Liikenne- ja viestintäviraston tulkintamuistio vahvan ja rekisteröimättömän sähköisen tunnistuspalvelun eriyttämisestä

Sisällys

1 Tulkintamuistion tarkoitus ja sisältö

1.1 Tausta ja vuonna 2017 laaditun aiemman tulkintamuistion päivitys 2020-2021

Viestintävirasto julkaisi 3.10.2017 tulkintamuistion vahvan ja heikon tunnistuspalvelun tarjoamisesta (dnro 657/620/2017). Muistion tarkoitus oli antaa ennakoivaa neuvontaa vahvasta sähköisestä tunnistamisesta ja luottamuspalveluista annetun lain (617/2009, jäljempänä tunnistuslaki) tulkitsemisesta tilanteissa, joissa vahvan sähköisen tunnistuspalvelun tarjoaja tarjoaa myös heikkoa sähköistä tunnistusta.

Vuonna 2017 toimijoiden tulkintakysymykset liittyivät pääasiassa siihen, voiko pankkien tarjoamassa tunnistuksessa joissain tilanteissa jättää noudattamatta vahvan sähköisen tunnistuksen vaatimuksia asiointipalvelurajapinnassa.

Nyt vuonna 2020 Liikenne- ja viestintävirasto on laatinut asiasta tämän uuden tarkennetun tulkintamuistion. Sähköisten tunnistuspalveluiden kehityksen takia on syntynyt tarve tarkentaa tulkintaa siitä, millainen vahvan ja rekisteröimättömän sähköisen tunnistamisen eriyttäminen on tunnistuslain kannalta riittävää. Ajankohtaiset kysymykset liittyvät erityisesti mobiilisovelluksiin ja rekisteröimättömän tunnistusmenetelmän korottamiseen vahvaksi tunnistukseksi.

Aikaisempi termi heikko tunnistus on tässä korvattu paremmin asiantilaa kuvaavalla termillä *rekisteröimätön tunnistus*, koska kysymys on siitä, ettei menetelmää ole ilmoitettu tunnistuslain mukaiseen rekisteriin viranomaisvalvonnan piiriin.

Liikenne- ja viestintävirasto pyysi 27.3.2020 lausuntoja muistioluonnoksesta. Yhteenveto lausunnoista ja niiden perusteella tehdyistä muutoksista on muistion liitteenä.

1.2 Ennakoiva neuvonta säädetyistä vaatimuksista

Muistion oikeudellinen luonne on neuvonta. Tämä tarkoittaa sitä, että valvonnassa velvoitteet tulkitaan tapauskohtaisten tosiseikkojen ja lain ja määräyksen säännösten perusteella. Muistiossa ilmaistaan selkeästi, milloin kysymys on viraston näkemyksestä vaatimusten tulkinnassa ja milloin suosituksesta.

Vahvan sähköisen tunnistamisen sääntelyn vaatimukset koskevat kaikkia Liikenne- ja viestintävirastolle ilmoittautuneita tunnistuspalvelun tarjoajia ja niiden vahvoja tunnistuspalveluita. Lainsäädännön tulkinnan on sovelluttava yhtäläisesti kaikkiin nykyisiin ja myös tuleviin kotimaisiin tai ulkomaisiin Suomeen ilmoittautuviin tunnistuspalvelun tarjoajiin.

Muistion tarkoituksena on antaa toimijoille ennakoivaa neuvontaa siitä, miten Liikenne- ja viestintävirasto tulkitsee tunnistuslaissa säädettyjä velvoitteita tilanteessa, jossa sama tunnistuspalvelun tarjoaja tarjoaa rinnakkain vahvaa ja rekisteröimätöntä sähköistä tunnistamista. Muistiossa tarkastellaan vahvan ja heikon sähköisen tunnistusmenetelmän ja niitä tuottavan tunnistusjärjestelmän riittävää eriyttämistä lain vaatimusten kannalta, jotta:

- tunnistusmenetelmien käyttäjät ja tunnistukseen luottavat osapuolet voivat selkeästi erottaa käyttämänsä vahvan tunnistuksen rekisteröimättömästä tunnistuksesta
- rekisteröimättömän tunnistuksen tarjonta ei heikennä teknisesti vahvan sähköisen tunnistusjärjestelmän toteutusta.

Neuvontamuistiossa esitetään esimerkkejä, mutta muistiossa ei ole mahdollista eikä tarkoituksenmukaista pyrkiä ennakoimaan ja linjaamaan neuvontakysymyksiä kaikista nykyisistä ja tulevista teknisistä toteutuksista.

Tyypillisin esimerkkitilanne, jossa neuvontaa on virastolta pyydetty, on samaan mobiilitunnistussovellukseen perustuvan tunnistusmenetelmän tarjoaminen varmuustasoltaan erilaisilla ensitunnistamismenettelyillä. Siksi esimerkit käsittelevät tällaista tilannetta ja erityisesti mobiilisovelluksen tason korottamista rekisteröimättömästä vahvaksi tunnistusmenetelmäksi. Samat periaatteet soveltuvat myös muihin tunnistusmenetelmiin.

1.3 Valvonta ja rekisteröinti vahvan sähköisen tunnistuspalvelun luotettavuuden takaajana

Tunnistuslaissa säädetyt luotettavuusvaatimukset kohdistuvat tunnistuspalveluun, joka on ilmoitettu ja merkitty tunnistuslain mukaisesti liikenne- ja viestintäviraston rekisteriin. Vahvan sähköisen tunnistamisen luotettavuus perustuu osaltaan viranomaisvalvontaan. Ilmoittautuneisiin tunnistuspalveluihin kohdistuvat kokonaisuutena kaikki tunnistuslain vaatimukset.

Sama palveluntarjoaja voi tarjota sekä vahvaa että rekisteröimätöntä tunnistusta. Yritys tai yhteisö voi tunnistuslain estämättä sinänsä tarjota sekä ilmoittautuneena vahvaa sähköistä tunnistuspalvelua että tunnistuslain sääntelyn ulkopuolella rekisteröimätöntä tunnistuspalvelua.

Samaa tunnistusmenetelmää ei tunnistuslain valossa voi tarjota kahdella eri statuksella sekä vahvana että rekisteröimättömänä, vaan menetelmät on eriytettävä riittävästi.

Tunnistusvälineiden käyttäjien ja vahvaan sähköiseen tunnistukseen luottavien osapuolten on voitava luottaa siihen, että viraston rekisteriin merkityt tunnistuspalveluntarjoajien tunnistuspalvelut täyttävät kaikilta osin tunnistuspalvelulle säädetyt vaatimukset. Käyttäjien ja luottavien osapuolten on pystyttävä erottamaan vahvat ja rekisteröimättömät tunnistusvälineet ja menetelmät.

Tunnistuslain 1 §:n perusteella tehdyt poikkeukset lain vaatimuksista tunnistusvälineen tarjoajan omissa palveluissa eivät saa heikentää yleisölle tarjottavaksi ilmoitetun tunnistuspalvelun luotettavuutta.

Sopimusehtojen selkeyden ja kohtuullisuuden arviointi kuuluu yleisen kuluttajansuojasääntelyn alaan ja kuluttaja-asiamiehen toimivaltaan.

Henkilötietojen käsittelyä valvoo toimivaltaisena viranomaisena Tietosuojavaltuutettu.

Pankki- ja maksupalveluita valvoo Finanssivalvonta.

1.4 Lainsäädäntöpoliittinen tavoite lisätä vahvan tunnistuksen käyttöä

Lainsäädäntöpoliittiset seikat eivät ole oikeudellisia tulkintaperusteita, kun arvioidaan, täyttääkö palvelu sille säädetyt vaatimukset. Tässä kohdassa virasto tuo esille lainsäädännön tavoitteita.

Hallituksen esityksessä (HE 36/2009 s. 7–11) viitataan Sähköisen tunnistamisen kehittämisryhmän 2008 laatimiin vahvan sähköisen tunnistamisen kansallisiin linjauksiin. Linjauksien tavoitteena on mm. edistää vahvan tunnistamisen käyttämistä myös palveluissa, jotka eivät välttämättä tarvitsisi vahvaa tunnistamista:

> *Myös sellaisissa palveluissa, jotka eivät itsessään välttämättä tarvitsisi vahvaa tunnistamista, tulee siksi viime kädessä pyrkiä siihen, että käyttäjät voisivat*

käyttää itselleen tuttua ja helppokäyttöistä vahvan tunnistamisen menetelmää. Tämän toteutumiseksi vahvan tunnistustapahtuman kustannustason täytyy olla riittävän edullinen kaikkien toimijoitten kannalta. Toimivien markkinoiden yhtenä tavoitteena onkin pitää hintataso kohtuullisena, mikä toteutuu markkinoilla riittävien vaihtoehtojen ollessa tarjolla. Vaikka tavoitteena on se, että kukin käyttäjä voisi käyttää valitsemaansa vahvan tunnistusvälinettä mahdollisimman monessa palvelussa, ei palveluntarjoajia voida kuitenkaan pakottaa hyväksymään jotakin välinettä tai vahvan sähköisen tunnistamisen palvelun tarjoajaa.

Viraston käsityksen mukaan tavoite on edelleen ajankohtainen. Vuonna 2020 ilmi tullut vakava psykoterapiapalveluun kohdistunut tietomurto järkytti yhteiskuntaa ja käynnisti Suomessa laajan julkisen keskustelun mm. tarpeesta lisätä vahvan sähköisen tunnistuksen käyttöä yksityisen sektorin asiointipalveluissa. Myös EU:n eIDAS-asetuksen muutostarpeiden arvioinnissa komissio on korostanut tarvetta lisätä sähköisen tunnistuksen käyttöä yksityisellä sektorilla.

2 Termit

Vahvalla sähköisellä tunnistamisella tai tunnistusmenetelmällä tarkoitetaan tässä muistiossa tunnistusta, jonka tarjoaminen on ilmoitettu ja hyväksytty tunnistuslain mukaiseen tunnistuspalvelurekisteriin. Vahvan tunnistuspalvelun vaatimustenmukaisuus on arvioitu ja sitä valvotaan sääntelyn mukaisesti. Palvelun varmuustaso voi olla korotettu tai korkea.

Rekisteröimättömällä tai heikolla tunnistuspalvelulla tai tunnistusmenetelmällä tarkoitetaan tässä muistiossa sähköistä tunnistuspalvelua, jota ei ole ilmoitettu tunnistuslain mukaiseen rekisteriin. Rekisteröimättömän tunnistuspalvelun luotettavuutta ei siten ole arvioitu eikä sitä valvota sääntelyn mukaisesti.

Tunnistusvälineen tarjoaja tarjoaa tunnistusvälineitä yleisölle eli käyttäjille sekä tarjoaa tunnistusvälinettään tunnistusvälityspalvelun tarjoajalle välitettäväksi luottamusverkostossa.

Tunnistusvälityspalvelun tarjoaja välittää tunnistustapahtumia luottaville osapuolille eli sähköisten asiointipalveluiden tarjoajille.

