetelmiin, niiden parametreihin tai määräyksessä mainittuihin salausprotokolliin olisi tehtävä? Miten määräyksen perusteluissa olevia ciphersuiteja olisi mahdollisesti päivitettävä?
16) **Salaus.** Onko määräyksen perustelumuistiossa oleva suositus korkean varmuustason algoritmeista mielestänne ajan tasalla? Olisiko suositus muutettava velvoittavaksi ja siirrettävä se määräykseen? Miten tämä vaikuttaisi korkean varmuustason tunnistuksen käytettävyyteen, yhteentoimivuuteen ja asiointipalveluihin?
17) **Salaus.** Onko 7 §:n salausvaatimusten toteutettavuudessa teknisiä ongelmia tai ristiriitaisuuksia? Miten olette ratkaisseet ne ja miten määräystä tulisi mielestänne muuttaa?
18) **Salaus.** Olisiko salausvaatimusten sääntelylle mielestänne vaihtoehtoisia malleja sen sijaan, että vaatimukset määritellään nykyisellä tavalla pykälässä? Mitä yhdenmukaisesti mitattavissa ja määriteltävissä olevia (sääntelyn vaatimusten kannalta ennakoitavia) malleja ja referenssejä määräyksessä voisi mielestänne käyttää?
19) **Salaus.** Onko tietoliikenneyhteyksillä muita relevantteja yhteyskäytäntöjä kuin TLS? Pitäisikö ne huomioida sääntelyssä tai soveltamisohjeissa?

3.2.7 Kysymykset tietoliikenneyhteyksistä

20) **Tietoliikenteen osapuolten varmentaminen.** Ovatko luottamusverkoston sisäiset tietoliikenneyhteyksien varmentamisvaatimukset 8 §:ssä mielestänne selkeät?
21) **Asiointipalveluyhteydet.** Onko tietoliikenneyhteyden varmentaminen ja avaintenvaihtokäytännöt asiointipalveluiden kanssa saatu toteutettua? Miten? Tarvitaanko asiasta teknistä ohjausta suosituksella, ohjeella tai määräyksellä?
22) **Käyttäjärajapinnat.** Onko käyttäjärajapinnan vaatimuksia mielestänne tarpeen muuttaa jotenkin? Miten ja miksi?

3.2.8 Kysymykset uhkien ja häiriöiden hallinnasta

23) **Häiriöt.** Onko tietoturvauhkien, tietoturvaloukkausten ja häiriöiden havainnoinnissa, hallinnassa ja häiriöilmoituksissa asioita, joita olisi arvioitava määräysvalmistelussa?
24) **Uhkat, fraud.** Onko tunnistamisessa jotain käyttäjään tai asiointipalveluun liittyviä tietoturvauhkia tai fraud-ilmiöitä, joita määräysvalmistelun yhteydessä olisi hyvä käsitellä?

3.2.9 Kysymykset toteutettavuudesta ja vaikuttavuudesta

25) **Toteutettavuus.** Onko määräyksessä teknisiä vaatimuksia, jotka on vaikea toteuttaa teknisesti? Mitkä vaatimukset ja missä toteutustilanteissa? Miten asia pitäisi ratkaista, onko esimerkiksi kompensoivia kontrolleja?
26) **Toteutettavuus.** Onko määräyksessä teknisiä vaatimuksia, jotka ovat ristiriidassa keskenään tai joiden toteuttaminen on teknisesti mahdotonta tai vaikeaa jossain käyttötapauksissa? Miten ristiriidat tai toteutettavuusongelmat voisi mielestänne korjata?

27) **Soveltaminen.** Onko määräyksessä vaatimuksia, joiden tulkinta ja soveltaminen on epäselvää?
28) **Palvelut.** Onko määräyksessä vaatimuksia, joita on vaikea sovittaa yhteen käyttäjille tai asiointipalveluille tarjoamiinne tunnistuspalveluihin tai jotka hankaloittavat niiden kehittämistä?
29) **Vaikuttavuus.** Miten määräys on vaikuttanut omaan tunnistusjärjestelmänne ja tunnistusvälineenne ylläpitoon ja sen turvallisuuteen?
30) **Vaikuttavuus.** Mikä on käsityksenne määräyksen vaikutuksesta muiden luottamusverkostoon rekisteröityjen vahvojen tunnistuspalveluiden tekniseen turvallisuuteen? Luotatteko siihen, että muiden luottamusverkoston jäsenen tunnistusjärjestelmät ovat yhtä turvallisia kuin omanne?

3.3 PSD2:sta tai muusta lainsäädännöstä tulevat rinnakkaiset tekniset vaatimukset

3.3.1 Yleistä

Tähän kohtaan on koottu sähköisen tunnistamisen sääntelyn yksityiskohtia, joiden tarkastelu voi olla tarpeellista yleisen toimialariippumattoman tunnistamisen (eIDAS) ja maksupalvelualan (PSD2) sääntelyjen erojen tunnistamiseksi ja erojen vaikutusten arvioimiseksi. Kyselyn liitteenä on myös vuoden 2018 tarkastelu.

Monia tunnistuslain mukaan rekisteröityjä vahvoja sähköisiä tunnistusmenetelmiä käytetään Suomessa myös maksupalvelusääntelyn mukaisena vahvana tunnistamisena. eIDAS-asetuksen ja tunnistuslain sääntely on neutraalia sen suhteen, millä toimialalla ja missä palvelussa tunnistusta käytetään.

Traficom (tuolloin Viestintävirasto) ja Finanssivalvonta tarkastelivat 2018 sääntelyjen teknistä yhteensopivuutta ja pyysivät arviosta lausuntoja toimialalta (Fivan PSD2-yhteistyöryhmä ja Traficomin eIDAS-työryhmä. Arvion ja lausuntojen perusteella saman tunnistusmenetelmän käyttämiselle molempien sääntelyjen puitteissa ei havaittu esteitä. Sittemmin Fivan linjaus tunnuslukulistojen kelpaamattomuudesta ilman lisävahvistustekijää on hieman muuttanut tilannetta.

eIDAS-sääntelyn osalta tähän on koottu poimintoja komission varmuustasoasetuksesta (EU) 2015/1502 (eIDAS-varmuustasoasetus) ja siihen liittyvästä eIDAS Cooperation networkin laatimasta soveltamisohjeesta vuodelta 2016 (LOA Guidance 2016).

PSD2-sääntelyssä toimialakohtaiset vahvan tunnistamisen vaatimukset säädetään komission delegoidussa asetuksessa (EU) 2018/389 *Euroopan parlamentin ja neuvoston direktiivin (EU) 2015/2366 täydentämisestä asiakkaan vahvaa tunnistamista sekä yhteisiä ja turvallisia avoimia viestintästandardeja koskevilla teknisillä sääntelystandardeilla (RTS SCA & CSC).*

Kesäkuussa 2018 Euroopan pankkiviranomainen EBAn julkaisi kannanoton (EBA-Op-2018-04) Opinion RTS SCA & CSC:n tulkinnasta.

Kesäkuussa 2019 EBA julkaisi kannanoton (EBA-Op-2019-06) Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2

EBA on myös julkaissut PSD2 Q&A prosessin mukaisia vastauksia, jotka koskevat RTS SCA & CSC sääntelyä. Työkalussa oli 25.5.2020 nähtävissä 79 tulkintavastausta.

3.3.2 Hallussapitoon perustuvat todentamistekijät yleisesti

Ks. EBA-Op-2019-06

> *30. Table 2 summarises the views expressed above on what does or does not constitute a possession element under the RTS on SCA and CSC. The table is for illustrative purposes only and is not intended to be exhaustive; the possible elements included reflect current practices and developments in the market at the time of publication of the opinion.*
>
> *Possession of a device evidenced by an OTP generated by, or received on, a device (hardware or software token generator, SMS OTP) Yes**
> *Possession of a device evidenced by a signature generated by a device (hardware or software token) Yes**
> *Card or device evidenced through a QR code (or photo TAN) scanned from an external device Yes**
> *App or browser with possession evidenced by device binding — such as through a security chip embedded into a device or private key linking an app to a device, or the registration of the web browser linking a browser to a device Yes**
> *Card evidenced by a card reader Yes**
> *Card with possession evidenced by a dynamic card security code Yes**
>
> **Compliance with SCA requirements is dependent on the specific approaches used in the implementation of the elements.*

Ks. LOA Guidance 2016

> *The relevant security characteristic of a possession-based authentication factor (e.g. token) is the sole control of it by the owner. This implies that it is important that reproduction of it by a third party is so difficult and unlikely that the risk of this is negligible. The Level of Assurance depends on the level of resistance against reproduction. For example: asymmetric cryptographic (private) keys, the private keys may be stored on dedicated hardware devices (e.g. smartcards), or software token, uniquely identifiable token (e.g. the SIM card of a cell phone) or devices with one-time-passwords (e.g. "RSA-Token" or printed cards).*
>
> *Typical attacks on possession-based authentication factors are theft, duplication or tampering (manipulation), as well as attacks on the proof-of-possession during authentication.*

3.3.3 Tunnuslukulistat

Tunnuslukulista on hallussapitoon perustuva todentamistekijä, joka on erityisen altis mm. phishing-hyökkäyksille.

Finanssivalvonta on linjannut, ettei tunnuslukulista täytä hallussapitoon perustuvan todentamistekijän vaatimuksia ilman vahvistustekijää ja tunnistusvälineen tarjoajat ovat esim. lisänneet listan käyttöön maksupalvelutapahtumissa tekstiviestivahvistuksen.

Ks. myös EBA-Op-2019-06

> *28. Following the publication of the EBA Opinion on the implementation of the RTS, which stated that the card details and card security code that are printed on the card cannot constitute a knowledge element, a number of industry participants have queried if such details could constitute a possession element. The EBA is of the view that such details cannot do so for approaches currently observed in the market, in particular given the requirements under Article 7 of the RTS, and it advises CAs to closely monitor their application. That being said, dynamic card security codes7 (where the code is not printed on the card and changes regularly) may provide evidence of possession in line with Article 7 of the RTS.*

> *29. The EBA is also of the view that printed matrix cards or printed OTP lists that are designed to authenticate the PSU are not a compliant possession element for approaches currently observed in the market, for similar reasons to those mentioned for card details above, namely that they are unlikely to comply with the requirements under Article 7 of the RTS.*

Tunnistuslain nojalla paperisia tunnuslukulistoja ei *toistaiseksi* ole valvonnassa katsottu vaatimustenvastaiseksi *korotetulla* varmuustasolla, mutta eIDAS-sääntelyssä vertaisarvioinneissa tekijä on jo tullut esille Tanskan tunnistusjärjestelmän vertaisarvioinnissa, jonka yhteydessä Tanska on ilmoittanut luopuvansa tunnuslukulistoista. Ks. eIDAS Cooperation network Opinion 1/2020

31) **PSD2 ja eIDAS.** Onko tunnuslukulistojen tarkastelu määräysvalmistelun yhteydessä tarpeen? Onko niiden käyttöä tarkoitus jatkaa vielä?

3.3.4 SMS OTP

Tekstiviestillä lähetettävä kertakäyttösalasana on puhelimen hallussapitoon perustuva todentamistekijä, joka on altis mm. tekstiviestin lähettäjän väärennöksille ja vastaanoton kaappaamiselle.

EBA on ottanut kantaa tekstiviestillä toimitettavaan salasanaan kysymyksessä 2018_4039 Qualification of SMS OTP as an authentication factor https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4039

Ks. myös EBA-Op-2019-06

> *25. As stated in the EBA Opinion on the implementation of the RTS (paragraph 35), a device could be used as evidence of possession, provided that there is a 'reliable means to confirm possession through the generation or receipt of a dynamic validation element on the device'. Evidence could, in this context, be provided through the generation of a one-time password (OTP), whether generated by a piece of software or by hardware, such as a token, text message (SMS) or push notification. In the case of an SMS, and as highlighted in Q&A 4039, the possession element 'would not be the SMS itself, but rather, typically, the SIM-card associated with the respective mobile number'.*

eIDAS-sääntelyssä asiaan ei ole vakiintunutta kantaa, mutta eräiden vertaisarviointien yhteydessä on arvioitu, että SMS OTP ei täytä korkean varmuustason hyökkäyksensietovaatimuksia.

32) **PSD2 ja eIDAS.** Onko SMS OTP:n tarkastelu määräysvalmistelun yhteydessä tarpeen?

3.3.5 Mobiilisovellus

Mobiilisovellus on puhelimen hallussapitoon perustuva todentamistekijä, jonka turvallisuus riippuu siitä, mitä turvaominaisuuksia puhelimessa ja sen käyttöjärjestelmässä on tarjolla ja käytetäänkö niitä. Lisäksi turvallisuuteen vaikuttaa tietoliikenneyhteys taustajärjestelmään ja taustajärjestelmän turvallisuus.

EBA:n Q&A:ssa kysymys 2018-4047 liittyy asiaan ja siinä todetaan tarve arvioida sovellusturvallisuutta ja esim. käyttää SEE-elementtiä https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4047

Ks. myös EBA-Op-2019-06

> *24. Article 4(30) of PSD2 defines possession as 'something only the user possesses'. Possession does not solely refer to physical possession but may refer to something that is not physical (such as an app). Recital 6 of the RTS refers to the requirement to have adequate*

> *security features in place and provides examples of possession, 'such as algorithm specifications, key length and information entropy'. Article 7 of the RTS refers to the requirement for PSPs to have mitigation measures to prevent unauthorised use and to have measures designed to prevent the replication of the elements.*
>
> *26. The EBA is of the view that approaches relying on mobile apps, web browsers or the exchange of (public and private) keys may also be evidence of possession, provided that they include a devicebinding process that ensures a unique connection between the PSU's app, browser or key and the device. This may, for instance, be through hardware crypto-security, web-browser and mobile-device registration or keys stored in the secure element of a device. By contrast, an app or web browser that does not ensure a unique connection with a device would not be a compliant possession element.*

eIDAS-sääntelyn ja tunnistus- ja luottamuspalvelulain vaatimusten valvonnassa ja tulkinnassa merkitykselliset tekijät ilmenevät mobiilisovelluskriteeristöstä C ohjeessa 211/2019. Tarkastelutapa vastaa EU-vertaisarvioinneissa syntyneitä yhteistoimintaryhmän linjauksia sääntelyn turvallisuusvaatimuksista. Mobiilisovelluksen käyttö korkealla varmuustasolla edellyttäisi turvaelementtien sertifiointia.

33) **PSD2 ja eIDAS.** Onko PSD2-sääntelyn vaatimuksissa mobiilisovellusten turvallisuudelle nähdäksenne eroja suhteessa tunnistuslain ja eIDAS-asetuksen vaatimuksiin? Estävätkö mahdolliset erot saman sovelluksen käyttämisen maksupalveluissa ja yleisessä tunnistamisessa?

3.3.6 Tunnuslukulaitteet

Tunnuslukulaite on hallussapitoon perustuva todentamistekijä, jonka turvallisuuteen vaikuttavat laitteen ohjelmisto, käytetyt algoritmit ja fyysiset komponentit.

eIDAS-varmuustasoasetus

> *(EU) 2015/1502 johdantokappale (11) Kansainvälisiin standardeihin perustuva tietotekninen tietoturvasertifiointi on tärkeä väline tarkastettaessa, vastaavatko tuotteet turvallisuudeltaan tämän täytäntöönpanosäädöksen vaatimuksia*

Traficom on neuvontamuistiossaan 12/2018 edellyttänyt, että vuoden 2019 määräaikaisarviointien yhteydessä arvioidaan tunnuslukulaitteiden turvallisuus.

EBA-Op-2018-04

> *35 …For a device to be considered possession, there needs to be a reliable means to confirm possession through the generation or receipt of a dynamic validation element on the device.*

34) **PSD2 ja eIDAS.** Oletettavasti kansainväliset laitesertifioinnit eivät ole riippuvaisia siitä, minkä alan palvelussa niitä käytetään. Onko tunnuslukulaitteiden sääntelyssä eroja, joita olisi tarkasteltava määräysvalmistelun yhteydessä?

3.3.7 Tietoon perustuva todentamistekijä

EBA-Op-2019-06

> *31. Article 4(30) of PSD2 defines knowledge as 'something only the user knows'. Article 6 of the RTS refers to the requirement for PSPs to mitigate the risk that the element is 'uncovered by, or disclosed to, unauthorised parties' and to have mitigation measures in place 'in order to prevent their disclosure to unauthorised parties'.*

32. The EBA is of the view that the following elements could constitute a knowledge element: a password, a PIN, knowledge-based responses to challenges or questions, a passphrase and a memorised swiping path (as opposed to keystroke dynamics, namely the manner in which the PSU types or swipes, which may be considered an inherence element).

34. The same opinion also stated that a user ID (username) would not constitute a compliant knowledge element. Neither would an email address.

36. Table 3 summarises the views expressed above on what does or does not constitute a knowledge element under the RTS on SCA and CSC. The table is for illustrative purposes only and is not intended to be exhaustive; the possible elements included reflect current practices and developments in the market at the time of publication of the opinion.

*Password Yes**
PIN Yes
*Knowledge-based challenge questions Yes**
*Passphrase Yes**
*Memorised swiping path Yes**

Email address or user name No
Card details (printed on the card) No
OTP generated by, or received on, a device (hardware or software token generator, SMS OTP) No (for approaches currently observed in the market)
Printed matrix card or OTP list No

**Compliance with SCA requirements is dependent on the specific approach used in the implementation of the elements.*

LOA Guidance 2016

The knowledge-based factor likely to be known only by the owner of the factor and the verifying entity, *for example: PINs, passwords, memorable words or dates, pass phrases, pre-registered knowledge and other information likely to only be known by the subject.* In some cases even the verifying entity may not know the actual knowledge-based factor, but are able confirm that they and the applicant know the exact same information, *for example using the hash of a password*.

If knowledge is used as a factor it is necessary to mitigate against guessing (either random or brute force) of the knowledge by an adversary. *For example: where the knowledge is a password, good practice prescribes a suitable password policy (e.g. see safeguard S 2.11 "Provisions governing the use of passwords" of the BSI IT-Grundschutz catalogues, Single token authentication & Password entropy of NIST 800-63-2 Appendix A).*

Typical attacks on knowledge-based authentication factors are guessing, phishing eavesdropping or duplication. A characteristic of knowledge-based factors is that attacks are not necessarily noticed by the subject of the electronic identification means. *For example: brute force/dictionary attacks on a password with low entropy and without retry counter or a password that has been copied from a letter or email without knowledge of the owner or the verifier.*

3.3.8 Biometrinen todentamistekijä

Biometrisen todentamistekijän käyttö liittyy nykyisissä tunnistusmenetelmissä yleensä mobiililaitteen ominaisuuksilla toteutettuun sormenjäljen tai kasvotunnistuksen käyttöön mobiilisovelluksessa. Muita biometrisen tekijän lukulaitteita käyttäjille ei tällä hetkellä juurikaan ole tarjolla tai käytössä. Biometrisen todentamistekijän turvallisuus riippuu mm. sensoreiden tarkkuudesta ja biometristä tietoa käsittelevän ohjelmiston ja laitteiston toteutustavasta.

EBA-Op-2019-06

17. Article 4(30) of PSD2 defines inherence as 'something the user is'. Article 8 of the RTS on SCA and CSC refers to the 'authentication elements categorised as inherence and read by access devices and software' and recital 6 refers to the need to have 'adequate security features' in place that could, for example, be 'algorithm specifications, biometric sensor and template protection features'.

18. As stated in the Opinion on the implementation of the RTS, inherence may include behavioural biometrics identifying the specific authorised user. The EBA is of the view that inherence, which includes biological and behavioural biometrics, relates to physical properties of body parts, physiological characteristics and behavioural processes created by the body, and any combination of these. In addition, it is (the quality of) the implementation of any inherence-based approach that will determine whether or not it constitutes a compliant inherence element. Inherence is the category of elements that is the most innovative and fastest moving, with new approaches continuously entering the market.

20. The swiping path memorised by the PSU and performed on a device would not constitute an inherence element, but may rather constitute a knowledge element, something only the user knows.

22. Table 1 summarises the views expressed above on what does or does not constitute an inherence element under the RTS on SCA and CSC. The table is for illustrative purposes only and is not intended to be exhaustive; the possible elements included reflect current practices and developments in the market at the time of publication of the opinion.
Table 1 — Non-exhaustive list of possible inherence elements
Fingerprint scanning Yes
Voice recognition Yes V
ein recognition Yes
Hand and face geometry Yes
Retina and iris scanning Yes
Keystroke dynamics Yes
Heart rate or other body movement pattern identifying that the PSU is the PSU (e.g. for wearable devices) Yes
The angle at which the device is held Yes …
…
**Compliance with SCA requirements is dependent on the specific approach used in the implementation of the elements.*

eIDAS-sääntelyssä tai määräyksessä 72 ei ole eriteltyjä vaatimuksia biometriselle todentamistekijälle, vaan sen turvallisuuden ja luotettavuuden arviointi on osa tunnistusmenetelmän ja todentamismekanismin hyökkäyksenkeston kokonaisarviointia. Belgian mobiilisovelluksen perustuvan tunnistusmenetelmän vertaisarvioinneissa on 2019 linjattu, että biometrinen todentamistekijä ei ole riittävän luotettava *korkealla* varmuustasolla.
Ks. eIDAS Cooperation network Opinion 8/2019

35) **PSD2 ja eIDAS.** Onko biometrisen todentamistekijän sääntelyssä eroja, joita olisi tarkasteltava määräysvalmistelussa?