Tunnistusvälineen haltija on luonnollinen tai oikeushenkilö, jolle tunnistusvälineen tarjoaja on sopimukseen perustuen antanut tunnistusvälineen. Tässä muistiossa käytetään haltijasta pääsääntöisesti termiä käyttäjä.

Luottava osapuoli on luonnollinen tai oikeushenkilö, joka luottaa sähköiseen tunnistamiseen. Luottavia osapuolia ovat asiointipalvelut, jotka hankkivat asiakkaidensa sähköisen tunnistuksen tunnistusvälityspalvelulta.

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.

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.

Tunnistusvälineen tarjoajia ovat muistion laatimishetkellä pankit, mobiiliteleyritykset ja Digi- ja väestötietovirasto. Osa niistä toimii myös tunnistusvälityspalveluna. Lisäksi rekisterissä on 2 pelkästään tunnistusvälityspalvelua tarjoavaa toimijaa.

3 Säännökset ja tulkinnat

3.1 Vahvan sähköisen tunnistuksen tarjonnan luotettavuus ja soveltamisala lain perusteella

3.1.1 Säännökset

Tunnistuslain (617/2009 muutoksineen) 1 §:n mukaan laissa säädetään vahvasta sähköisestä tunnistamisesta sekä tunnistuspalveluiden tarjoamisesta palveluntarjoajille, yleisölle ja toisille tunnistuspalvelun tarjoajille. Lakia ei sovelleta yhteisön sisäiseen tunnistamiseen käytettävien palveluiden tarjontaan. Lakia ei sovelleta myöskään yhteisöön, joka käyttää omaa tunnistusmenetelmäänsä omien asiakkaidensa tunnistamiseen omissa palveluissaan.

Lain 10 §:n mukaan tunnistuspalvelun tarjoajan on ennen toiminnan aloittamista tehtävä kirjallinen ilmoitus Liikenne- ja viestintävirastolle ja annettava palveluntarjoajasta ja palvelusta pykälässä säädetyt tiedot. Lain 11 §:n mukaan ilmoituksen voi tehdä myös Euroopan talousalueelle sijoittautunut tunnistuspalvelun tarjoaja.

Lain 12 §:n mukaan Liikenne- ja viestintävirasto ylläpitää julkista rekisteriä 10 §:n mukaisen ilmoituksen tehneistä tunnistuspalvelun tarjoajista ja niiden tarjoamista palveluista.

Lain 14 §:n mukaan tunnistuspalvelun tarjoajalla on oltava tunnistusperiaatteet, joissa määritellään tarkemmin, kuinka palveluntarjoaja täyttää tässä laissa säädetyt velvollisuutensa. Tunnistuspalvelun tarjoajan on pidettävä tunnistusperiaatteet yleisesti saatavilla ja ajantasaisina.

Hallituksen esityksessä 36/2009 todetaan seuraava:

> *Rekisterin olemassaolo on yksi ajatellun järjestelyn kulmakivistä. Sekä tunnistusvälinettä hankkiva, usein kuluttajan ominaisuudessa toimiva henkilö että tunnistuspalvelua hankkiva palveluntarjoaja joutuvat ratkaisemaan kysymyksen siitä, mihin tunnistuspalvelun tarjoajaan ne voivat luottaa. Viestintäviraston internetsivustolla julkaistava julkinen rekisteri antaa helpolla tavalla tiedon niistä palveluntarjoajista, joiden voidaan lähtökohtaisesti odottaa noudattavan tämän lain säännöksiä, ja jotka ovat viranomaisen valvonnassa.*
>
> *…*
>
> *Suurin osa sähköisistä palveluista ei edellytä sähköistä tunnistamista tai sähköisiä allekirjoituksia. Osassa sähköisiä palveluita voidaan kuitenkin muun muassa tehdä erilaisia oikeustoimia. Tällaiset sähköiset palvelut edellyttävät osapuolten välisen luottamussuhteen olemassa oloa. Palvelun käyttäjän on voitava luottaa siihen, että palveluntarjoaja on palveluansa rakentaessaan ottanut huomioon tietoturvan ja yksityisyyden suojan vaatimukset. Palveluntarjoajan on puolestaan voitava luottaa siihen, että etäyhteyden päässä oleva palvelunkäyttäjä on se, joka väittää olevansa. Sähköisten palveluiden ja sähköisen asioinnin kehittyminen edellyttää siten hyvin toimivia sähköisen tunnistamisen palveluita.*

Hallituksen esityksessä 272/2014 todetaan 12 a §:n perusteluissa seuraavaa:

Tunnistuspalvelua on mahdollista tarjota myös ilmoittautumatta Viestintävirastoon, mutta tällöin tunnistuspalvelun tarjoajalla ei ole vahvan sähköisen tunnistuspalvelun tarjoajan asemaa. Luottamusverkostossa toimivaa tunnistuspalvelun tarjoajaa velvoittavat ne säädökset, joista laissa vahvasta sähköisestä tunnistamisesta ja [sähköisistä allekirjoituksista] on säädetty, kuten tunnistuspalvelun tarjoajan yleiset velvollisuudet.

3.1.2 Linjaukset

Liikenne- ja viestintävirasto katsoo tunnistuslain ja sen perustelujen perusteella, että luotettavuusvaatimukset kohdistuvat virastolle ilmoitettuun ja rekisterissä julkaistuun tunnistuspalveluun kokonaisuutena ja että vahvan sähköisen tunnistamisen luotettavuus perustuu osaltaan viranomaisvalvontaan.

Tilannetta, jossa väitetään tarjottavan faktisesti samaa tunnistusvälinettä kahdella eri statuksella, ei ole oikeudellisesti ottaen lainkaan mahdollista erottaa siitä, että säädettyjä vaatimuksia ei noudateta (esimerkki: asiakkaiden vahvan tunnistuksen tarjoaminen asiointipalvelulle ilman vaadittua salausta). Vahvaa sähköistä tunnistusta koskevat vaatimukset soveltuvat joka tapauksessa, kun on kyse vahvan sähköisen tunnistuspalvelun tarjonnasta.

Eri asia on, että tunnistuslakia ei lain 1 §:n poikkeusäännöksen mukaan sovelleta yhteisön oman tunnistusmenetelmän käyttöön sen omien asiakkaiden tunnistamiseen yhteisön omissa palveluissa. Siten myös tunnistuslain mukaiseen rekisteriin ilmoitetun tunnistuspalvelun tunnistuslaissa säädettyjä vaatimuksia ei tarvitse noudattaa tunnistuspalveluntarjoajan omissa palveluissa. Tällaiset poikkeukset eivät saa heikentää yleisölle tarjottavaksi ilmoitetun tunnistuspalvelun luotettavuutta.

Esimerkiksi verkkopankkitunnuksia voidaan tarjota yleisölle tunnistuslain mukaisena vahvana sähköisenä tunnistusvälineenä ja samaa tunnistusmenetelmää ja -välinettä voidaan lain poikkeussäännöksen perusteella käyttää rajoitettuina verkkopankkitunnuksina pankin omien asiakkaiden tunnistamisessa pankin omissa palveluissa noudattamatta näissä asiointilanteissa kaikkia tunnistuslain vaatimuksia.

Pankki- ja maksupalveluita valvoo Finanssivalvonta.

3.2 Ensitunnistaminen ja rekisteröimättömän tunnistusvälineen korottaminen vahvaksi

3.2.1 Yleistä

Ensitunnistamisella tarkoitetaan niitä menettelyjä, joilla verifioidaan tunnistusvälineen hakijan henkilöllisyys, jotta vahva sähköinen tunnistusväline myönnetään varmasti oikealle henkilölle ja oikean henkilön haltuun.

Luotettavat lähteet ja ensitunnistaminen. Tunnistuslain 17 §:ssä säädetään menettelyvaihtoehdoista ja Suomessa hyväksyttävistä luotettavista lähteistä, joihin henkilöllisyyden osoittaminen voi perustua. Luotettavat lähteet ovat kansallisesti säädettävä asia. Ensitunnistusmenettelyt tunnistuslaissa vastaavat EU:n varmuustasoasetuksen menettelyjä. Luotettavia lähteitä ovat viranomaisen myöntämät passit ja henkilökortit.

Ensitunnistus voi perustua passin tai henkilökortin esittämisen sijasta myös toiseen vahvaan sähköiseen tunnistusmenetelmään, poliisin tekemään ensitunnistamiseen tunnistusvälineen myöntämistä varten tai muuhun lakiin perustuvaan menettelyyn, jonka liikenne- ja viestintävirasto erikseen hyväksyy.

Lisäksi henkilöllisyys on tarkistettava väestötietojärjestelmästä. Vahva sähköinen tunnistusväline perustuu siten aina valtion takaamaan henkilöllisyyteen.

Etäensitunnistaminen (*remote identification*). Tulkintakysymyksiä liittyy tällä hetkellä Euroopan laajuisesti erityisesti siihen, miten voidaan luotettavasti todistaa ja varmentaa (engl. *identity proofing and verification*) tunnistusvälineen hakijan henkilöllisyys virallisista henkilöllisyystodistuksista sähköisellä menettelyllä. Liikenne- ja viestintävirasto on koonnut tarkasteltavat näkökohdat tunnistuspalveluiden arviointiohjeeseen 211/2019 S kohtaan 3.10. Virasto seuraa kansainvälistä keskustelua ja tarkentaa tulkintaa.

Tunnistusmenetelmän varmuustason korottaminen. Tulkintakysymyksiä voi syntyä myös siitä, miten rekisteröimätön sähköinen tunnistusmenetelmä voidaan korottaa vahvaksi sähköiseksi tunnistusmenetelmäksi. Erityisesti mobiilisovellusten tarjoamisessa monet toimijat suunnittelevat, että sovelluksen voi ottaa käyttöön rekisteröimättömänä tunnistusmenetelmänä ilman lain mukaista ensitunnistusta ja sovelluksen voi korottaa vahvaksi menetelmäksi, kun luotettava ensitunnistus tehdään.

Esimerkkitilanteessa samanlainen mobiilisovellus on käyttäjille tarjolla kahdella erilaisella myöntämistavalla

- Kevyempi myöntämistapa ei täytä tunnistuslain ensitunnistusvaatimuksia eikä tähän menettelyyn perustuvaa tarjontaa ilmoiteta tunnistuspalvelurekisteriin
- sääntelyn vaatimukset täyttävällä ensitunnistamisella käyttäjä voi korottaa tunnistussovelluksen varmuustason vahvalle tasolle ja tämä myöntämismenettely ja tunnistuspalvelun tarjonta ilmoitetaan tunnistuspalvelurekisteriin

3.2.2 Linjaukset

Vahvan sähköisen tunnistusvälineen myöntämisen täytyy aina perustua lain mukaiseen ensitunnistamisen menettelyyn ja lain mukaisiin lähteisiin.