3.3.9 Todentamistekijöiden riippumattomuus

EBA-Op-2019-06

38. Another requirement under the RTS, in line with PSD2, is that the two elements used for SCA be independent. Independence under Article 9 of the RTS requires that the use of the elements 'is subject to measures which ensure that, in terms of technology, algorithms and parameters, the breach of one of the elements does not compromise the reliability of the other elements'.

eIDAS-sääntelyssä tai määräyksessä 72 ei ole eriteltyjä vaatimuksia todentamistekijöiden riippumattomuudesta, vaan se on osa tunnistusmenetelmän ominaispiirteiden ja todentamismekanismin hyökkäyksenkestävyyden kokonaisarviointia (varmuustasoasetus Liite 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu sekä 2.3.1 Todentamismekanismi)

LOA Guidance 2016

> *If multi-factor authentication is used[1], the different factors should be chosen in a way to counter different threats/attack vectors.*
> *Evaluating the strength of authentication needs to take into account not only the factor(s) itself, but also the mechanism to verify the factor(s).*
>
> *Using multiple authentication factors from different categories in a complementary manner can increase the overall security of the identification means. A common example is combining a possession-based token with a password or PIN to unlock the token. Even if the token is lost or stolen, it still cannot be used for authentication without the PIN.*
>
> *The authentication mechanisms used in the authentication phase cannot prevent all attacks completely, they can only offer resistance to attacks on a certain level of security/assurance. A standard way to quantify the resistance of different mechanisms is to rank them according their resistance against attacks with a certain attack potential (i.e. strength of an attacker). The Level of Assurance use the terms "enhanced-basic", "moderate" and "high" to denote the different attack potentials. This terminology is borrowed from ISO/IEC 15408 "Information technology – Security techniques – Evaluation criteria for IT security" and ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation". The text of the standards is also freely available at www.commoncriteriaportal.org/cc (CCPART1-3 being equivalent to ISO/IEC 15408 and CEM equivalent to ISO/IEC 18045). ISO/IEC 15408-1 defines "attack potential – measure of the effort to be expended in attacking a [mechanism], expressed in terms of an attacker's expertise, resources and motivation".*
>
> *Annex B.4 of ISO/IEC 18045 / CEM contains Guidance on how to calculate the attack potential necessary to exploit a given weakness of an authentication mechanism.*
> *In order to meet the requirements set out in the implementing act, some assessment of resistance against potential attacks should be carried out.*
>
> *The assessment should take relevant threats into accounts. For example, ISO 29115 mentions: online guessing, offline guessing, credential duplication, phishing, eavesdropping, replay attack, session hijacking, man-in-the-middle, credential theft, spoofing and masquerading.*
>
> *During assessing attack resistance, the whole authentication mechanism should be taken into account including the risks resulting from verification of the possession of the electronic identification means.*
>
> *For example*
> - *For LoA high, it is not sufficient that a smart card protects a cryptographic key against manipulation with high attack potential, also the cryptographic protocol should protect the verification of the possession of the key against manipulation/replay against high attack potential.*
> - *For a one-time-password token, where the generated one-time-password is transmitted via a secure channel (e.g. TLS), the strength of the possession-based-factor is limited not only by the strength of the token, but also by the strength of the secure channel.*
> - *The mechanism for proof-of-possession of a time-based one-time-password generator is the submission of a generated one-time-password to the verifier. The strength of this mechanism is limited, among others, by the length of the one-time-password, the time-window for validity of the password, and the confidentiality of the transmission.*

[1] Varmuustasoasetuksessa määritellään myös matalan varmuustason vaatimukset, joiden mukaan ei tarvita todentamistekijöitä eri luokista.

> *Reasonable assumptions on the level of security of components used by, but not part of, the authentication scheme (e.g. the environment of the user, browser, smart phone, etc.) should be taken into account during the risk assessment.*
> *Components can be operated in different configurations with different security settings. As an example, the assessment might assume that the user operates a personal firewall and virus protection on his/her computer.*
>
> *As a counterexample, currently it would not be reasonable to assume that the browser of the user is configured to use only secure cipher suites for Transport Layer Security (TLS); however this can be enforced by the service.*
>
> *The assessment might presume reasonable settings for the components not part of the authentication scheme.*

3.3.10 Dynaaminen linkitys

Sääntelyjen suhteessa kysymyksiä on liittynyt ainakin siihen, miten maksunvahvistuksen vaatimukset vaikuttavat mahdollisuuteen käyttää samaa tunnistusmenetelmää pohjana yleisessä tunnistamisessa ja maksupalveluissa. Maksun vahvistaminen edellyttää tunnistamista ja maksutietojen *dynaamista linkittämistä* tunnistustapahtumaan (*tunnistamiskoodiin*).

EBA-Op-2019-06

> *40. The EBA also notes (as published in Q&A 4141) that an element used for the purpose of SCA may be reused within the same session for the purpose of applying SCA at the time that a payment is initiated, provided that the other element required for SCA is carried out at the time of the payment initiation and that the dynamic linking element is present and linked to that latter element.*

EBA:n Q&A:ssa käsitellään mm. tätä tunnistamisen ja maksunvahvistuksen suhdetta ja kysymyksen 2018-4141 perusteella vaikuttaa siltä, että suhteessa yleiseen tunnistamiseen on mahdollista tehdä tunnistus samalla menetelmällä kuin missä tahansa palvelussa ja tunnistautuneena vahvistaa maksu RTS SCA & CSC:n edellyttämällä tavalla istunnon myöhemmässä vaiheessa.

https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4141

3.3.11 Istunnon tunniste, dynaaminen todentaminen/tunnistamiskoodi

Vaatimus liittyy siihen, että jokaisen tunnistusistunnon täytyy olla ainutkertainen, eikä se saa olla toistettavissa. Istunto/tunnistustapahtuma perustuu todentamistekijöiden käyttöön ja mm. salaukseen.

Tunnistuslain ja eIDAS-asetuksen vaatimukset sisältyvät yleiseen **dynaamisen todentamisen** vaatimukseen ja todentamismekanismin hyökkäyksensietoon:

eIDAS-varmuustasoasetus

> Liite kohta 1 Määritelmät
> *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;*
>
> Liite kohta 2.3.1 Todentamismekanismi
> *Korotettu varmuustaso*

1. Henkilön tunnistetietojen luovutusta edeltää sähköisen tunnistamisen menetelmän ja sen voimassaolon luotettava varmentaminen käyttämällä dynaamista todentamista.
2. 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"), voi heikentää todentamismekanismeja.

LOA Guidance 2016

The primary purpose of dynamic authentication is to mitigate against attacks such as 'man-in-the-middle' or misusing verification data from a previously recorded authentication replay to the verifier. This includes:

- *replay attacks, i.e. intercepting verification data and reusing them in a different authentication context*
- *certain types of session hijacking, e.g. exchanging (parts of) the authentication contexts of two or more simultaneously occurring authentications.*

It is important to understand that multi-factor and dynamic authentication are not the same; multi-factor authentication does not require that the authentication is dynamic (e.g. PIN and fingerprint) and can therefore be more exposed to replay attack than a dynamic authentication.

Dynamic authentication might be implemented by the authentication factor (e.g. a one time key from a device) or by the authentication mechanism (e.g. dynamic challenge in a challenge-response authentication).

Examples for dynamic authentications are:

- *possession of a private key stored on a smart card and verified using a challenge-response-protocol*
- *protocols based on an ephemeral Diffie-Hellman and providing authentication (e.g. PACE), cryptographic nonces, timestamps and/or non-repeating sequence numbers.*
- *protocols based on a static-ephemeral Diffie-Hellman, if the ephemeral key is provided by the relying party (e.g. EAC)*
- *dynamically generated one time access code (e.g OTP tokens) or challenge response protocols where the one time code has been previously generated and distributed out of band but selected dynamically during authentication (e.g. OTP cards)*

If the subject's private key is stored remotely (centrally stored, e.g. in an HSM operated by the identity provider), the authentication used to access the private key should also be dynamic.

PSD2-sääntelyssä RTS SCA & CSC -asetuksen 4 artikla

Johdantokappale 4) Dynaamisen yhdistämisen mahdollistaa tunnistamiskoodien tuottaminen, jonka on täytettävä tiukat turvallisuusvaatimukset. Teknologianeutraaliuden säilyttämiseksi ei saisi vaatia, että tunnistamiskoodit toteutetaan tietyllä teknologialla. Sen vuoksi tunnistamiskoodien olisi perustuttava sellaisiin ratkaisuihin kuin kertakäyttösalasanojen tai digitaalisten allekirjoitusten tuottaminen ja validointi tai muut salaukseen perustuvat validiuden vahvistamiset, joissa käytetään tunnistamisen tekijöihin tallennettuja avaimia tai salausteknistä aineistoa, edellyttäen, että turvallisuusvaatimukset täytetään.

4 artikla Tunnistamiskoodi
1. Jos maksupalveluntarjoajat soveltavat asiakkaan vahvaa tunnistamista direktiivin (EU) 2015/2366 97 artiklan 1 kohdan mukaisesti, tunnistamisen on perustuttava kahteen tai useampaan tekijään, jotka kuuluvat ryhmiin "tieto", "hallussapito" ja "erityinen ominaisuus", ja sen on johdettava tunnistamiskoodin tuottamiseen.

Maksupalveluntarjoajan on hyväksyttävä tunnistamiskoodi ainoastaan kerran, kun maksaja käyttää sitä päästäkseen maksutililleen verkon kautta, käynnistääkseen sähköisen maksutapahtuman tai toteuttaakseen etäkanavan kautta minkä tahansa toimen, joka voi aiheuttaa maksupetoksen tai muunlaisen väärinkäytöksen riskin.

2. Sovellettaessa 1 kohtaa maksupalveluntarjoajien on toteutettava turvatoimenpiteet, joilla varmistetaan kaikkien seuraavien vaatimusten täyttyminen:
a) tunnistamiskoodin ilmoittamisesta ei ole mahdollista johtaa mitään tietoja 1 kohdassa tarkoitetuista tekijöistä;
b) uutta tunnistamiskoodia ei ole mahdollista tuottaa mihinkään muuhun, aiemmin tuotettuun tunnistamiskoodiin liittyvien tietojen perusteella;
c) tunnistamiskoodin väärentäminen ei ole mahdollista.

3. Maksupalveluntarjoajien on varmistettava, että tunnistamiseen, joka perustuu tunnistamiskoodin tuottamiseen, kuuluvat kaikki seuraavat toimenpiteet:
a) jos tunnistamisessa, joka suoritetaan etäkäyttöä, sähköisiä etämaksuja ja muita toimia varten etäkanavan kautta, johon voi liittyä maksupetoksen tai muunlaisen väärinkäytöksen riski, ei ole kyetty tuottamaan tunnistamiskoodia 1 kohdan tarkoituksia varten, ei ole mahdollista määrittää, mikä mainitussa kohdassa tarkoitetuista tekijöistä on ollut virheellinen;
b) tunnistamisyrityksiä, jotka voidaan tehdä peräkkäin, minkä jälkeen direktiivin (EU) 2015/2366 97 artiklan 1 kohdassa tarkoitetut toimet estetään väliaikaisesti tai pysyvästi, saa olla enintään viisi tietyn ajanjakson aikana;
c) viestintäistunnot suojataan tunnistamisen aikana lähetettävien tunnistamistietojen sieppaamiselta ja oikeudettomien tahojen suorittamalta manipuloinnilta V luvun vaatimusten mukaisesti;
d) enimmäisaika, jonka maksaja voi olla passiivinen sen jälkeen, kun se on tunnistettu verkon kautta tapahtuvaa maksutilin käyttöä varten, on viisi minuuttia.
…

RTS SCS & CSC:n 4 artiklan tunnistuskoodin vaatimus koskee samoja asioita kuin eIDAS-sääntelyn dynaamisen todentamisen ja todentamismekanismin hyökkäyksenkestävyyden vaatimus. Tämä ilmenee seuraavassa EBA:n vastauksesta kysymykseen 2018-4053, jossa käsitellään tunnistuskoodin turvallisuutta. eIDAS-sääntelyn kannalta samaa asiaa suojataan mm. määräyksen 7 §:n salausvaatimuksilla.

https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4053

Article 4(2) of the Commission Delegated Regulation (EU) 2018/389 states that no information on any of the two elements necessary for strong customer authentication can be derived from the disclosure of the authentication code; that no new authentication code should be generated based on the knowledge of any other authentication code previously generated and that such code cannot be forged. Article 4(3) and 4(4) of the Delegated Regulation provides further requirements on authentication codes. Recital 4 of the Delegated Regulation states that "authentication codes should be based on solutions such as generating and validating one-time passwords, digital signatures or other cryptographically underpinned validity assertions using keys or cryptographic material stored in the authentication elements, as long as the security requirements are fulfilled". The Delegated Regulation does not specify the length for the authentication code. Accordingly, a three decimal-digit authentication code could be valid, providing that it complies with the requirements under the Delegated Regulation and in particular, that it is resistant against the risk of being forged in its entirety or by disclosure of any of the elements from which the code was generated.

Further, given that 'the authentication code shall be only accepted once' as stated in Article 4(1) phrase 2 of the Delegated Regulation meaning a 3-decimal digit authentication code would only give 1000 combinations, and since Article 4(3)(b) of the Delegated Regulation specifies the maximum of 5 failed authentication attempts, there is a higher probability of guessing the value of the authentication code.