Ensitunnistus voi perustua henkilöllisyyden todentamiseen vahvalla sähköisellä tunnistuksella tai passin tai henkilökortin esittämiseen käyntiasioinnissa tai luotettavalla etäyhteysmenetelmällä. Passin tai henkilökortin esittämisessä on voitava varmistua siitä, että se on aito ja että se on esittäjän oma.

Rekisteröimätön tunnistusmenetelmä voi olla osa vahvan tunnistusmenetelmän myöntämistä ja ensitunnistusta eli hakijan henkilöllisyyden varmentamista.

Rekisteröimätön tunnistusmenetelmä ja sen myöntämisessä käytetty henkilöllisyyden varmentaminen ei yksistään voi toimia vahvan ensitunnistamisen perustana. Se voi kuitenkin olla osa vahvan tunnistusmenetelmän myöntämisprosessia ja ensitunnistusta eli hakijan henkilöllisyyden varmentamista.

Menettelyssä on otettava jo korotetulla varmuustasolla huomioon se riski, että rekisteröimätön tunnistusväline ja passi tai henkilökortti ovat voineet joutua vääriin käsiin tai että passi tai henkilökortti voi olla väärennetty.

Esimerkiksi sovellus on voitu alun perin ottaa käyttöön väärillä henkilötiedoilla, mobiililaite voi olla väärissä käsissä tai sovelluksesta on voitu luoda oikeudettomasti instanssi ulkopuolisen tahon haltuun.

Rekisteröimättömän tunnistusmenetelmän ja sen todentamistekijöiden (kuten pankkitunnukset tai mobiilisovellus) muuttaminen vahvaksi tunnistusmenetelmäksi edellyttää sellaisia lisävarmistuksia, että vaatimukset vahvan tunnistusmenetelmän hakijan henkilöllisyyden varmentamisesta täyttyvät kokonaisuutena arvioiden.

Lisävarmistuksilla on voitava varmistua siitä, että vahvaksi muutettava rekisteröimätön tunnistusväline on ja pysyy oikean hakijan hallussa.

Kokonaisarvioinnissa voidaan huomioida seuraavat

- passin tai henkilökortin aitouden tarkistamisen luotettavuus
- passin tai henkilökortin voimassaolon tarkistus
- hakijan ominaisuuksien vertailu esittämäänsä henkilöllisyystodistukseen
- erilaiset lisäkontrollit kuten kysymykset vain oikean hakijan tiedossa olevista seikoista
- myöntämisen jälkeen tehtävä haltijan tiedottaminen eri kanavia käyttäen
- seuranta, poikkeamien havainnointi ja niihin reagointi
- rekisteröimättömän tunnistusvälineen myöntämisen, toimitusmenettelyn ja käytön yhteydessä tehdyt varmistukset
- toimitusmenettelyyn liittyvät varmistukset varmuustason korottamisen yhteydessä

3.2.3 Säännökset

TunnL 8 § (29.6.2016/533) Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset

Sähköisen tunnistamisen järjestelmän on täytettävä seuraavat vaatimukset:

1) tunnistusmenetelmän perustana on 17 ja 17 a §:n mukainen tunnistaminen, jota koskevat tiedot ovat jälkikäteen 24 §:n mukaisesti tarkastettavissa;

2) tunnistusmenetelmällä voidaan yksiselitteisesti tunnistaa tunnistusvälineen haltija siten, että 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 annetussa komission täytäntöönpanoasetuksen (EU) 2015/1502, jäljempänä sähköisen tunnistamisen varmuustasoasetus, liitteen kohdissa 2.1.2, 2.1.3 ja 2.1.4 vähintään korotetulle varmuustasolle säädetyt edellytykset täyttyvät;

[…]

17 § (23.11.2018/1009) Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen

Ensitunnistamisessa luonnollisen henkilön tunnistaminen tulee tehdä henkilökohtaisesti tai sähköisesti siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.1.2 korotetulle tai korkealle varmuustasolle säädetyt vaatimukset täyttyvät. Henkilön henkilöllisyyden varmentaminen voi perustua viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan tai tässä laissa tarkoitettuun vahvaan sähköiseen tunnistusvälineeseen. Lisäksi henkilöllisyyden varmentaminen voi perustua julkisen tai yksityisen tahon aiemmin muuhun tarkoitukseen kuin vahvan sähköisen tunnistusvälineen myöntämiseen käyttämään menettelyyn, jonka Liikenne- ja viestintävirasto hyväksyy menettelyä koskevien säännösten ja viranomaisvalvonnan perusteella tai 28 §:n 1 kohdassa tarkoitetun vaatimustenmukaisuuden arviointilaitoksen vahvistuksen perusteella.

Ensitunnistamisessa, joka perustuu yksinomaan viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan, hyväksyttäviä asiakirjoja ovat voimassa oleva Euroopan talousalueen jäsenvaltion, Sveitsin tai San Marinon viranomaisen myöntämä passi tai henkilökortti.

Halutessaan tunnistusvälineen tarjoaja voi käyttää henkilöllisyyden varmentamisessa myös muun valtion viranomaisen myöntämää voimassa olevaa passia.

Jos tunnistusvälineen hakijan henkilöllisyyttä ei voida luotettavasti todentaa, hakemukseen liittyvän ensitunnistamisen tekee poliisi. Poliisin tekemästä ensitunnistamisesta tunnistusvälineen hakijalle aiheutuva kustannus on julkisoikeudellinen suorite. Suoritteen maksullisuudesta säädetään valtion maksuperustelaissa.

[…]

TunnL 7 § (20.2.2015/139) Väestötietojärjestelmän tietojen käyttäminen

Tunnistusvälineen tarjoajan ja luottamuspalvelua tarjoavan varmentajan on hankittava ja päivitettävä luonnollisen henkilön tunnistuspalvelun tarjoamiseksi tarvitsemansa tiedot väestötietojärjestelmästä. Tämän lisäksi tunnistuspalvelun tarjoajan on varmistettava, että sen tunnistuspalvelun tarjoamiseksi tarvitsemat tiedot ovat ajan tasalla väestötietojärjestelmän tietojen kanssa. (29.6.2016/533)

[…]

3.3 Vahvan ja rekisteröimättömän tunnistusmenetelmän eriyttäminen käyttäjän tunnistusvälineessä

3.3.1 Yleistä

Käyttäjän todentamistekijät. Tunnistusvälineen käyttöön ja tunnistusmenetelmään liittyvät käyttäjän havaittavissa olevat todentamistekijät ja tunnistustapahtumien teknisen toteuttamisen todentamismekanismi, joka ei ole käyttäjän havaittavissa.

Tässä kohdassa tarkastellaan käyttäjän havaittavissa olevia ominaispiirteitä, joiden perusteella käyttäjä pystyy erottamaan yhden tunnistusmenetelmän muista tunnistusmenetelmistä ja siten myös vahvan tunnistusmenetelmän rekisteröimättömästä menetelmästä. Kysymys on siis eroista, joiden perusteella käyttäjä pystyy selkeästi ymmärtämään sähköisessä asioinnissa käyttävänsä eri tunnistusmenetelmiä, joihin liittyy erilainen sääntelyn suoja.

Tuotteistaminen. Liikenne- ja viestintävirasto toteaa, että tunnistuslaissa ei luonnollisestikaan säädetä nimenomaisesti tuotteistamisesta tai brändäämisestä, joten tulkinta on perustettava yleiseen mahdollisimman objektiiviseen arviointiin ja toteutettavuuteen. Huomioon täytyy ottaa sähköisen tunnistusmenetelmän ominaisen käyttöympäristön vaatimukset, koska esimerkiksi tunnuslukulaitteen, verkkoselaimen, mobiilisovelluksen ja sirukortin käyttö eroavat toisistaan.

Tunnistuspalveluiden yhteiset käytännöt. Virasto toteaa myös, että tuotteistamisessa olisi toivottavaa pyrkiä löytämään esimerkiksi tunnistuspalveluiden luottamusverkoston yhteistyössä yhteisiä hyviä käytäntöjä, joita kaikki tunnistuspalvelun tarjoajat voisivat käyttää samansuuntaisesti vahvan ja rekisteröimättömän tunnistuksen erottamiseksi. Tämä parantaisi käyttäjien mahdollisuutta ymmärtää tunnistuspalvelujen eroja ja luottamusta vahvaan tunnistamiseen.

3.3.2 Linjaukset

Liikenne- ja viestintävirasto katsoo, että vahvan ja rekisteröimättömän tunnistusmenetelmän erottamisessa on huomioitava seuraavat käyttäjän havaittavissa olevat piirteet

1) Tunnistusmenetelmien nimien täytyy erota riittävästi
2) Tunnistusmenetelmien visuaalisen ulkoasun on erottava riittävästi.

3) Vahvassa ja rekisteröimättömässä tunnistusmenetelmässä voi harkita käytettäväksi eri luokkien todentamistekijöitä, jos se on teknisesti toteutettavissa.
4) Käyttäjän mahdollisuus huolehtia vahvasta tunnistusvälineestä on turvattava.
5) Saavutettavuus on huomioitava

Liikenne- ja viestintävirasto katsoo, että vahvan ja heikon tunnistusmenetelmän erottamisessa on huomioitava seuraavat käyttäjän havaittavissa olevat piirteet

1) Tunnistusmenetelmien nimien täytyy erota riittävästi. Kokonaan erinäminen tunnistustuote erottaa vahvan menetelmän riittävästi. Jos kuitenkin tuotenimi halutaan pitää vahvalla ja rekisteröimättömällä menetelmällä pääosin samana, vahva menetelmä on erotettava jollain selkeästi ymmärrettävällä ja erottavalla nimen osalla tai lisäyksellä. Nimien erottuvuudessa on syytä huomioida myös esteelliset henkilöt.

2) Tunnistusmenetelmien visuaalisen ulkoasun on erottava riittävästi. Erottamisessa voidaan käyttää erilaisia logoja, eri värejä, erottavaa sanastoa ja muita visuaalisesti erottavia piirteitä. Erottamisessa on syytä huomioida esteelliset henkilöt, joten pelkkää näköaistilla havaittavissa olevaa erottamista ei voida pitää riittävänä.

3) Vahvassa ja heikossa tunnistusmenetelmässä voi harkita käytettäväksi eri luokkien todentamistekijöitä, jos se on teknisesti toteutettavissa.

Toteutettavuudessa voidaan huomioida käyttöympäristö ja käytettävyys.

Todentamistekijät jaetaan sääntelyssä seuraaviin luokkiin:
- hallussapitoon perustava todentamistekijä
- tiedossa oloon perustava todentamistekijä
- luontainen todentamistekijä perustuu johonkin luonnollisen henkilön fyysiseen ominaisuuteen

Virasto arvioi, että vahvassa ja rekisteröimättömässä tunnistusmenetelmässä on aina mahdollista käyttää erilaista tiedossa oloon perustuvaa todentamistekijää (esimerkiksi PIN-koodi tai muu salasana). Saman todentamistekijäluokan todentamistekijöiden käyttö on siis hyväksyttävää. Tunnistusvälineen tarjoaja voi harkita eri PIN-koodin tai salasanan määrittelyä tarjotessaan heikkoa ja vahvaa tunnistusta esimerkiksi samalla tunnistussovelluksella. Tunnistuspalvelun tarjoajien selvityksen perusteella on kuitenkin perusteltua ottaa huomioon havainnot siitä, pysyvätkö käyttäjät hallitsemaan eri salasanat tai PIN-koodit tällaisessa käyttöyhteydessä.

Hallussapitoon perustuva todentamistekijä (esimerkiksi salasanalaite, salasanalista, mobiilisovellus, SIM-kortti) voi olla erotettavissa, mutta erottamisen toteutettavuudessa voi olla teknisiä toteutettavuusongelmia ja menetelmän käytettävyydelle voi syntyä kielteisiä vaikutuksia.

Ominaisuuksiin perustuva todentamistekijä (sormenjälki, kasvokuva, jne.) on mahdollista erottaa esimerkiksi siten, että biometristä tekijää ei käytetä lainkaan jommassakummassa menetelmässä tai menetelmissä käytetään eri ominaisuutta tai vahvassa menetelmässä olisi käytettävä useamman biometrisen ominaisuuden yhdistelmää. Tässäkin on perusteltua ottaa huomioon havainnot käyttäjien tyypillisestä toiminnasta.

4) Käyttäjän mahdollisuus huolehtia vahvasta tunnistusvälineestä on turvattava.

Tunnistuslain 23 §:ssä säädetään tunnistusvälineen haltijan velvollisuudesta huolehtia tunnistusvälineensä säilyttämisestä ja kiellosta luovuttaa välinettä toisen käyttöön.

Liikenne- ja viestintävirasto katsoo, että vahvan ja rekisteröimättömän tunnistusmenetelmän piirteiden määrittelyssä on huomioitava käyttäjän mahdollisuus säilyttää tunnistusvälineensä laissa säädetyn velvollisuutensa mukaisesti huolellisesti siten, että rekisteröimättömän tunnistusmenetelmän käyttö ei vaaranna vahvan menetelmän tekijöiden pysymistä vain käyttäjän hallussa ja käytettävissä.

5) Saavutettavuus

Digitaalisten palveluiden tarjoamisesta annetun lain (306/2019, nk. digipalvelulaki) eräät vaatimukset koskevat vahvan sähköisen tunnistuspalvelun tarjoajia. Lain 2 § 4 kohdan mukaan tarkoitetaan *saavutettavuudella periaatteita ja tekniikoita, joita on noudatettava digitaalisten palvelujen suunnittelussa, kehittämisessä, ylläpidossa ja päivittämisessä, jotta ne olisivat paremmin käyttäjien, erityisesti vammaisten henkilöiden, saavutettavissa.*

Lain vaatimuksiin liittyy kansainvälisesti annettavia standardeja, jotka koskevat verkkoselaimia ja mobiilisovelluksia.

Liikenne- ja viestintävirasto ei valvo lakia, mutta neuvoo tässä yhteydessä huomioimaan digipalvelulain vaatimusten mahdollisen vaikutuksen eriyttämiseen. Virasto arvioi, että myös esteellisen käyttäjän on kyettävä havainnoimaan, käyttääkö vahvaa vai rekisteröimätöntä tunnistusmenetelmää.

3.3.3 Säännökset

TunnL 8 a § (29.6.2016/533) Tunnistusmenetelmässä käytettävät todentamistekijät

Tunnistusmenetelmässä on käytettävä vähintään kahta seuraavista todentamistekijöistä:

1) tiedossa oloon perustuvaa todentamistekijää, jonka henkilön on osoitettava olevan tiedossaan;

2) hallussapitoon perustuvaa todentamistekijää, jonka henkilön on osoitettava olevan hallussaan;

3) luontaista todentamistekijää, joka perustuu johonkin luonnollisen henkilön fyysiseen ominaisuuteen.

[…]

TunnL 8 § (29.6.2016/533) Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset

Sähköisen tunnistamisen järjestelmän on täytettävä seuraavat vaatimukset:

[…]

3) tunnistusmenetelmällä voidaan varmistua, että ainoastaan tunnistusvälineen haltija voi käyttää välinettä siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdissa 2.2.1 ja 2.3 vähintään korotetulle varmuustasolle säädetyt edellytykset täyttyvät;

[…]

[…]

3.4 Todentamismekanismin ja tunnistusjärjestelmän tekniset vaatimukset

3.4.1 Yleistä

Tunnistuslain 8 §:ssä ja 8 a §:ssä sekä EU:n varmuustasoasetuksen liitteen kohdassa 2.3 säädetään siitä, että tunnistusmenetelmän täytyy olla ainoastaan tunnistusvälineen haltijan käytettävissä ja todentamismekanismin täytyy kestää varmuustason mukaan määriteltävän vakavuustason hyökkäys. Tunnistuslain 23 §:ssä säädetään käyttäjän velvollisuudesta huolehtia tunnistusvälineestään.

Todentamismekanismin vaatimukset kohdistuvat erityisesti tunnistusmenetelmään liittyviin eritasoisiin salaisuuksiin. Tähän liittyvät myös viraston määräyksen 72 6 §:ssä määrätyt tarkennukset.

Tunnistusjärjestelmän vaatimuksia säädetään muutoin tunnistuslain 13 §:ssä ja EU:n varmuustasoasetuksen kohdissa 2.4.4 Tietojen säilyttäminen, 2.4.5 Tilat ja henkilökunta ja 2.4.6 Tekniset tarkastukset. Vaatimuksia tarkennetaan viraston määräyksen 72 5 §:ssä Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet ja 7 §:ssä Tunnistusjärjestelmän ja rajapintojen salausvaatimukset.

Tässä muistiossa ei ole tarkoitus selostaa kaikkia vaatimuksia, mutta alle Säännökset -kohtaan on poimittu viittaus keskeisiin luotettavuutta koskeviin säännöksiin.

3.4.2 Linjaukset

Vahvan sähköisen tunnistusmenetelmän salaisuuksien suoja käsittää käyttäjän tiedossa olevat salaisuudet ja menetelmän omaispiirteisiin liittyvät salaisuudet.

Vahvan tunnistusmenetelmän todentamistekijöiden kytkemisessä vahvasti ensitunnistettuun henkilöön on huomioitava erityisesti todentamistekijöiden ja tunnistusmekanismin salaisuuden (yksityisen avaimen) turvallisuus.

Menetelmään liittyvä salaisuus on tyypillisesti esimerkiksi mobiilivarmenteen PKI-toteutukseen liittyvä käyttäjälle näkymätön yksityinen allekirjoitusavain, joka on tallennettu SIM-kortille tai mobiilisovelluksen yksityinen avain, joka on tallennettu mobiililaitteen suojattuun SE- tai TEE-komponenttiin.

Tunnistusmenetelmän ja todentamismekanismin toteutuksessa on varmistettava vahvan tunnistusmenetelmän todentamismekanismissa käytettävien salaisuuksien suoja tunnistusmenetelmän elinkaaren kaikissa vaiheissa.

Rekisteröimättömän tunnistusmenetelmän rinnakkainen tarjonta ei saa miltään osin heikentää vahvan tunnistuksen salaisuuksien suojaa varmuustason mukaisen vakavuustason hyökkäykseltä.

Liikenne- ja viestintävirasto katsoo, että jos heikolla ensitunnistamisella myönnetty tunnistusmenetelmä korotetaan lain mukaisella ensitunnistamisella vahvaksi, täytyy kiinnittää huomiota erityisesti siihen, että tunnistusmenetelmän ja todentamismekanismissa käytettävät salaisuudet on luotu ja että niistä huolehditaan vahvan tunnistamisen vaatimusten mukaisesti.

Liikenne- ja viestintävirasto katsoo, että jos avaintietojen/salaisuuksien käsittely rekisteröimättömässä tunnistusmenetelmässä käytettävässä mobiilisovelluksessa ei täytä vahvan tunnistusmenetelmän vaatimuksia, vahvassa tunnistusmenetelmässä on lähtökohtaisesti luotava uusi yksityinen avain/salaisuus.

Virasto arvioi, että ainakin SE- tai TEE-komponenttiin tallennettu salaisuus on niin luotettavasti suojattu, että saman salaisuuden käyttämistä voi harkita rekisteröimättömässä ja vahvassa tunnistusmenetelmässä. Salaisuuksien turvallisuus on kuitenkin arvioitava kokonaisuutena ja ottaen huomioon käytössä olevat turvakontrollit.

Virasto katsoo, että todentamismekanismin ja salaisuuksien suojaamisesta täytyy huolehtia koko tunnistusjärjestelmässä eli myös tunnistuksen luotettavuuteen ja hyökkäyksenkestävyyteen vaikuttavissa taustajärjestelmissä siten, että rekisteröimättömän tunnistuksen tarjoaminen ei heikennä vahvan tunnistusmenetelmän suojaa. Tunnistusjärjestelmässä on huomioitava mm. seuraavat asiat:
- Todentamistekijöiden kytkeminen käyttäjään taustajärjestelmässä
- Todentamistekijöiden tekninen toteutus
- Tietojen säilytys
- Pääsynhallinta järjestelmään ja tietoihin
- Rajapintojen salaus ja yhteyskäytännöt.

3.4.3 Säännökset

TunnL 8 § (29.6.2016/533) Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset

Sähköisen tunnistamisen järjestelmän on täytettävä seuraavat vaatimukset:

[…]

4) tunnistusjärjestelmä on turvallinen ja luotettava siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdissa 2.2.1, 2.3.1 ja 2.4.6 vähintään korotetulle varmuustasolle säädetyt edellytykset täyttyvät ottaen huomioon kulloinkin käytettävissä olevaan tekniikkaan liittyvät tietoturvallisuusuhat sekä tunnistuspalvelun tarjoamiseen käytettävät tilat ovat turvallisia sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.4.5 säädetyllä tavalla;

5) tietoturvallisuuden hallinnasta on huolehdittu siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdan 2.4 johdanto-osassa ja kohdissa 2.4.3 ja 2.4.7 vähintään korotetulle varmuustasolle säädetyt edellytykset täyttyvät.

[…]

TunnL 8 a § (29.6.2016/533) Tunnistusmenetelmässä käytettävät todentamistekijät

Tunnistusmenetelmässä on käytettävä vähintään kahta seuraavista todentamistekijöistä:

[…]

Jokaisessa tunnistusmenetelmässä on käytettävä sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.3.1 tarkoitettua sellaista dynaamista todentamista, joka muuttuu jokaisessa uudessa henkilön ja hänen henkilöllisyytensä varmentavan järjestelmän välillä tapahtuvassa todentamistapahtumassa.