3.3.12 Tietoliikenneturvallisuus tunnistuspalvelun yhteyksillä käyttäjään ja asiointipalveluun.

eIDAS-sääntelyssä ja määräyksessä 72 edellytetään tietoliikenneyhteyksien turvallisuutta (osapuolten välisiä rajapintoja käsitellään tarkemmin jäljempänä). Määräyksen 7 §:ssä määritellään

TLS:n vähimmäistaso, liikenteen salausvaatimus ja hyväksytyt salausalgoritmit. Salausta edellytetään luottamuksellisuuden turvaamiseksi myös sanomatasolla.

> *Varmuustasoasetus Liite*
> *2.3.1 Todentamismekanismi*
> *2. 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"), voi heikentää todentamismekanismeja.*
>
> *2.4.6 Tekniset tarkastukset*
> *2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät sähköisen viestinnän kanavat on suojattu salakuuntelulta, manipuloinnilta ja toistolta.*

LOA Guidance 2016

> *It has to be considered that communication channels may arise between different parties involved within an identification scheme, e.g. between the owner of the identification means and a service or between municipality and manufacturer.*
>
> *One possibility for technical controls for communication channels are technical guidelines issued by an authority that gives requirements on cryptography and security measures to be used. This will typically be achieved using cryptographic protocols with described verification steps.*
>
> *Requirements for communication channels between nodes of the eIDAS Interoperability Framework are given in the eIDAS Technical Specification for the framework.*
>
> *For an information security management system according to ISO/IEC 27001:2013, this requirement is covered as part of the controls A.10 'Cryptography', A.13 'Communications security' and A.18.1.5 'Regulation of cryptographic controls', which may also include references to technical guidelines as stated above.*

RTS SCA & CSC

> *35 artikla Viestintäistuntojen turvallisuus*
>
> *1. Tiliä ylläpitävien maksupalveluntarjoajien, korttipohjaisia maksuvälineitä liikkeeseen laskevien maksupalveluntarjoajien, tilitietopalvelun tarjoajien ja maksutoimeksiantopalvelun tarjoajien on varmistettava, että vaihdettaessa tietoja internetissä viestinnän osapuolten välillä sovelletaan turvallista salausta koko viestintäistunnon ajan käyttämällä vahvoja ja yleisesti tunnustettuja salaustekniikoita, jotta turvataan tietojen luottamuksellisuus ja eheys.*
>
> *2. Korttipohjaisia maksuvälineitä liikkeeseen laskevien maksupalveluntarjoajien, tilitietopalvelun tarjoajien ja maksutoimeksiantopalvelun tarjoajien on pidettävä tiliä ylläpitävien maksupalveluntarjoajien tarjoamat pääsyistunnot mahdollisimman lyhyinä, ja niiden on aktiivisesti lopetettava nämä istunnot heti, kun pyydetty toimi on saatu päätökseen.*
>
> *3. Ylläpitäessään rinnakkaisia verkkoistuntoja tiliä ylläpitävän maksupalveluntarjoajan kanssa tilitietopalvelun tarjoajien ja maksutoimeksiantopalvelun tarjoajien on varmistettava, että nämä istunnot liitetään turvallisesti maksupalvelunkäyttäjän (maksupalvelunkäyttäjien) kanssa käynnistettyihin istuntoihin, jotta estetään niiden välillä vaihdettujen viestien tai tietojen ohjaaminen väärille tahoille.*
>
> *4. Tilitietopalvelun tarjoajien, maksutoimeksiantopalvelun tarjoajien ja korttipohjaisia maksuvälineitä liikkeeseen laskevien tarjoajien on kommunikoidessaan tiliä ylläpitävän maksupalveluntarjoajan kanssa viitattava yksiselitteisesti kaikkiin seuraaviin seikkoihin:*

a)maksupalvelunkäyttäjä tai maksupalvelunkäyttäjät ja vastaava viestintäistunto, jotta samalta maksupalvelunkäyttäjältä tai samoilta maksupalvelunkäyttäjiltä tulevat pyynnöt voidaan erottaa toisistaan;
b)kun on kyse maksutoimeksiantopalveluista, käynnistetty maksutapahtuma, joka on varmennettu yksilöllisesti;
c)kun on kyse varojen saatavuuden vahvistamisesta, yksilöllisesti varmennettu pyyntö, joka koskee korttipohjaisen maksutapahtuman toteuttamiseen tarvittavaa määrää.
[...]

EBA:n lausunnossa EBA-Op-2018-04 on joitain viittauksia tietoliikenneturvallisuuteen. Ne voivat liittyä erityisesti maksutoimeksiantopalveluille tai tilitietopalveluille tarjottuun dedikoituun rajapintaan, joka voi kuitenkin olla eri rajapinta kuin yleisen tunnistamisen tai muille maksupalvelutoimijoille tarjottu rajapinta.

EBA-Op-2018-04

12
Table 1. Main requirements for dedicated interfaces and API initiatives

Enabling a secure data exchange between the ASPSP and the PISP, AISP and CBPII, mitigating the risk of any misdirection of communication to other parties
Articles 28 and 35 RTS

Ensuring security at transport and application levels Article 97(3) PSD2 Articles 30(2)(c) and 35 RTS

EBA:n vastaus kysymykseen 2018-4054 koskee tietoliikenteen salausta.

https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4054

Are EMV (Europay, MasterCard, Visa) transactions (for which the application cryptogram is not enciphered during its transmission) compliant with the RTS on strong customer authentication?

In accordance with Article 22(1) of the Commission Delegated Regulation (EU) 2018/389 payment service providers are required to "ensure the confidentiality and integrity of the personalised security credentials of the payment service user, including authentication codes, during all phases of the authentication".
In that regard, in the case where the issuer uses a cryptogram, which contains personalised security credentials, including authentication codes, the issuer would need to protect the confidentiality and integrity of the respective personalised security credentials in accordance with Article 22 of the Delegated Regulation, including during the transmission of the cryptogram. This also applies when the cryptogram is used as an authentication code.
The issuer is responsible for ensuring compliance with the requirements of Article 22 of the Delegated Regulation.

3.3.13 Tietoliikenteen osapuolten varmentaminen

PSD2-sääntelyssä tietyiltä tunnistusta hyödyntäviltä kolmansilta toimijoilta edellytetään eIDAS-asetuksen mukaisen qualified varmenteen käyttämistä (sähköisen leiman eli "järjestelmäallekirjoituksen" varmenteen tai verkkosivun todentamisen varmenteen).

eIDAS-sääntelyssä ei ole vastaavia täsmällisiä vaatimuksia. Määräyksen 72 8 §:ssä määrätään yleisellä tasolla osapuolten tunnistamisesta luottamusverkoston sisällä.

3.3.14 Muut PSD2-asiat

Ks. EBA-Op-2018-04, jossa huomioidaan, että tunnistuksen voi tuottaa myös muu kuin tilinpitäjäpankki.

EBA-Op-2018-04

> *Kohta 38. The articles mentioned above are to be read in conjunction with one another, which means that the PSP applying SCA is the PSP that issues the personalised security credentials. It is consequently also the same provider that decides whether or not to apply an exemption in the context of AIS and PIS. The ASPSP may, however, choose to contract with other providers such as wallet providers or PISPs and AISPs for them to conduct SCA on the ASPSP's behalf and determine the liability between them. The EBA also notes that a number of governmental (national) agreements on universal sets of personalised security credentials that can be used by PSUs with multiple PSPs already exist in some Member States.*

3.3.15 Kysymykset kohdista 3.3.9. - 3.3.14

36) **PSD2 ja eIDAS.** Onko PSD2-sääntelyssä tietoliikenteen salauksesta yleisiä vaatimuksia, joita ei ole teknisesti mahdollista toteuttaa, jos täyttää määräyksen 72 7 §:n vaatimukset TLS:stä (vähintään TLS 1.1) ja salausalgoritmeista?
37) **PSD2 ja eIDAS.** Onko tietoliikenteen osapuolten varmentamisessa (tunnistusvälineen tarjoaja, välityspalvelu, asiointipalvelu) ristiriitaisia vaatimuksia tai eroja, joita olisi tarkasteltava?
38) **PSD2 ja eIDAS.** Sääntelyjen yhteensopivuutta on selvitetty jo vuoden 2018 yhteensopivuustarkastelun yhteydessä. Onko sääntelyssä teknisiä tekniseen luotettavuuteen tai yhteentoimivuuteen liittyviä vaatimuksia tai eroja, joita olisi tarkasteltava mahdollisten yhteensopivuusongelmien takia uudestaan määräysvalmistelun yhteydessä?
39) **PSD2 ja eIDAS.** Estääkö jokin PSD2- ja eIDAS-sääntelyn liittyvä tekninen vaatimus saman tunnistusmenetelmän tarjonnan ja käytön yleisessä tunnistamisessa ja maksupalvelutunnistamisessa?

3.4 Blockchain ja self sovereign identity

3.4.1 Komission SSI eIDAS Legal Report

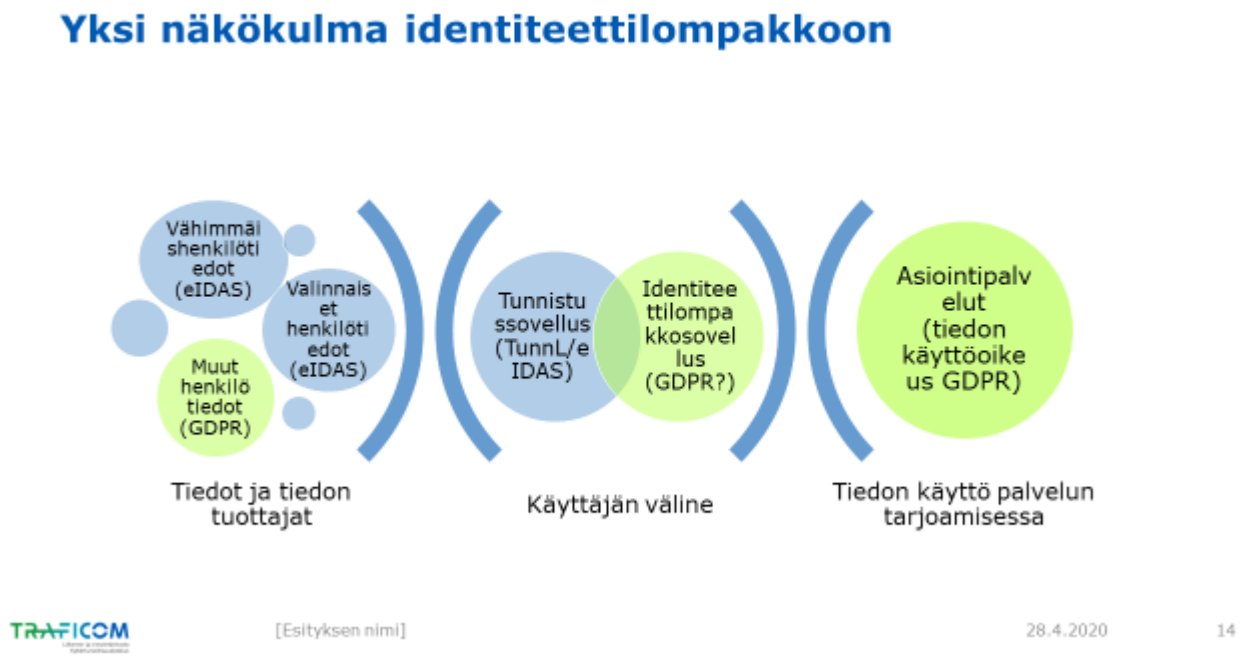
Sähköisen tunnistuspalvelun vallitsevaa perusmallia voi luonnehtia esimerkiksi seuraavasti: tunnistuspalveluntarjoaja kerää luotettavista lähteistä tunnistusvälineen hakijan henkilötiedot ja kytkee ne teknisesti tunnistusvälineen todentamistekijöihin. Asiointitapahtumassa henkilö autentikoidaan luottavalle osapuolelle todentamistekijöiden perusteella.