EU:n varmuustasoasetus Liite, 1. Sovellettavat 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;

Tunnistuslaki 13 § Tunnistuspalvelun tarjoajan yleiset velvollisuudet

Tunnistuspalvelun tarjoajan tunnistamiseen liittyvien tietojen säilyttämisen, henkilökunnan ja alihankintana käyttämien palvelujen tulee täyttää sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdissa 2.4.4 ja 2.4.5 vähintään korotetulle varmuustasolle säädetyt vaatimukset. Lisäksi tunnistuspalvelun tarjoajalla tulee olla kattava suunnitelma tunnistuspalvelun päättämisen varalta. (29.6.2016/533)

[…]

TunnL 23 § Tunnistusvälineen haltijan velvollisuudet

Tunnistusvälineen haltijan on käytettävä tunnistusvälinettä sopimuksen ehtojen mukaisesti. Haltijan on säilytettävä tunnistusvälinettä huolellisesti. Haltijan velvollisuus huolehtia tunnistusvälineestä alkaa, kun hän on vastaanottanut sen.

Tunnistusvälineen haltija ei saa luovuttaa välinettä toisen käyttöön.

EU:n varmuustasoasetus Liite, 2.3.1 Todentamismekanismi

MATALA

[…]

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

[…]

KOROTETTU

Taso ”matala” lisättynä seuraavalla:

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.

KORKEA

Taso ”korotettu” lisättynä seuraavalla:

Todentamismekanismissa toteutetaan turvatoimenpiteitä sähköisen tunnistamisen menetelmän varmentamiseksi siten, että on erittäin epätodennäköistä, että viestin arvaaminen, salakuuntelu, toisto tai manipulointi hyökkäyksessä, jonka vakavuusaste on korkea (”high”), voi heikentää todentamismekanismeja.

M72 6 § Tunnistusmenetelmän tietoturvavaatimukset

Tunnistusvälinettä ei saa yhdistää hakijaan ennen hakijan ensitunnistamista tai tunnistusvälineen myöntämisprosessissa on muutoin varmistettava, että tunnistusväline ei ole käytettävissä ennen kuin tunnistus- ja luottamuspalvelulain 17 §:n mukainen ensitunnistaminen on tehty.

Palveluntarjoajan on varmistettava, etteivät tunnistusvälineeseen liittyvät salaiset tiedot paljastu sen henkilöstölle missään tilanteessa.

Palveluntarjoaja ei saa kopioida tunnistusvälineeseen liittyviä salaisia tietoja.

Tunnistuslaki 13 § Tunnistuspalvelun tarjoajan yleiset velvollisuudet

Tunnistuspalvelun tarjoajan tunnistamiseen liittyvien tietojen säilyttämisen, henkilökunnan ja alihankintana käyttämien palvelujen tulee täyttää sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdissa 2.4.4 ja 2.4.5 vähintään korotetulle varmuustasolle säädetyt vaatimukset. Lisäksi tunnistuspalvelun tarjoajalla tulee olla kattava suunnitelma tunnistuspalvelun päättämisen varalta. (29.6.2016/533)

[…]

LoA 2.4.4 Tietojen säilyttäminen

MATALA

1. Asiaankuuluvat tiedot kirjataan ja säilytetään käyttämällä tehokasta tiedonhallintajärjestelmää ottaen huomioon sovellettava lainsäädäntö ja tietosuojaan ja tietojen säilyttämiseen liittyvät hyvät käytännöt

2. Järjestelmään kirjatut tiedot säilytetään siltä osin kuin tämä on kansallisen lainsäädännön tai muun kansallisen hallinnollisen järjestelyn mukaan sallittua ja suojataan niin kauan kuin niitä tarvitaan tarkastuksia ja tietoturvaloukkausten tutkimista varten ja säilytetään siihen asti, kun tiedot hävitetään turvallisesti

KOROTETTU/KORKEA

Sama kuin tasolla "matala" lisättynä seuraavalla:

Arkaluonteinen salaustekninen aineisto, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, on suojattu luvattomalta käsittelyltä.

LoA 2.4.5 Tilat ja henkilökunta

MATALA/KOROTETTU

1. Käytössä on menettelyt, joilla varmistetaan, että henkilöstöllä ja alihankkijoilla on riittävä koulutus, pätevyys ja kokemus taidoissa, joita he tarvitsevat suorittaakseen tehtävänsä

2. Käytössä on riittävästi henkilöstöä ja alihankkijoita, jotta palvelua voidaan toteuttaa ja resursoida asianmukaisesti sen toimintaperiaatteiden ja menettelyjen mukaisesti.

3. Palvelun tarjoamiseen käytetyt tilat ovat jatkuvasti seurattuja ja suojattuja ympäristötapahtumien aiheuttamilta vahingoilta, luvattomalta käytöltä ja muilta tekijöiltä, jotka voivat vaikuttaa palvelun turvallisuuteen.

4. Palvelun tarjoamiseen käytetyissä tiloissa varmistetaan, että pääsy alueille, joilla säilytetään tai käsitellään henkilötietoja, salattuja tietoja tai muita arkaluonteisia tietoja, rajoitetaan koskemaan valtuutettuja henkilöstön jäseniä tai alihankkijoita.

EU:n varmuustasoasetus Liite, 2.4.6 Tekniset tarkastukset

MATALA/KOROTETTU

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

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

3. Pääsy arkaluonteiseen salaustekniseen aineistoon, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, rajoitetaan tiukasti niihin tehtäviin ja sovelluksiin, jotka edellyttävät tällaista pääsyä. On varmistettava, ettei tällaista aineistoa koskaan tallenneta pysyväisluonteisesti ilmitekstinä.

4. Käytössä on menettelyt, joilla varmistetaan, että turvallisuus säilyy ja että kyetään vastaamaan muutoksiin riskitasoissa, poikkeamiin ja tietoturvaloukkauksiin.

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

M72 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet

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

1) tietoliikenneturvallisuus
   a) verkon rakenteellinen turvallisuus
   b) tietoliikenneverkon vyöhykkeistäminen
   c) suodatussäännöt vähimpien oikeuksien periaatteilla
   d) suodatuksen ja valvontajärjestelmien hallinnointi koko elinkaaren ajan
   e) hallintayhteydet

2) tietojärjestelmäturvallisuus
   a) pääsyoikeuksien hallinta
   b) järjestelmien käyttäjien tunnistaminen
   c) järjestelmien koventaminen
   d) haittaohjelmasuojaus
   e) turvallisuuteen liittyvien tapahtumien jäljitys
   f) poikkeamien havainnointikyky ja toipuminen
   g) kansainvälisesti tai kansallisesti suositellut salausratkaisut muutoin kuin 7 §:ssä säädetyltä osin

3) käyttöturvallisuus
   a) muutosten hallinta
   b) salassa pidettävän aineiston käsittely-ympäristö
   c) etäkäyttö ja -hallinta
   d) ohjelmistohaavoittuvuuksien hallinta
   e) varmuuskopiointi

Tuotantoverkko ja sen edellä 1 momentin 1) e) ja 3) c) alakohdissa tarkoitetut hallintayhteydet ja etäkäyttö- ja etähallinta on toteutettava siten, että organisaation muiden palveluiden kuten sähköpostin tai web-selailun kautta aiheutuvat tietoturvauhat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvauhat on

   a) korotetulla varmuustasolla erityisesti arvioitu ja minimoitu ja
   b) korkealla varmuustasolla kokonaisuutena arvioiden estetty.

M72 7 § Tunnistusjärjestelmän ja rajapintojen salausvaatimukset

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

*1) **Avaintenvaihto**: Avaintenvaihdossa on käytettävä DHE-menetelmiä tai elliptisiä käyriä käyttäviä ECDHE-menetelmiä. Laskutoimituksissa käytetyn äärellisen kunnan (finite field) koon tulee olla DHE-menetelmässä vähintään 2048 bittiä ja ECDHE-menetelmässä vähintään 224 bittiä.*

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

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

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

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

Mikäli yhteyskäytännössä käytetään TLS-protokollaa, tulee käyttää vähintään TLS versiota 1.2 tai uudempaa versiota. TLS versiota 1.1 voi käyttää ainoastaan, jos käyttäjän päätelaite ei tue uudempia versioita.

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

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

3.5 Käyttäjän sopimusehdot ja vastuut

3.5.1 Yleistä

Lain 20 §:ssä todetaan, että tunnistusvälineen liikkeelle laskeminen perustuu tunnistusvälineen hakijan ja tunnistuspalvelun tarjoajan väliseen sopimukseen. Sopimus on tehtävä kirjallisesti. Sopimus voidaan tehdä myös sähköisesti, jos sen sisältöä ei voida yksipuolisesti muuttaa ja se säilyy osapuolten saatavilla.

Tunnistuslain 15 §:ssä säädetään tiedoista (sopimusehdoista), jotka tunnistuspalveluntarjoajan on annettava käyttäjälle ennen sopimuksen tekemistä.

Lain 23 §:ssä säädetään käyttäjän velvollisuudesta säilyttää tunnistusväline huolellisesti ja lain 21–27 §:ssä säädetään muutoinkin tunnistusvälineen tarjoajan ja tunnistusvälineen haltijan oikeuksista, velvollisuuksista ja vastuista.

Liikenne- ja viestintävirasto valvoo tunnistuslain 15 §:n vaatimusta, että vahvan sähköisen tunnistuspalvelun tarjoaja antaa tunnistusvälineen hakijalle (käyttäjälle) säädetyt tiedot ennen sopimuksen tekemistä. Sopimusehtojen selkeyden ja kohtuullisuuden arviointi on yleisen kuluttajansuojasääntelyn alaan kuuluva asia.

Tarjonnan kysymykset voivat tulla arvioitavaksi myös yleisen kuluttajansuojalainsäädännön tai yleisen kilpailulainsäädännön kannalta. Nämä tehtävät kuuluvat Kilpailu- ja kuluttajavirastolle tai siellä toimivalle kuluttaja-asiamiehelle.

3.5.2 Linjaukset

Samaa tunnistusmenetelmää ei voi käyttäjän oikeuksien näkökulmasta tarjota sekä vahvana että rekisteröimättömänä sillä perusteella, että toteuttaisi tunnistuslakia vastaavat oikeudet sopimusehdoilla.

Vahvan sähköisen tunnistamisen luotettavuus perustuu osaltaan viranomaisvalvontaan. Tunnistuslain pakottavat säännökset käyttäjän oikeuksista eivät koske rekisteröimätöntä tunnistuspalvelua eikä Liikenne- ja viestintävirastolla ei ole toimivaltaa valvoa rekisteröimättömän sähköisen tunnistuksen toteutusta tai sopimusehtoja. Tunnistuslakia vastaavien oikeuksien toteuttaminen sopimusehdoilla ei riitä korvaamaan käyttäjän ja asiointipalvelun tunnistuslaissa säädettyä lakisääteistä suojaa, joka ei koske rekisteröimätöntä tunnistusmenetelmää.

Liikenne- ja viestintävirasto *ei* katso, että heikolle ja vahvalle tunnistusmenetelmälle olisi TunnL:n nojalla välttämättä oltava kokonaan erilliset sopimukset ja sopimusehdot.

Joka tapauksessa sopimusehdoista on ilmettävä selkeästi vahvan tunnistuksen ehdot lain 15 §:n mukaisesti, eivätkä rekisteröimättömän tunnistuksen ehdot saa sekoittua niihin.