Blockchain voidaan nähdä teknisenä toteutustapana, jota tunnistuspalvelut voisivat käyttää tietojen käsittelyssä ja varmentamisessa. SSI puolestaan voitaisiin nähdä modernina tunnistusvälineenä, jolla käyttäjä pystyisi nykyisin tarjolla olevia menetelmiä paremmin itse hallinnoimaan henkilötietojensa (*attestation*) käytön luvitusta eri asiointitilanteissa ilman, että tunnistuspalvelun tarjoajan on tarpeen välittää tietoja osapuolten välillä. Merkittävästi pidemmälle menevässä kehityksessä lohkoketjuteknologian ja PKI-arkkitehtuurin perusluonteisen muutoksen voi ilmeisesti nähdä muuttavan tunnistuspalvelun roolin nykyisessä muodossaan tarpeettomaksi.

EU:n komissio on hiljan julkaissut selvityksen lohkoketjuteknologian ja itsehallittavan identiteetin suhteesta eIDAS-asetukseen: *SSI eIDAS Legal Report, How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market*
https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf

Selvityksessä kuvataan teknistä perustaa ja oikeudellista eIDAS-perustaa. Siinä arvioidaan erilaisia lyhyen ja pitkän tähtäimen kehitysvaihtoehtoja ja niiden suhdetta eIDAS-asetukseen. Raportin lähitulevaisuuden näkökulma on arvioida lohkoketjun ja SSI:n toteutuksia voimassa olevan eIDAS-sääntelyn valossa.

3.4.2 Kuva: identiteettilompakko ja henkilötiedot



3.4.3 Kysymykset blockhainista ja SSI:stä

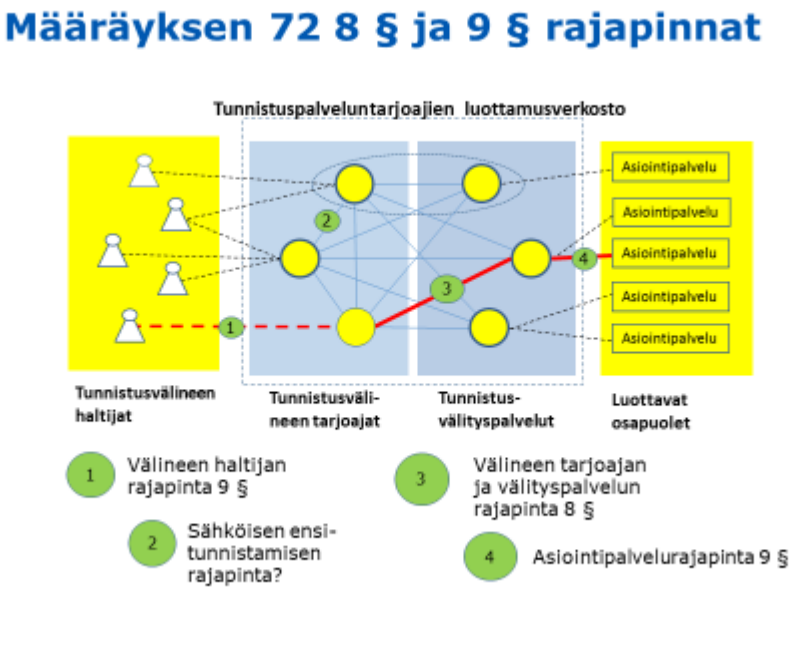
Seuraavilla kysymyksillä on tarkoitus selvittää kehityksen yleistä kypsyysastetta ja aloittaa valmistautuminen mahdollisiin muutoksiin. Viraston käsityksen mukaan kehitys ja eurooppalainen tulkinta ei ole niin kypsää, että kehitystä tai uusien tekniikoiden soveltamista voitaisiin edesauttaa määräyksellä. Pyrimme kartoittamaan, onko muu tekninen ohjaus, tiedonvaihto tai soveltamiskeskustelu ajankohtaista.

40) **Blockchain ja SSI.** Miten yleisesti ottaen näette lohkoketjuteknologian ja itse hallittavan identiteetin suhteen vahvan sähköisen tunnistuspalvelun tarjontaan?
41) **Blockchain.** Ovatko nykyiset tunnistussääntelyn tekniset vaatimukset ristiriidassa lohkoketjuteknologian hyödyntämisen kanssa? Estääkö mahdollinen ristiriita nähdäksenne teknologian käytön vai onko kysymys siitä, että soveltamiskäytäntö lohkoketjuteknologiaan on epäselvä?
42) **SSI.** Ovatko tunnistussääntelyn nykyiset tekniset vaatimukset ristiriidassa SSI-toteutusten kanssa? Estääkö mahdollinen ristiriita nähdäksenne SSI-toteutukset vai onko kysymys siitä, että soveltamiskäytäntö on epäselvä?
43) **Muut tekniset kehitysilmiöt.** Onko muita vastaavia kehityssuuntia, joita tunnistuspalvelujen teknisessä sääntelyssä olisi huomioitava?

4 Vahvan sähköisen tunnistamisen yhteentoimivuus (rajapinnat ja attribuutit)

4.1 Määräyksessä säännellyt luottamusverkoston rajapinnat

Kuva Luottamusverkoston rajapinnat



Määräyksen tarkennetut tietoturvallisuusvaatimukset koskevat seuraavia rajapintoja:

Kuvan rajapinta (3) tunnistusvälineen tarjoaja - tunnistusvälityspalvelun tarjoaja
Rajapintaa koskevat tietoturvallisuusvaatimukset ja protokollasuositus.

Kuvan rajapinta (4) tunnistusvälityspalvelun tarjoaja - asiointipalvelu
Rajapintaa koskevat tietoturvallisuusvaatimukset.

4.1.1 Tunnistusvälineen haltijan ja tunnistusvälineen tarjoajan välinen rajapinta

Kuvan rajapinta (1) Tunnistusvälityspalvelu - tunnistusvälineen haltija
Rajapintaa koskevat 9 §:n tietoturvaatimukset. Lisäksi tunnistusmenetelmän ja todentamismekanismin turvallisuuteen liittyvät vaatimukset vaikuttavat rajapinnan turvallisuusvaatimuksiin.

Vrt. vuoden 2016 määräysvalmistelun arvio:

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

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

4.2 Rajapinnat, joille ei ole määräyksessä teknisiä vaatimuksia

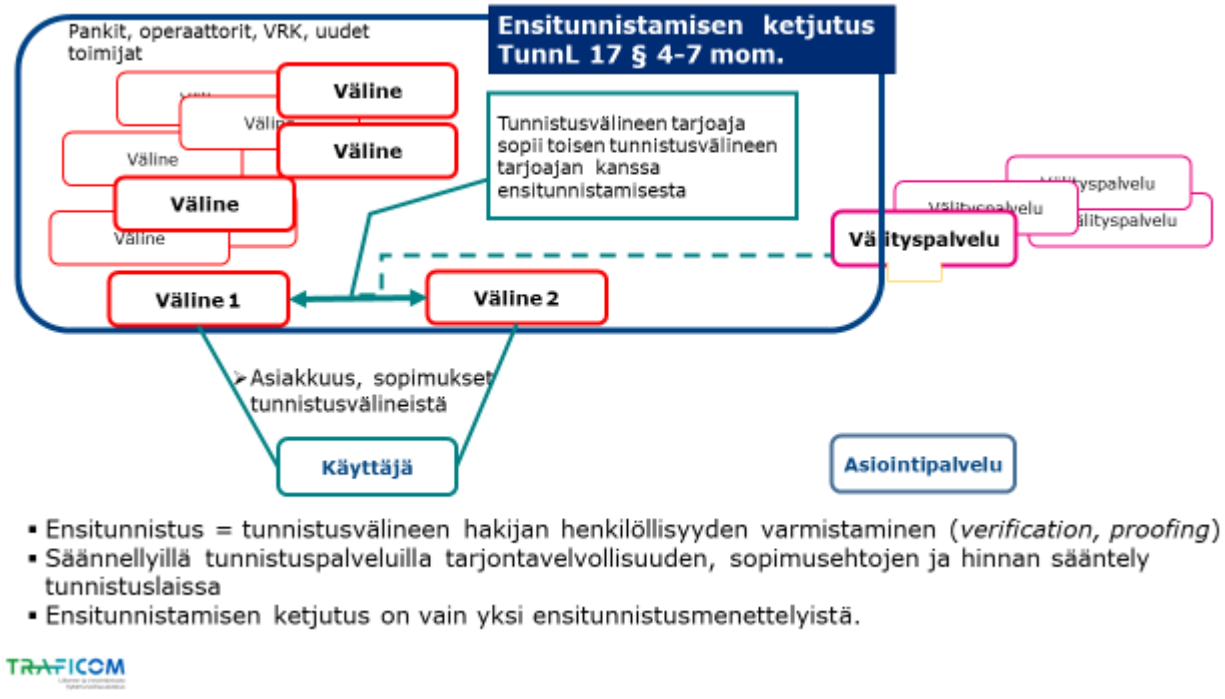
4.2.1 Sähköinen ensitunnistus

Kohdan 4.1 kuvan rajapinta (2) Tunnistusvälineiden tarjoajien välisellä rajapinnalla tarkoitetaan sähköisessä **ensitunnistamisessa käytettävää rajapintaa**. Muut tunnistusvälineiden tarjoajien väliset rajapinnat voidaan tulkita tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan väliseksi rajapinnaksi ja rajapintaa koskevat siten kyseisen rajapinnan vaatimukset.

Vrt. vuoden 2016 määräysvalmistelun arvio:

Sähköisen ensitunnistamisen rajapinta (SAML/TUPAS) on ollut käytössä jo useita vuosia, koska sähköinen ensitunnistaminen mahdollistettiin tunnistuslaissa (17 §) jo ennen luottamusverkostosääntelyn lisäämistä. Siksi ei nähty tarkoituksenmukaiseksi lisätä sähköisen ensitunnistamisen rajapintaa koskevia vaatimuksia määräykseen. Valmistelussa tuli kuitenkin esille pidemmän tähtäimen toivomuksia, että rajapinnan kautta voitaisiin välittää tietoa ensitunnistamisesta (esim. mihin henkilökohtainen ensitunnistaminen on perustunut: passi, henkilökortti, sähköinen tunniste).

Kuva Ensitunnistus vahvalla sähköisellä tunnistusvälineellä



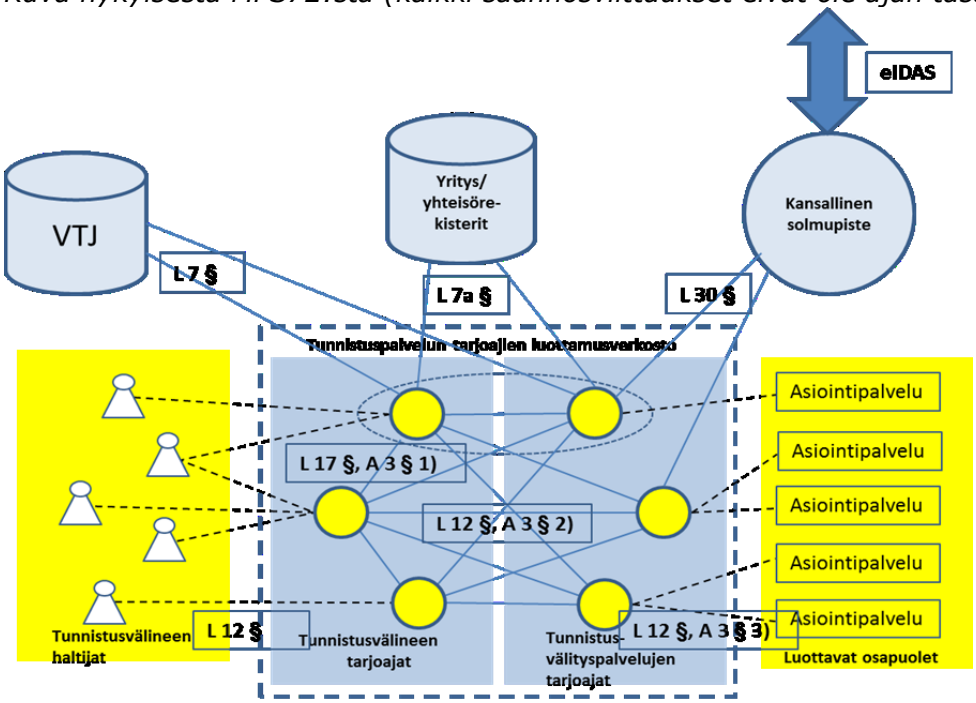
4.2.2 Väestötietojärjestelmän rajapinta ja Yritys- ja yhteisörekisterien rajapinta

Digi- ja väestötietoviraston ja patentti- ja rekisterihallitus määrittelevät omat rajapintansa asiakkailleen.

4.3 Kansallinen solmupiste ja suomi.fi

Lisäksi säädetään määräyksen 10 §:ssä tietoturvavaatimukset tunnistusvälityspalvelun ja kansallisen solmupisteen välillä. Digi- ja väestötietovirasto ylläpitää kansallista solmupistettä käytännössä suomi.fi -tunnistuksen yhteydessä tai rinnalla. Suomi.fi on kuvassa yksi asiointipalveluista. Seuraavassa kuvassa on kuvattu myös solmupiste, VTJ ja yritys- ja yhteisörekisterit.

Kuva nykyisestä MPS72:sta (kaikki säännösviittaukset eivät ole ajan tasalla)



4.4 Rajapintaprotokollat (OIDC ja SAML)

Määräyksessä ei määrätä, mitä protokollaa säännellyissä rajapinnoissa tulisi käyttää. Määräyksen 14 §:ssä on informatiivinen säännös, jonka mukaan tunnistuspalvelut sopivat protokollasta ja muista kuin määräyksen mukaisista ominaisuuksista keskenään.

Sopimusvapauteen vaikuttaa tunnistus- ja luottamuspalvelulain ja valtioneuvoston luottamusverkostoasetuksen sääntely (asetuksen säännösviittaukset ovat tunnistuslakiin ennen muutosta 412/2019, jolloin velvoitteet ovat siirtyneet eri kohtiin tunnistuslaissa).

> *Valtioneuvoston asetus vahvan sähköisen tunnistuspalvelun tarjoajien luottamusverkostosta 2016/169*
>
> *1 § Luottamusverkoston tekniset rajapinnat*
>
> *Vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain (617/2009), jäljempänä tunnistuslaki, 12 a §:n 2 momentissa 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.

Luottamusverkostoon kuuluvat tunnistuspalvelun tarjoajat voivat sopia tunnistuslain 12 a §:n 3 momentissa tarkoitetun tunnistetiedon veloituksen välittämiseen tarvittavasta tai muusta luottamusverkoston toiminnassa tarpeellisesta rajapinnasta.

Luottamusverkostoon kuuluvan tunnistuspalvelun tarjoajan on tarjottava 1 momentin 1 ja 2 kohdassa tarkoitetuissa rajapinnoissa kummassakin vähintään yhtä yleisesti käytetyn standardin mukaista teknistä rajapintaa.

Määräyksen perustelumuistiossa virasto suosittelee käyttämään SAML 2.0 - tai Open ID Connect -protokollaa ja näiden kansallisesti laadittuja profiileja, jotka virasto julkaisee erillisinä suosituksina (212/2018 S ja 213/2018 S).

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

Rajapintasuositusten 212 ja 213 päivittäminen on käynnissä ja mahdollisia muutostarpeita voidaan mahdollisesti ratkaista näillä suosituksilla.

4.5 Kysymykset rajapinnoista

44) **Määräysvaatimukset rajapinnoista.** Onko rajapintasuosituksissa asioita, joita tulisi mielestänne yhtenäistää tai tehostaa nostamalla ne määräykseen? Mitkä asiat ja miksi?
45) **Asiointipalvelurajapinta.** Olisiko asiointipalvelurajapinnasta tarpeen laatia teknistä ohjausta (suositus)?
46) **Käyttäjärajapinta.** Olisiko käyttäjärajapinnasta tarpeen laatia teknistä ohjausta (määräys, ohje, suositus)?
47) **Sopiminen protokollasta.** Onko määräyksen 14 § mielestänne tarpeellinen?
48) **Kansallisen solmupisteen rajapinta.** Solmupisteen rajapinnalla luottamusverkostoon voi olla merkitystä, jos jokin luottamusverkoston tunnistusväline notifioidaan komissiolle tai jos solmupisteen ja tunnistusvälityspalvelun kautta voisi välittää ulkomaisen tunnistusvälineen käyttäjän tunnistuksen suomalaiselle yksityiselle asiointipalvelulle. Onko luottamusverkoston ja kansallisen solmupisteen välisen rajapinnan tietoturvallisuudesta määrääminen (10 §) edelleen tarpeellista huomioiden se, että luottamusverkoston ja suomi.fi:n välinen rajapinta kuuluu 9 §:n vaatimusten piiriin?

4.6 Attribuutit, köyhdyttäminen ja rikastaminen

4.6.1 Tunnistamisessa välitettävät attribuutit (12 §)

Vähimmäistiedot, jotka vahvan tunnistuspalvelun täytyy määräyksen 12 §:n mukaisesti pystyä tuottamaan, ovat yksilöivä tunniste (hetu tai satu), nimi ja syntymäaika. Lisäksi on säädetty joukko valinnaisia tietoja, joita tunnistuspalvelu voi halutessaan tarjota.

Määräyksen vähimmäistiedot ja valinnaiset tiedot vastaavat rajat ylittävän tunnistamisen eIDAS-vaatimuksia. Tämän tietojoukon merkitys verrattuna kaikkiin muihin mahdollisiin henkilötietoihin on se, että ne on määritelty viraston suositusrajapinnoissa (suositukset 212 ja 213/2018) ja ne vastaavat eIDAS-sääntelyä, mikä edistää rajat ylittävä yhteentoimivuutta. Näiden säädettyjen tietojen tuottaminen tunnistuksessa sisältyy myös luottamusverkoston hintasääntelyyn tunnistuslain 12 c §:n mukaisesti.

Tavallisin vahvan tunnistuksen tarjontatapa on välittää ja vahvistaa luottavalle osapuolelle käyttäjästä tunnistustapahtumassa henkilötiedot, joiden perusteella henkilöllisyys voidaan yksilöidä. **Vahvan tunnistamisen sääntely on kuitenkin neutraalia siten, että tunnistamisessa voi myös köyhdyttää tietoja ja vaikkapa vahvistaa vain käyttäjän täysi-ikäisyyden.** Tällaiset vahvistukset ovat tunnistuspalvelun lakisääteisten lokitietojen perusteella yhdistettävissä henkilöön, joten vaikka ne ovat asiointipalvelulle anonyymejä, henkilötietojen sääntelyn kannalta ne ovat pseudonyymejä.

Säädettyjen tietojen lisäksi tunnistuspalvelu voi tarjota muita **rikastettuja tietoja** yleistä henkilötietojen suojan sääntelyä tai mahdollista toimialakohtaista sääntelyä noudattaen. Rikastamisen voisi tehdä tunnistusvälineen tarjoaja tai tunnistusvälityspalvelu.

Suomessa vahvassa tunnistamisessa on toistaiseksi nähtävissä vain perustyyppisen nimi ja henkilötunnus -yhdistelmän välittämistä. Traficom ei ole selvittänyt toimijoilta syytä tähän.

4.6.2 Valinnaiset attribuutit

Konkreettisia velvoitteita valinnaisten attribuuttien toteuttamiseen arvioitiin vuonna 2018 määräyksen osittaisuudistuksen yhteydessä (Tupas-siirtymäajan pidentäminen).

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

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

Vuonna 2018 arvioitiin, että ei ole tarvetta velvoittaa käsittelemään julkinen/yksityinen-attribuuttia kansallisessa tunnistamisessa eri tavalla kuin muita valinnaisia attribuutteja tai vaatia sitä toteutettavaksi nopeammassa aikataulussa.

4.6.3 Tunnistuspalvelun tarjoajien näkemyksiä 2018

Virasto selvitti määräysvalmistelun yhteydessä keväällä 2018 tunnistuspalvelun tarjoajien ja Digi- ja väestötietoviraston näkemyksiä tarpeesta valmistautua rajat ylittävään tunnistamiseen. Viraston määräyksessä asia liittyy pakollisten ja valinnaisten attribuuttien määrittelyyn luottamusverkoston rajapinnoissa.

Seuraavassa on ote viraston 3.5.2018 julkaisemasta lausuntoyhteenvedosta.

Valinnaisten attribuuttien määrittelyn tarpeellisuudesta yleisesti esitettiin vastakkaisia näkemyksiä. Varautuminen eIDAS-asetuksen mukaiseen toimintaan nähtiin perustelluksi ja tarkoituksenmukaiseksi (Väestörekisterikeskus) tai tarpeettomaksi ja kustannuksia aiheuttavaksi (OP Ryhmä). Vaatimukset nähtiin tarpeelliseksi säilyttää määräyksessä, jotta asiaa edistetään tehokkaasti (Kilpailu- ja kuluttajavirasto), kun taas yhdessä lausunnossa kannatettiin vaatimusten muuttamista suositukseksi (OP Ryhmä).

Useimmat asiaan kantaa ottaneet lausujat eivät pitäneet julkinen/yksityinen attribuuttia tarpeellisena kansallisesti tässä vaiheessa (Finanssiala, Danske, Nordea, OP Ryhmä). Kuitenkin yksi lausuja piti attribuuttia tarpeellisena (Ålandsbanken) ja yksi lausuja piti tarpeellisena suoraa kontaktia tunnistusvälineen tarjoajan ja suomi.fi:n välillä häiriöiden ja petosten selvittämisessä, mikä puhuisi erottamisen tarpeellisuuden puolesta (Nordea). Toisaalta kannatettiin valmistautumista rajat ylittävään tunnistamiseen tältäkin osin (Väestörekisterikeskus).

Vaikka valinnaisia attribuutteja ei pidetty tässä vaiheessa tarpeellisena, rajat ylittävän tunnistamisen tarpeita ja kysyntää sekä luonnollisten että oikeushenkilöiden tunnistamiselle pidettiin kuitenkin liiketoiminnassa olennaisina (Danske, Nordea, OP Ryhmä, Nets, Signom). Lausunnoissa tuotiin esille toiveita kansallisen solmupisteen palveluille yksityiselle sektorille (OP Ryhmä, Signom).