Jos tunnistusvälineen tarjoaja laatii sopimusehdot, jotka koskevat sekä rekisteröimätöntä että vahvaa tunnistusta, edellyttää tunnistusvälineen tarjoajan tiedonantovelvollisuuden täyttäminen erityistä huolellisuutta:

- Palveluntarjoajan on tarkoin tuotava esiin TunnL 15 §:ssä lueteltuihin ja muihin mahdollisiin olennaisiin seikkoihin liittyvät erot rekisteröimättömän ja vahvan tunnistuksen palveluissa ja niihin sovellettavissa ehdoissa. Viraston toimivaltaan kuulua valvoa sitä, että TunnL 15 §:n mukaiset tiedot esitetään tunnistuslain tarkoittamalla tavalla käyttäjälle vahvan sähkön tunnistusvälineen osalta.

- Korostettu tiedonantovelvollisuus seuraa siitä, että käyttäjän tulee esimerkiksi käsittää vahvan tunnistusmenetelmän erot muuhun samassa sopimuksessa käsiteltyyn tunnistukseen nähden (tiedonantovelvollisuus tarjottavista palveluista, palvelun ja palveluntarjoajan kuulumisesta julkisen valvonnan piiriin vain vahvan tunnistuksen osalta) sekä erot käyttäjän oikeusasemassa sen mukaan, kumpaa tunnistusvälinettä tämä käyttää (tiedot osapuolten oikeuksista ja velvollisuuksista). Yksi ero oikeusasemassa syntyy esimerkiksi väistämättä siitä, että käyttäjän vastuuta oikeudettomasta käytöstä säännellään tunnistuslain nojalla vain vahvan sähköisen tunnistuksen osalta[1].

- Kuluttajille tarjottujen ehtojen tulee lisäksi olla kuluttajansuojalain nojalla selkeät ja ymmärrettävät; tätä valvoo kuluttaja-asiamies. Liikenne- ja viestintävirasto ei ole toimivaltainen ottamaan kantaa myöskään tunnistuspalveluiden markkinointiin kuluttajansuojalain näkökulmasta.

Rekisteröimättömän ja vahvan tunnistusvälineen elinkaaren hallinta on selvästi eriytettävä, jos niissä käytetään erilaisia menettelyjä.

Esimerkiksi vahvaa tunnistusvälinettä tai sen todentamistekijää ei voi uusia muutoin kuin lain vaatimalla varmuustasolla, eivätkä rekisteröimättömän tunnistusmenetelmän mahdollisesti kevyemmät uusimismenettelyt saa heikentää vahvaa tunnistusmenetelmää. Yhtäaikainen vahvan ja rekisteröimättömän välineen myöntäminen on mahdollista, jos se tehdään vahvan välineen avaamisen edellyttämällä tavalla. Samoin samanaikainen sulkeminen on mahdollista.

Liikenne- ja viestintävirasto katsoo, että käyttäjän on tiedettävä aina, mitä tunnistusvälinettä hänen täytyy käyttää ja mitä hän on käyttämässä.

Käyttäjän on voitava luottaa siihen, että hänelle sopimuksella vahvana sähköisenä tunnistusvälineenä tarjotun tunnistusvälineen käytössä noudatetaan aina kaikilta osin lainsäädännön velvoitteita.

3.5.3 Säännökset

TunnL 3 § Pakottavuus

[1] Näitä eroja ei voine täysin poistaa sopimusperusteisesti, sillä esimerkiksi käyttäjän vastuuta oikeudettomasta käytöstä suhteessa kolmansiin ei voida pätevästi rajoittaa käyttäjän ja tunnistuspalvelun tarjoajan välisin sopimuksin.

Sopimusehto, joka poikkeaa tämän lain säännöksistä kuluttajan vahingoksi, on mitätön, jollei jäljempänä toisin säädetä.

[…]

TunnL 15 § Tunnistusvälineen tarjoajan tiedonantovelvollisuus ennen sopimuksen tekemistä (29.6.2016/533)

Tunnistusvälineen tarjoajan on ennen tunnistusvälineen hakijan kanssa tehtävän sopimuksen tekemistä annettava hakijalle tiedot: (29.6.2016/533)
1) palveluntarjoajasta;
2) tarjottavista palveluista ja hinnoista;
3) 14 §:ssä tarkoitetuista tunnistusperiaatteista;
4) osapuolten oikeuksista ja velvollisuuksista;
5) mahdollisista vastuunrajoituksista;
6) valitus- ja riitojenratkaisumenettelyistä;
7) mahdollisista 18 §:ssä tarkoitetuista estoista ja käyttörajoituksista; sekä
8) muista mahdollisista tunnistusvälineen käyttöehdoista.

Edellä 1 momentissa tarkoitetut tiedot on annettava kirjallisesti tai sähköisesti siten, että tunnistusvälineen hakija voi tallentaa ja toisintaa ne muuttumattomina. Jos sopimus tehdään tunnistusvälineen hakijan pyynnöstä sellaista etäviestintä käyttäen, että tietoja ja sopimusehtoja ei voida antaa edellä tarkoitetulla tavalla ennen sopimuksen tekemistä, tiedot on annettava sanotulla tavalla viipymättä sopimuksen tekemisen jälkeen.

Henkilötietojen käsittelyä koskevasta tiedonantovelvollisuudesta säädetään henkilötietolaissa.

TunnL 20 § Tunnistusvälineen myöntäminen (29.6.2016/533)

Tunnistusvälineen liikkeelle laskeminen perustuu tunnistusvälineen hakijan ja tunnistuspalvelun tarjoajan väliseen sopimukseen. Sopimus on tehtävä kirjallisesti. Sopimus voidaan tehdä myös sähköisesti, jos sen sisältöä ei voida yksipuolisesti muuttaa ja se säilyy osapuolten saatavilla. Tunnistuspalvelun tarjoajan tulee kohdella asiakkaitaan syrjimättä ja tunnistusvälineiden hakijoita tasapuolisesti sopimuksen tekemisen yhteydessä.

Sopimus voi olla voimassa toistaiseksi tai määräaikaisesti. Tunnistusvälineellä voi olla oma voimassaoloaikansa, joka on lyhyempi kuin sopimuksen voimassaoloaika.

Tunnistusväline myönnetään aina luonnolliselle henkilölle tai oikeushenkilölle. Luonnollisen henkilön ja oikeushenkilön tunnistusvälineiden kytkös on toteutettava sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdan 2.1.4 mukaisesti. Tunnistusvälineen on oltava henkilökohtainen. Tunnistusvälineeseen voidaan tarvittaessa liittää tieto siitä, että tunnistusvälineen haltija voi tapauskohtaisesti myös edustaa toista luonnollista henkilöä tai oikeushenkilöä. (29.6.2016/533)

TunnL 21 § (29.6.2016/533) Tunnistusvälineen luovuttaminen hakijalle

Tunnistusvälineen tarjoajan on luovutettava tunnistusväline sen hakijalle siten kuin sopimuksessa on sovittu. Tunnistuspalvelun tarjoajan on varmistettava, ettei tunnistusväline joudu oikeudettomasti toisen haltuun välinettä luovutettaessa siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.2.2 vähintään korotetulle varmuustasolle säädetyt vaatimukset täyttyvät.

EU:n varmuustasoasetus 2.2.2 Myöntäminen, toimittaminen ja aktivointi

KOROTETTU

Sähköisen tunnistamisen menetelmän myöntämisen jälkeen se toimitetaan käyttäen mekanismia, jonka kautta se voidaan olettaa toimitettavan vain sen henkilön haltuun, jolle se kuuluu.

TunnL 22 § (29.6.2016/533) Tunnistusvälineen uusiminen

Tunnistusvälineen tarjoaja saa toimittaa tunnistusvälineen haltijalle uuden välineen ilman nimenomaista pyyntöä vain, jos aikaisemmin annettu tunnistusväline on korvattava uudella. Tunnistusvälineen uusimisessa tulee noudattaa sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.2.4 vähintään korotetulle varmuustasolle säädettyjä vaatimuksia.

EU:n varmuustasoasetus 2.2.4 Uusiminen ja korvaaminen

MATALA/KOROTETTU

Ottaen huomioon riskit henkilön tunnistetiedoissa tapahtuvista muutoksista uusimisen tai korvaamisen on täytettävä samat varmuusvaatimukset kuin henkilöllisyyden alkuperäisen todistamisen ja varmentamisen yhteydessä tai sen on perustuttava saman tai korkeamman varmuustason voimassa olevaan sähköisen tunnistamisen menetelmään.

TunnL 25 § Tunnistusvälineen peruuttamista tai käytön estämistä koskeva ilmoitus

Tunnistusvälineen haltijan on ilmoitettava tunnistusvälineen tarjoajalle tai tämän nimeämälle muulle taholle tunnistusvälineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä ilman aiheetonta viivytystä havaittuaan asian. (29.6.2016/533)

Tunnistusvälineen tarjoajan on tarjottava mahdollisuus tehdä 1 momentissa tarkoitettu ilmoitus milloin tahansa. Tunnistusvälineen tarjoajan on viipymättä peruutettava tunnistusväline tai estettävä sen käyttö saatuaan asiaa koskevan ilmoituksen. (29.6.2016/533)

Tunnistusvälineen tarjoajan on asianmukaisesti ja viipymättä merkittävä järjestelmään tieto peruuttamisen tai käytön estämisen ajankohdasta. Tunnistusvälineen haltijalla on oikeus saada pyynnöstä todistus siitä, että hän on tehnyt 1 momentissa tarkoitetun ilmoituksen. Todistusta on pyydettävä 18 kuukauden kuluessa ilmoituksesta. (29.6.2016/533)

Järjestelmän on oltava sellainen, että tunnistuspalvelua käyttävä palveluntarjoaja voi helposti tarkastaa siihen merkityt tiedot ympäri vuorokauden. Velvollisuutta järjestää tarkastusmahdollisuutta ei kuitenkaan ole, jos tunnistusvälineen käyttö voidaan teknisesti estää tai se voidaan sulkea.

Tunnistuspalvelua käyttävän palveluntarjoajan on tarkastettava tunnistuspalvelun tarjoajan ylläpitämistä järjestelmistä ja rekistereistä mahdolliset peruutukset ja käytön estot tunnistusvälineen käytön yhteydessä. Tarkastaminen ei kuitenkaan ole tarpeen, jos tunnistusvälineen käyttö voidaan teknisesti estää tai se voidaan sulkea.

Jos tunnistuspalvelu perustuu varmenteisiin ja peruutettuja varmenteita koskevat tiedot annetaan sulkulistan avulla, varmennepalvelun tarjoaja saa tallentaa tiedot sulkulistalta tehdystä varmenteen voimassaolon tarkastamisesta. Vaihtoehtoisesti varmentaja voi tallentaa sulkulistan.

TunnL 26 § (29.6.2016/533) Tunnistusvälineen tarjoajan oikeus peruuttaa tai estää tunnistusvälineen käyttö

Sen lisäksi, mitä 25 §:ssä säädetään, tunnistusvälineen tarjoaja voi peruuttaa tunnistusvälineen tai estää sen käytön, jos:

1) tunnistusvälineen tarjoajalla on syytä epäillä, että joku muu kuin se, jolle tunnistusväline on myönnetty, käyttää sitä;

2) tunnistusväline sisältää ilmeisen virheellisyyden;

3) tunnistusvälineen tarjoajalla on syytä epäillä, että tunnistusvälineen käytön turvallisuus on vaarantunut;

4) tunnistusvälineen haltija käyttää tunnistusvälinettä olennaisesti sopimusehtojen vastaisella tavalla;

5) tunnistusvälineen haltija on kuollut.

Tunnistusvälineen tarjoajan tulee ilmoittaa haltijalle niin pian kuin mahdollista tunnistusvälineen peruuttamisesta tai käytön estämisestä ja sen ajankohdasta sekä siihen johtaneista syistä.

Tunnistusvälineen tarjoajan on palautettava mahdollisuus käyttää tunnistusvälinettä tai annettava haltijalle uusi väline välittömästi 1 momentin 2 ja 3 kohdassa tarkoitetun syyn poistuttua.

TunnL 27 § Tunnistusvälineen haltijan tunnistusvälineen oikeudetonta käyttöä koskevat vastuunrajoitukset

Tunnistusvälineen haltija vastaa tunnistusvälineen oikeudettomasta käytöstä vain, jos:

1) hän on luovuttanut tunnistusvälineen toiselle;

2) tunnistusvälineen katoaminen, joutuminen oikeudettomasti toisen haltuun tai oikeudeton käyttö johtuu hänen huolimattomuudestaan, joka ei ole lievää; tai

3) hän on laiminlyönyt ilmoittaa tunnistuspalvelun tarjoajalle tai sen ilmoittamalle muulle taholle tunnistusvälineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä ilman aiheetonta viivytystä sen havaittuaan.

Tunnistusvälineen haltija ei kuitenkaan vastaa tunnistusvälineen oikeudettomasta käytöstä:

1) siltä osin kuin tunnistusvälinettä on käytetty sen jälkeen, kun hän on ilmoittanut tunnistuspalvelun tarjoajalle tunnistusvälineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä;

2) jos tunnistusvälineen haltija ei ole voinut tehdä ilmoitusta välineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä ilman aiheetonta viivytystä sen havaittuaan sen johdosta, että tunnistuspalvelun tarjoaja on laiminlyönyt 25 §:n 2 momentissa tarkoitetun velvollisuutensa huolehtia siitä, että tunnistusvälineen haltijalla on milloin tahansa mahdollisuus tehdä kyseinen ilmoitus; tai

3) tunnistuspalvelua käyttävä palveluntarjoaja on laiminlyönyt 18 §:n 4 momentin tai 25 §:n 5 momentin mukaisen velvollisuutensa tarkastaa tunnistusvälineeseen liittyvän käyttörajoituksen olemassaolon tai tiedon välineen käytön estämisestä tai sulkemisesta.

3.6 Henkilötietojen, tunnistustapahtumien ja lokien käsittely

3.6.1 Yleistä

Tunnistuslain 6 §:ssä ja 7 §:ssä säädetään henkilötietojen käsittelystä vahvassa sähköisessä tunnistamisessa. HE 237/2020:ssä 6 §:ää ehdotetaan muutettavaksi. Tietojen luotetuksi lähteeksi on säädetty väestötietojärjestelmä.

Pääosin henkilötietojen käsittelystä säädetään EU:n yleisessä tietosuoja-asetuksessa ja henkilötunnuksen käytöstä tietosuojalain 29 §:ssä.

Henkilötietojen käsittelyä tunnistuslain, yleisen tietosuoja-asetuksen ja tietosuojalain nojalla valvoo tietosuojavaltuutettu.

Tunnistuslain 24 §:ssä säädetään tunnistustapahtumatietojen tallentamisesta ja tietojen käyttämisen sallituista perusteista. Pykälässä säädetään myös käsittelylokien ylläpitovelvollisuus.

Viraston määräyksessä 72 määrätään 12 §:ssä ne pakolliset henkilötiedot (*pakolliset attribuutit*), jotka tunnistuspalvelun on kyettävä tuottamaan luottamusverkostossa ja ne valinnaiset henkilötiedot (*optionaaliset attribuutit*), joiden tuottamiseen tulee olla suunniteltu valmius. Määräyksen tarkoitus on turvata tunnistamisen yh-

teentoimivuus. Tiedot vastaavat täysin eIDAS-sääntelyä (komission täytäntöönpanoasetus (EU) 1501/2015) ja sääntelyn tarkoitus on turvata tarvittaessa myös rajat ylittävä yhteentoimivuus.

On syytä huomata, että vahvan sähköisen tunnistuksen sääntely ei edellytä, että pakolliset tai valinnaiset attribuutit toimitetaan tai vahvistetaan luottavalle osapuolelle. Vahva sähköinen tunnistuspalvelu voidaan tuotteistaa myös siten, että luottavalle osapuolelle toimitetaan vain pseudonyymi tai vaikkapa vain tieto tunnistautujan täysi-ikäisyydestä.

3.6.2 Linjaukset

Liikenne- ja viestintävirasto katsoo, että vahvan tunnistuksen sääntely on tietosuoja-asetuksen mukainen käsittelyperuste niille henkilötiedoille, joista säädetään tunnistuslain 12 b §:n 2 alakohdassa ja tunnistuslain nojalla annetussa viraston määräyksessä. Yksilöivien ja henkilöä kuvaavien tietojen lisäksi tunnistuslain sääntely koskee tunnistustapahtumien tallennusta ja tietoturvallisuusvelvoitteet edellyttävät erilaisten teknisten lokien ylläpitoa.

Tunnistuslaki ei koske rekisteröimätöntä tunnistusta eikä anna käsittelyperustetta henkilötietojen käsittelyyn rekisteröimättömässä tunnistuspalvelussa. Rekisterinpitäjän on siten perusteltava ja arvioitava henkilötietojen käsittelyperusteet, luovuttaminen asiointipalvelulle ja tapahtumalokien ylläpito rekisteröimättömässä tunnistamisessa erikseen tietosuoja-asetuksen ja tietosuojalain mukaisesti. On hyvä huomata, että henkilötiedon käsittelyperuste vaikuttaa myös rekisteröidyn oikeuksiin. Myös tapahtumalokien ylläpito on arvioitava rekisteröimättömässä tunnistamisessa muulla perusteella kuin tunnistuslain 24 §:n perusteella.

Samoin, jos vahvan tunnistuksen yhteydessä tarjotaan muita kuin tunnistussäänte-lyssä tarkoitettuja henkilötietoja (nk. rikastetut tiedot), niiden käsittelyn peruste täytyy arvioida erikseen tietosuoja-asetuksen perusteella.

3.6.3 Säännökset

Tunnistuslain 6 § on esitetty muutettavaksi (HE 237/2020). Henkilötunnuksen käsittelyvelvoite esitetään edelleen säädettäväksi. Lain muutoksella ei ole tarkoitus muuttaa oikeustilaa, vaan lain 533/2016 mukaisten velvoitteiden arvioidaan seuraavan jo yleisestä tietosuoja-asetuksesta ja tietosuojalaista.

Esitetty TunnL 6 § Henkilötunnuksen käsittely

Tunnistuspalvelun tarjoajan ja luottamuspalveluja tarjoavan varmentajan tulee tarkastaessaan hakijan henkilöllisyyden vaatia hakijaa ilmoittamaan henkilötunnuksensa.

Ks. myös Tietosuojalaki 1050/2018 ja (EU) 2016/679 (yleinen tietosuoja-asetus).

TunnL 7 § (20.2.2015/139) Väestötietojärjestelmän tietojen käyttäminen

Tunnistusvälineen tarjoajan ja luottamuspalvelua tarjoavan varmentajan on hankittava ja päivitettävä luonnollisen henkilön tunnistuspalvelun tarjoamiseksi tarvitsemansa tiedot väestötietojärjestelmästä. Tämän lisäksi tunnistuspalvelun tarjoajan on varmistettava, että sen tunnistuspalvelun tarjoamiseksi tarvitsemat tiedot ovat ajan tasalla väestötietojärjestelmän tietojen kanssa. (29.6.2016/533)

[…]

TunnL 8 § (29.6.2016/533) Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset

[…]

Mitä 1 momentissa säädetään, ei estä palvelun tarjoamista palvelukohtaisesti siten, että tunnistuspalvelun tarjoaja ilmoittaa tunnistuspalvelua käytävälle palveluntarjoajalle tunnistusvälineen haltijan salanimen tai ainoastaan rajoitetun määrän henkilötietoja.

TunnL 24 § (29.6.2016/533) Tunnistustapahtumaa ja tunnistusvälinettä koskevien tietojen tallentaminen ja käyttö

Tunnistuspalvelun tarjoajan on tallennettava:

1) yksittäisen tunnistustapahtuman ja sähköisen allekirjoittamisen tapahtuman todentamiseksi tarvittavat tiedot;

2) tiedot 18 §:ssä tarkoitetuista tunnistusvälineen käyttöön liittyvistä estoista ja käyttörajoituksista;

3) varmenteen osalta 19 §:ssä tarkoitetun varmenteen tietosisältö.

Tunnistusvälineen tarjoajan on tallennettava tarvittavat tiedot 17 ja 17 a §:ssä tarkoitetusta hakijan ensitunnistamisesta ja siinä käytetystä asiakirjasta tai sähköisestä tunnistamisesta.

Edellä 1 momentin 1 kohdassa tarkoitetut tiedot on säilytettävä viiden vuoden ajan tunnistustapahtumasta. Muut 1 ja 2 momentissa tarkoitetut tiedot on säilytettävä viiden vuoden ajan vakituisen asiakassuhteen päättymisestä.

Tunnistustapahtuman yhteydessä syntyneet henkilötiedot on hävitettävä tunnistustapahtuman jälkeen, jollei tallentaminen ole välttämätöntä yksittäisen tunnistustapahtuman todentamiseksi.

Tunnistuspalvelun tarjoaja saa käsitellä tallennettuja tietoja ainoastaan palvelun toteuttamiseksi ja ylläpitämiseksi, laskutusta varten, omien oikeuksiensa turvaamista varten riitatilanteissa, väärinkäytöstilanteiden selvittämisessä sekä tunnistuspalvelua käyttävän palveluntarjoajan tai tunnistusvälineen haltijan pyynnöstä. Tunnistuspalvelun tarjoajan on tallennettava tieto käsittelyn ajankohdasta, syystä ja käsittelijästä.

Jos palveluntarjoaja ainoastaan laskee liikkeelle tunnistusvälineitä:

1) 1 momentin 1 kohtaa ja 4 momenttia ei sovelleta siihen;

2) 3 momentissa tarkoitettu viiden vuoden tallennusaika lasketaan tunnistusvälineen voimassaolon päättymisestä.