4.7 Kysymykset attribuuteista

49) **Suosituksen ja määräyksen suhde.** Attribuuttien määrittelystä SAML ja OpenIDConnect -rajapinnoissa on suositukset, joilla pyritään yhdenmukaistamaan vähimmäisattribuuttien ja valinnaisten attribuuttien käsittely. Onko määräyksen ja suosituksen suhteessa jotain asioita, joita olisi arvioitava määräysvalmistelussa?
50) **Vähimmäisattribuutit.** Onko EU-sääntelyn kanssa yhdenmukaisten attribuuttien lisäksi joitain muita tietoja, joita olisi arvioitava määräysvalmistelun yhteydessä?
51) **Valinnaiset attribuutit.** Onko EU-sääntelyn kanssa yhdenmukaisten attribuuttien lisäksi joitain muita tietoja, joita olisi arvioitava määräysvalmistelun yhteydessä?
52) **Julkinen/yksityinen luottava osapuoli**. Näettekö kansallisessa tunnistamisessa tarvetta tiedolle siitä, onko tunnistusta pyytänyt yksityinen vai julkinen asiointipalvelu - esimerkiksi häiriötiedon vaihdon, tietosuojan tai hinnoittelun takia?
53) **Oikeushenkilöt.** Onko oikeushenkilöiden vahvan tunnistuksen sääntelyssä asioista, joita olisi tarkasteltava määräysvalmistelussa?
54) **Ulkomaiset tunnistettavat.** Onko yksityisellä sektorilla tarvetta ulkomaisten luonnollisten ja oikeushenkilöiden vahvaan tunnistamiseen sähköisessä asioinnissa? Mitkä attribuutit tällöin olisivat hyödyllisiä?
55) **Yleistä attribuuteista.** Mitä muuta haluatte tuoda esille attribuuteista?

5 Rajat ylittävä tunnistaminen

5.1 eIDAS-sääntely ja kansallinen solmupiste

Rajat ylittävällä tunnistamisella tarkoitetaan sitä, että käyttäjä tunnistautuu yhdessä valtiossa myönnetyllä tunnistusvälineellä asiointipalveluun toisessa valtiossa. eIDAS-asetuksen notifiointisääntely velvoittaa vain julkisen sektorin asiointipalveluita, joten on erotettava rajat ylittävä tunnistautuminen julkisen ja yksityisen sektorin asiointipalveluihin.

Suomen notifioimia tunnistusvälineitä on mahdollista käyttää tulevaisuudessa ulkomaisiin julkisen hallinnon asiointipalveluihin tunnistautumisessa ja toisaalta ulkomaisilla notifioiduilla tunnistusvälineillä on notifiointien myötä mahdollista tunnistautua suomalaisiin julkisen hallinnon asiointipalveluihin. Suomesta ei ole vielä notifioitu tunnistusvälinettä.

Tunnistamistapahtumat Suomen ja muiden maiden välillä välitetään Digi- ja väestötietoviraston ylläpitämän kansallisen solmupisteen (PEPS, Pan European Proxy Server) kautta.

Ulkomaiseen julkisen sektorin asiointipalveluun tunnistaminen suomalaisella välineellä tapahtuu tunnistusvälineen tarjoajalta tunnistusvälityspalvelun ja kansallisen solmupisteen kautta. Ulkomaisella tunnistusvälineellä tunnistaminen *suomalaiseen julkisen sektorin palveluun* tapahtuu kansallisen solmupisteen ja suomi.fi -tunnistuksen kautta.

Rajapintojen tekninen yhteentoimivuus ja välitettävien tietojen yhdenmukainen määrittely rajapinnoissa ovat olennaisia, jotta tunnistus on käytännössä mahdollista. eIDAS-asetuksen rajat ylittävän tunnistamisen yhteentoimivuus- ja turvallisuusvaatimukset säädetään komission asetuksessa (EU) 2015/1501.

Viraston tunnistus- ja luottamuspalvelumääräyksessä huomioidaan 13 §:ssä rajat ylittävä tunnistaminen luottamusverkostosta kansallisen solmupisteen kautta. Solmupisteiden välinen rajapinta määritellään EU-yhteistyössä, mutta kansallisesti tunnistusvälityspalvelun tarjoajan (luottamusverkoston) ja solmupisteen välinen rajapinta on määriteltävä kansallisesti. Rajapintaa koskevat määräyksen mukaan samat yleiset vaatimukset kuin tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välistä rajapintaa. Muilta osin välityspalvelun tarjoaja ja solmupisteen toteuttaja sopivat rajapinnan ominaisuuksista keskenään. Tarkoituksenmukaista kuitenkin on, että protokollaksi valitaan jokin luottamusverkostossa käytössä oleva protokolla (OpenID Connect tai SAML).

Viraston tunnistus- ja luottamuspalvelumääräyksessä edistetään rajat ylittävää tunnistusta siten, että luottamusverkoston rajapinnoissa välitettävät pakolliset ja valinnaiset attribuutit on määritelty 12 §:ssä yhdenmukaisesti eIDAS-sääntelyn kanssa. Erityisesti valinnaiset attribuutit ovat olettavasti lisätietoina tarpeen rajat ylittävässä tunnistamisessa, kun suomalainen henkilötunnus ei välttämättä riitä yksilöimään henkilöä toisessa valtiossa.

Edellisten lisäksi määräyksen 17 §:ssä määritellään kansallisen solmupisteen tietoturvallisuuden arviointiperusteiksi ISO/IEC 27001 -standardi ja Euroopan komission täytäntöönpanoasetus (EU) 2015/1501.

56) **Rajat ylittävä tunnistus julkiselle sektorille.** Onko edellä esitetty vuoden 2016 ja 2018 määräysvalmisteluun perustuva arvio oikea?
57) **Rajat ylittävä tunnistus julkiselle sektorille.** Onko määräyksen 13 §:ssä muutostarpeita?
58) **Arviointiperusteet.** Onko solmupisteen tietoturvallisuuden arvioinnin perusteita arvioitava määräysvalmistelussa?

5.2 Rajat ylittävä tunnistusvälitys yksityisellä sektorilla (yksityiset tunnistusvälityspalvelut)

Kansallisen solmupisteen käyttämisestä tunnistautumisessa yksityisiin asiointipalveluihin ei vielä ole sääntelyä tai yhdenmukaisia määrittelyjä EU-tasolla eikä Suomessa.

Kansallisessa solmupisteessä keskitytään ensi vaiheessa tunnistamiseen julkishallinnon asiointipalveluihin ja vasta seuraavassa vaiheessa arvioidaan yksityiskohtaisemmin mahdollisuudet toteuttaa tunnistaminen yksityisiin asiointipalveluihin.

Koska kansallinen solmupiste ei ole toistaiseksi käytettävissä yksityisiin asiointipalveluihin tunnistamisessa, ulkomaisia tunnistusvälineitä käyttävien asiakkaiden tunnistaminen suomalaisiin asiointipalveluihin voi tapahtua sopimusperusteisesti, samoin kuin suomalaisella tunnistusvälineellä tunnistautuminen ulkomaisessa yksityisen sektorin palvelussa. Ulkomaisen tunnistuspalvelun luotettavuus voisi olla todettavissa notifioinnin perusteella, tunnistuspalvelun kotivaltion mahdollisen sääntelyn ja valvonnan perusteella tai sopimusperusteisesti.

Jos jokin luottamusverkostoon kuuluva tunnistuspalvelu haluaa ryhtyä välittämään vahvaa tunnistusta myös ulkomaille, tunnistusvälityspalvelun ja asiointipalvelun rajapintaa ja sopimussuhdetta koskevat samat vaatimukset kuin kotimaisille asiointipalveluille tarjottaessa. Sääntely ja Liikenne- ja viestintäviraston valvonta kattavat tällöin tunnistuslain ja viraston määräyksen vaatimukset tunnistusvälitykselle.

Viraston käsityksen mukaan luottamusverkoston tunnistusvälityspalvelut tarjoavat suomalaisten asiakkaiden tunnistusta myös muissa maissa, mutta virasto ei ole selvittänyt toiminnan laajuutta. Monet tunnistusvälityspalvelut ovat pohjoismaisia yrityksiä (esim. Nets, Signicat, Danske, Nordea, Telia), joten niillä on muutoinkin toimintaa useassa maassa.

59) **Rajat ylittävä yksityinen tunnistus.** Onko edellä esitetty arvio oikea?
60) **Rajat ylittävä yksityinen tunnistus.** Onko rajat ylittävässä tunnistusvälityksessä asioita, joita olisi tarkasteltava määräysvalmistelun yhteydessä?

6 Tunnistuspalveluiden vaatimustenmukaisuuden arviointi

6.1 Arviointielimet

Tunnistus- ja luottamuspalvelulain ja eIDAS-asetuksen mukaan tunnistuspalveluiden vaatimustenmukaisuuden arviointi on pakollista ja siitä täytyy toimittaa valvovalle viranomaiselle arviointi- tai tarkastuskertomus. Arvioija voi palvelusta riippuen olla FINASin akkreditoima vaatimustenmukaisuuden arviointilaitos, muu ulkoinen arviointilaitos tai sisäinen tarkastuslaitos.

Määräyksessä määritellään ne kriteerit, joiden perusteella vaatimustenmukaisuuden arvioijan riippumattomuus ja pätevyys arvioidaan objektiivisesti. Kriteerit perustuvat pääasiassa kansainvälisesti tai kansallisesti yleisesti käytettyihin standardeihin, säännöksiin tai ohjeisiin.

Määräyksen 18 §:ssä ja 19 §:ssä määritellään esimerkkejä sellaisista kansainvälisistä standardeista tai sääntely- tai itsesääntelykehyksistä, joihin arviointielimen riippumattomuus ja pätevyys voi perustua. Luettelot eivät ole tyhjentäviä, vaan jokin vastaava objektiivinen standardi tai säännöstö voi osoittaa pätevyyden.

6.1.1 Arviointielimen riippumattomuuden ja pätevyyden osoittamisen standardit

18 § Tunnistuspalvelun ulkoisen arviointielimen vaatimukset

Tunnistus- ja luottamuspalvelulain 33 §:ssä arviointielimelle säädettyjen riippumattomuus- ja pätevyysvaatimusten täyttymisen voi osoittaa
1) *ISO/IEC 27001 -standardiin perustuvalla akkreditoinnilla tai osoittamalla muutoin pätevyys standardin mukaiseen arviointiin;*
2) *Webtrust -säännöstöön perustuvalla kansainvälisesti tunnetun itsesääntelyjärjestelyn mukaisesti osoitetulla pätevyydellä;*
3) *PCI DSS - maksukorttistandardiin perustuvalla akkreditoinnilla tai osoittamalla muutoin pätevyys standardin mukaiseen arviointiin;*
4) *ISACA:n standardien ja tietojärjestelmien valvontakehikon mukaisesti osoitetulla pätevyydellä; tai*
5) *muiden edellisiin rinnastettavien yleiseen tietoturvallisuuden hallintaan taikka sektorikohtaiseen sääntelyyn tai standardointiin liittyvien säännösten, ohjeiden tai standardien edellyttämän pätevyyden osoittamisella tai noudattamisella.*

19 § Tunnistuspalvelun sisäisen tarkastuslaitoksen vaatimukset

Tunnistus- ja luottamuspalvelulain 33 §:ssä sisäiselle tarkastuslaitokselle säädettyjen riippumattomuusvaatimusten täyttymisen voi osoittaa:
1) *IIA:n ammattistandardien (sisäisen tarkastuksen riippumattomuus ja objektiivisuus, ml. organisatorinen riippumattomuus) noudattamisella;*
2) *ISACA:n standardien ja tietojärjestelmien valvonnan kehikoiden noudattamisella;*
3) *BIS:in (Bank for International Settlements) sisäistä tarkastusta koskevien ohjeiden noudattamisella;*
4) *Finanssivalvonnan määräys- ja ohjekokoelman sisäistä tarkastusta koskevien ohjeiden noudattamisella;*
5) *Finanssivalvonnan määräys- ja ohjekokoelman sisäistä tarkastusta koskevien määräysten ja ohjeiden noudattamisella;*
6) *muiden ETA-alueen jäsenvaltioiden vastaavien valvontaviranomaisten antamien ohjeiden tai määräysten noudattamisella; tai*
7) *muilla edellisiin rinnastettavilla viranomaissääntelyyn tai yleiseen riippumattoman sisäisen tarkastuksen hallintaan liittyvien standardien noudattamisella.*

61) **Arviointielinten vaatimukset.** Ovatko määräyksen 18 §:n ja 19 §:n standardi- ja määräysluettelot ajan tasalla? Ovatko listatut lähteet relevantteja? Puuttuuko jotain?
62) **Arviointielinten vaatimukset.** Mitä listatuista itse hyödynnätte/käyttämänne arviointielin hyödyntää?

6.1.2 Arviointistandardit

Määräyksen perustelumuistioon koottiin määräysvalmistelussa työryhmältä esimerkkejä standardeista tai muista lähteistä, joiden mukaisia arviointeja tunnistuspalvelurekisteriin merkityt toimijat kyselyn perusteella käyttävät ja jotka voivat soveltua myös tunnistusjärjestelmän arviointiin. Valmistelussa tai perustelumuistiossa ei ole eritelty riippumattomuuden ja pätevyyden perusteita tai arvioitu, miltä osin lähteet soveltuisivat tunnistusjärjestelmän vaatimusten arviointiin.

Esimerkkilista
- ISO 27001
- PCI DSS, PCI/QSA
- Webtrustin Trust Services Principles and Criteria for Certification Authorities ja Webtrust for Certification Authorities - SSL Baseline Requirements Audit Criteria
- Information Security Forumin (ISF) "Standard of Good Practice"
- ISF:n IRAM-kriteeristö (Information Risk Analysis Methodology)
- ETSI TS 101456 (CA policy)
- ISRS 4400 ja ISAE 3000
- Katakri
- Vahti
- Euroopan keskuspankin tai FIVA:n määräykset tai ohjeet
- FIVA:n määräys ja ohje 2.4 "Asiakkaan tunteminen - rahanpesun ja terrorismin rahoittamisen estäminen"
- Euroopan keskuspankin Cybersecurity questionnary 2015
- BISin (Bank for International Settlements) ohje External audits of banks

63) **Arvioinnin vaatimukset.** Ovatko määräyksen perustelumuistion lähteet relevantteja? Puuttuuko jotain?
64) **Arvioinnin vaatimukset.** Mitä listatuista itse hyödynnätte/käyttämänne arviointielin hyödyntää?
65) **Arviointiohje.** Olisiko arvioinnin esimerkkistandardit ja lähteet tarkoituksenmukaisempaa siirtää perustelumuistiosta arviointiohjeeseen 211/2019?

6.2 Arviointikriteerit

Vuonna 2016 arvioitiin määräysvalmistelussa seuraavia asioita: Millä tarkkuudella tunnistuspalvelun arviointivaatimukset eli auditointikriteeristö laaditaan määräykseen? Vaihtoehdot olivat yksityiskohtainen yhdenmukainen kriteeristö tai yleistason kriteeristö, jota täydennetään soveltamissuosituksella.

Määräyksen 15 §:ään otettiin vaikutusarvioinnin perusteella otsikkotason luettelo asioista, jotka arvioinnin täytyy kattaa. Luettelossa tukeudutaan EU:n varmuustasoasetuksen mukaiseen vaatimusten ryhmittelyyn.

15 § Arviointikriteerit

(1 mom.) Tunnistuspalvelun arvioinnin täytyy kattaa vaatimukset, jotka kohdistuvat
1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän)
a) tietoturvallisuuden hallintaan

b) tietojen säilyttämiseen
c) tiloihin ja henkilökuntaan
d) teknisiin toimenpiteisiin

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

(2 mom.) Edellä 1 momentissa mainittujen osa-alueiden arvioinnin on perustuttava tunnistus- ja luottamuspalvelulain ja tämän määräyksen vaatimuksiin, EU:n tai muun kansainvälisen toimielimen antamiin säännöksiin tai ohjeisiin, julkaistuihin ja yleisesti tai alueellisesti sovellettuihin tietoturvallisuutta koskeviin ohjeisiin tai yleisesti käytettyihin tietoturvallisuusstandardeihin tai menettelyihin.

Tarkoitus on, että toimijat voivat 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. Virasto joutuu myös tarkastuskertomuksia valvoessaan arvioimaan, että tämä toteutuu.

Virasto on laatinut yhteistyössä toimialan kanssa tunnistuspalveluiden arviointiohjeen 211/2019. Sillä päivitettiin aikaisempia ohjeita 211/2016 auditointikriteeristöstä ja 215/2016 sähköisten tunnistus- ja luottamuspalveluiden tarkastuskertomuksista.

Viraston käsitys on, että määräyksen 15 §:n ja päivitetty tunnistuspalvelun arviointiohje 211/2019 muodostavat nyt toimivan kokonaisuuden, jonka puitteissa on edelleen mahdollista hyödyntää muista syistä tehtyjä tietoturva-arviointeja. Virasto arvioi myös, että ei ole tarkoituksenmukaista muuttaa tätä yhdistelmää olennaisesti, jotta kahden vuoden välien tehtävässä arvioinnissa päästäisiin vakiinnuttamana käytäntöjä.

66) **Arviointikriteerit.** Onko määräyksen 15 §:n tarkkuustaso arvioitavista asioista mielestänne tarkoituksenmukainen?
67) **Arviointikriteerit.** Olisiko kriteereitä tai arviointiperusteita tarkasteltava määräysvalmistelussa? Olisiko niitä tarkennettava joltain osin?
68) **Tunnistusjärjestelmä ja alihankkijat.** Onko määräysvalmistelussa tarpeen tarkastella tunnistusjärjestelmän arkkitehtuuriin ja alihankintaan liittyviä kysymyksiä?
69) **Arviointiohje.** Onko arviointiohje toimiva vai olisiko siinä jotain korjaustarpeita?

6.3 Selvitys muiden vaatimusten täyttämisestä (16 §)

Määräyksen 16 §:ään on koottu tunnistuspalveluntarjoajan luotettavuutta koskevat osa-alueet, joiden täyttämisen voi osoittaa yrityksen omalla selvityksellä aloitus- tai muutosilmoituksen yhteydessä. Näistä vaatimuksista ei siis tarvita riippumattoman arviointielimen tekemään arviointia tai tarkastuskertomusta.

16 § Selvitys muiden vaatimusten täyttämisestä

Tunnistuspalveluntarjoajan on osoitettava omalla kirjallisella selvityksellään tai edellä 15 §:ssä tarkoitetulla arvioinnilla seuraavien tunnistuspalveluntarjoajan luotettavuuteen ja tunnistuspalvelusta annettaviin tietoihin liittyvät vaatimukset
1) julkaistut ilmoitukset ja käyttäjätiedot, kuten tunnistusperiaatteet, sopimusehdot ja hinnastot
2) vakiintunut organisaatio
3) valmius ottaa vahinkoriskejä

4) riittävät taloudelliset varat
5) vastuu alihankkijoista
6) suunnitelma toiminnan päättämisen varalta

Viraston ohjeessa 214/2016 O tunnistus- ja luottamuspalveluiden ilmoituksista käsitellään tietoja tai liitteitä, joita ilmoituksessa on toimitettava. Tiedoista ei kuitenkaan ole laadittu yksityiskohtaisia soveltamisohjeita.

70) **Tunnistuspalveluntarjoajan muut vaatimukset.** Onko määräyksessä tai ilmoitusohjeessa muutostarpeita, joita pitäisi tarkastella määräysvalmistelun yhteydessä?

7 eIDAS-asetuksen luottamuspalvelut ja niiden arviointi

Määräyksen 6-8 luvuissa määrätään eIDAS-asetuksen hyväksytyistä luottamuspalveluista, niiden vaatimustenmukaisuuden arviointilaitoksista sekä sähköisen allekirjoituksen tai leiman luontivälineen sertifioinnista.

Luku 6 Hyväksytyt luottamuspalvelut
20 § Hyväksytyn luottamuspalvelun tarjoajan arviointikriteerit
21 § Hyväksytyn luottamuspalvelun arviointikriteerit

Luku 7 Luottamuspalvelujen vaatimustenmukaisuuden arviointilaitokset
22 § Arviointilaitosten pätevyyden arviointi

Luku 8 Hyväksytyn sähköisen allekirjoituksen ja sähköisen leiman luontivälineen sertifiointi
23 § Sähköisen allekirjoituksen tai leiman luontivälineen vaatimukset
24 § Sertifiointilaitosta koskevat vaatimukset

Määräyksen tarkoitus on

- täydentää hyväksyttyjen sähköisten luottamuspalveluiden vaatimuksia ja niiden vaatimustenmukaisuuden arvioinnin riippumattomuus- ja pätevyyskriteereitä siltä osin, kun näistä ei ole säädetty Euroopan unionin lainsäädännössä, sekä
- täydentää sähköisen allekirjoituksen tai sähköisen leiman luontivälineen sertifioinnin kriteereitä siltä osin, kun näistä ei ole säädetty Euroopan unionin lainsäädännössä.

Määräysvaltuus on rajattu ja siinä on tarkoin huomioitava EU-sääntely ja kansainvälisen standardoinnin tilanne.

Viraston arvion mukaan määräysmuutoksessa on keskeisintä tarkastella ETSI:n standardoinnin edistymistä. Määräysvalmistelussa on myös seurattava käynnissä olevaa eIDAS-asetuksen uudelleenarviointia ja mahdollisia komission täytäntöönpanosäädöksiä luottamuspalveluista sekä arviointilaitoksista.

Seuraavassa on asiaan liittyviä lähteitä:

Linkki: ETSI Digital signature

Linkki: ETSI standards ja full list

Linkki: Komission eIDAS-observatory

Linkki: Komission eIDAS-sivut

Linkki: Komission sivut eIDAS-asetus ja täytäntöönpanosäädökset

Linkki: Komission lausuntopyyntö 24.7.2020-2.10.2020 (kyselyssä on oma osio luottamuspalveluista)

Virasto on pyytänyt erikseen lausuntoa luottamuspalveluihin ja arviointilaitoksiin liittyvistä asioista suhteessa eIDAS-asetukseen (dnro Traficom/9355/09.02.00/2020) ja siihen annetut vastaukset huomioidaan määräysmuutostarpeiden arvioinnissa.

71) **Hyväksytyt luottamuspalvelut.** Onko määräyksessä luottamuspalveluihin liittyviä muutostarpeita? Olisiko hyväksyttyjen luottamuspalveluiden vaatimustenmukaisuutta mielestänne arvioitava joidenkin muiden kuin ETSIn standardien perusteella? Minkä?
72) **Akkreditoidut arviointilaitokset.** Onko määräyksessä arviointilaitoksiin liittyviä muutostarpeita?
73) **Sertifiointilaitokset.** Onko määräyksessä sertifiointilaitoksiin liittyviä muutostarpeita?
74) **Vaikuttavuus.** Onko määräyksellä ollut vaikutusta hyväksyttyjen luottamuspalveluiden tarjontaan?

Aki Tauriainen
Johtaja

Anne Lohtander
Johtava asiantuntija

Tämä asiakirja on allekirjoittamisen sijasta varmennettu siten, että siitä näkyy asian esittelijän ja ratkaisijan nimi, ja asiakirja toimitetaan esittelijän tai ratkaisijan sähköpostiosoitteesta. Tämä poikkeuksellinen varmentamistapa on tilapäisesti käytössä koronaviruksen leviämisen rajoittamistoimien johdosta, joiden seurauksena asiaa käsittelevä virkamies tekee etätöitä eikä tavanomainen asiakirjan allekirjoittaminen ole mahdollista.