M72 12 § Luottamusverkostossa välitettävät vähimmäistiedot

Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on välitettävä:

1) luonnollista henkilöä koskevassa tunnistustapahtumassa ainakin henkilön yksilöivä tunniste, henkilön etunimi, henkilön sukunimi ja henkilön syntymäaika;

2) oikeushenkilöä koskevassa tunnistustapahtumassa ainakin oikeushenkilöä edustavan luonnollisen henkilön yksilöivä tunniste, henkilön sukunimi, henkilön etunimi ja organisaation yksilöivä tunniste; sekä

3) tieto tunnistusvälineen korotetusta tai korkeasta varmuustasosta.

Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on oltava valmius välittää:

1) tieto siitä, koskeeko tunnistustapahtuma julkisen hallinnon asiointipalvelua vai yksityistä asiointipalvelua;

2) luonnollista henkilöä koskevassa tunnistustapahtumassa etunimi (-nimet) ja sukunimi (-nimet) syntymähetkellä, syntymäpaikka, nykyinen osoite ja sukupuoli;

3.7 Luottamusverkoston sopimusvelvoitteiden ja yhteistoiminnan sääntely

3.7.1 Yleistä

Tunnistuslain 12 a §:ssä säädetään vahvan sähköisen tunnistuksen tarjoajien luottamusverkostosta. Luottamusverkoston muodostavat tunnistuslain mukaisen ilmoituksen tehneet tunnistuspalvelut, jotka Liikenne- ja viestintävirasto on hyväksynyt rekisteriin. Luottamusverkosto-termiä käytetään paljon vahvan sähköisen tunnistamisen synonyyminä, mutta tarkasti ottaen luottamusverkosto tarkoittaa tunnistusvälineen tarjoajalle säädettyä velvollisuutta luovuttaa tunnistusvälityspalvelulle tunnistuspalvelun käyttöoikeus ja tähän liittyvien sopimusehtojen sääntelyä. Lisäksi tunnistuspalveluilla on yhteistyövelvollisuus teknisen yhteentoimivuuden turvaamiseksi.

Lain 16 §:ssä säädetään mm. palvelun toimivuuteen, tietoturvaan tai sähköisen henkilöllisyyden käyttöön kohdistuvista merkittävistä uhkista tai häiriöistä tiedottamiseen luottamusverkostossa toimiville sopimuspuolille.

Lain 12 a §:n 5 momentissa säädetään käyttöoikeuden luovutuksen tai 16 §:n nojalla saatujen toista tunnistuspalvelun tarjoajaa koskevien tietojen käsittelyrajoituksista ja säännöksen vastaisen käytön aiheuttaman vahingon korvausvastuusta.

3.7.2 Linjaukset

Tunnistuslain mukainen luottamusverkostosääntely eli tunnistuspalvelun käyttöoikeuden luovutus, sopimusehtojen sääntely, häiriötilanteiden hoitaminen ja näihin liittyvät erityiset salassapitovelvollisuudet koskevat vain vahvaa sähköistä tunnistamista.

Rekisteröimättömän sähköisen tunnistuksen välittäminen ei kuulu luottamusverkoston käyttöoikeussääntelyn piiriin, mutta tunnistuslaki ei estä sen välittämistä muulla perusteella.

3.7.3 Säännökset

12 a § (29.3.2019/412) Tunnistuspalvelun tarjoajien luottamusverkosto

Tunnistuspalvelun tarjoaja liittyy osaksi luottamusverkostoa tehdessään 10 §:n mukaisen ilmoituksen Liikenne- ja viestintävirastolle.

Tunnistusvälineen tarjoajan on tarjottava tunnistuspalvelunsa käyttöoikeutta tunnistusvälityspalvelun tarjoajille siten, että ne voivat välittää tunnistustapahtumia sähköiseen tunnistukseen luottavalle osapuolelle. Tunnistusvälineen tarjoajan on laadittava tunnistuspalvelunsa käyttöoikeuden toimitusehdot ja käytettävä niitä tehdessään sopimuksia tunnistusvälityspalveluiden tarjoajien kanssa. Käyttöoikeuden ehtojen on oltava tämän lain mukaisia sekä kohtuullisia ja syrjimättömiä. Tunnistusvälineen tarjoajan on hyväksyttävä tunnistusvälityspalvelun tarjoajan pyyntö toimitusehtojen mukaisen sopimuksen tekemisestä sekä annettava käyttöoikeus tunnistuspalveluun viipymättä ja viimeistään kuukauden kuluessa pyynnön tekemisestä. Tunnistusvälineen tarjoaja voi kieltäytyä sopimuksen tekemisestä ainoastaan, jos tunnistusvälityspalvelun tarjoaja toimii vastoin tätä lakia tai sen nojalla annettuja säännöksiä tai määräyksiä taikka kieltäytymiselle on muu painava peruste.

Tunnistuspalvelun tarjoajien on tehtävä yhteistyötä sen varmistamiseksi, että luottamusverkoston jäsenten väliset tekniset rajapinnat ovat yhteen toimivia ja että ne mahdollistavat yleisesti tunnettujen standardien mukaisten rajapintojen tarjoamisen luottaville osapuolille.

Tunnistuspalvelun tarjoajan on toteutettava ylläpito-, muutos- ja tietoturvatoimenpiteet muille tunnistuspalvelun tarjoajille, käyttäjille ja luottaville osapuolille mahdollisimman vähän haittaa aiheuttavalla tavalla. Sen lisäksi, mitä 25 ja 26 §:ssä säädetään, tunnistuspalvelun tarjoaja saa tilapäisesti ilman toisen tunnistuspalvelun tarjoajan suostumusta keskeyttää

tunnistuspalvelun tarjonnan tai rajoittaa sen käyttöä, jos se on välttämätöntä edellä tarkoitetun toimenpiteen onnistumiseksi. Keskeytyksestä ja muutoksesta on tiedotettava tehokkaasti niille muille tunnistuspalvelun tarjoajille, joiden palveluihin se voi vaikuttaa.

Tunnistuspalvelun tarjoaja saa käyttää käyttöoikeuden luovutuksen tai 16 §:n nojalla saatuja toista tunnistuspalvelun tarjoajaa koskevia tietoja vain siihen tarkoitukseen, jota varten ne on tunnistuspalvelun tarjoajalle annettu. Tietoja saavat tunnistuspalvelun tarjoajan palveluksessa tai sen lukuun käsitellä ainoastaan ne, jotka tarvitsevat tietoja välttämättä työssään. Tietoja on muutoinkin käsiteltävä siten, ettei toisen tunnistuspalvelun tarjoajan liikesalaisuuksia vaaranneta. Tunnistuspalvelun tarjoaja, joka aiheuttaa tämän momentin vastaisella menettelyllä vahinkoa toiselle tunnistuspalvelun tarjoajalle, on velvollinen korvaamaan menettelystään aiheutuvan vahingon.

Luottamusverkoston hallinnollisista käytännöistä, teknisistä rajapinnoista ja hallinnollisista vastuista annetaan tarkempia säännöksiä valtioneuvoston asetuksella.

16 § (29.3.2019/412) Tunnistuspalvelun tarjoajan ilmoitukset toimintaan ja tietojen suojaamiseen kohdistuvista uhkista tai häiriöistä

Tunnistuspalvelun tarjoajan on salassapitosäännösten estämättä ilmoitettava ilman aiheetonta viivästystä tunnistuspalveluunsa luottaville osapuolille, tunnistusvälineiden haltijoille, muille luottamusverkostossa toimiville sopimuspuolilleen sekä Liikenne- ja viestintävirastolle palvelun toimivuuteen, tietoturvaan tai sähköisen henkilöllisyyden käyttöön kohdistuvista merkittävistä uhkista tai häiriöistä. Ilmoituksessa on kerrottava niistä toimista, joita eri tahoilla on käytettävissään uhkien tai häiriöiden torjumiseksi sekä näistä toimenpiteistä aiheutuvista arvioiduista kustannuksista.

Tunnistuspalvelun tarjoaja voi salassapitosäännösten estämättä ilmoittaa kaikille luottamusverkoston jäsenille 1 momentissa tarkoitetuista uhkista ja häiriöistä sekä palvelun tarjoajista, joiden on syytä epäillä tavoittelevan oikeudetonta taloudellista hyötyä, antavan merkityksellisiä totuudenvastaisia tai harhaanjohtavia tietoja tai käsittelevän henkilötietoja lainvastaisesti.

Liikenne- ja viestintävirasto voi teknisesti välittää tietoja luottamusverkostossa osapuolten välillä ilmoittajan lukuun sen estämättä, mitä viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) säädetään.

Liite: Muistioluonnoksen 27.3.2020 lausuntoyhteenveto

Lausunnon antoivat Avaintec Oy, Danske Bank A/S, Suomen sivuliike, Digi- ja väestötietovirasto, Elisa Oyj, FiCom ry, Finanssiala ry, Kilpailu- ja kuluttajavirasto, Nets Denmark A/S, Branch Norway, OP Osuuskunta ja S-Pankki Oy.

Useissa lausunnoissa (KKV, Nets, Elisa, FiCom, DVV) kannatettiin muistion lähtökohtia ja tarkentamista, vahvan tunnistamisen vaatimusten turvaamista, vahvan ja rekisteröimättömän tunnistamisen riittävää eriyttämistä ja selkeyttä käyttäjän asemasta. Muistiota ja linjauksia pidettiin perusteltuina.

Danske ja S-Pankki esittivät täsmennyspyyntöjä.

Seuraavassa käsitellään lausuntoja aiheittain

Markkinoiden ja kehityksen edistäminen

KKV totesi, että saman tunnistusjärjestelmän käyttö sekä vahvan että heikon tunnistusvälineen tuottamiseen voi helpottaa tuloa sähköisen tunnistuksen markkinoille, mikä puolestaan on omiaan edistämään kilpailua ja markkinoiden toimivuutta.

Elisan ja pankkien sekä Finanssialan lausunnoissa esitettiin vastakkaiset näkemykset siitä, luoko tulkintamuistiossa annettu neuvonta edellytyksiä tunnistuspalveluiden kehittämiselle vai voiko se estää teknisen kehityksen hyödyntämistä.

Elisa katsoi, että Traficomin nyt ehdottama linjaus mahdollistaa kotimaisten vaihtoehtojen kilpailun pisimmälle edenneiden toimijoiden Googlen, Facebookin ja Applen kanssa.

Vaatimusten ennakoitavuutta pidettiin hyvänä palvelujen käynnissä olevalle kehittämiselle, mutta toisaalta kiinnitettiin huomiota siihen, että kankea ja yksityiskohtainen määrittely ei ole tarkoituksenmukaista ja esimerkiksi biometristen todentamistekijän tuomia kehitysmahdollisuuksia ei vielä osata ennakoida.

- Virasto pitää molempia näkökulmia oikeina ja perusteltuina. Viranomaisohjauksessa on löydettävä hyvä tasapaino vaatimusten ennakoitavuuden ja teknisen kehityksen joustavuuden välillä. Siksi nyt käsillä oleva neuvonta annetaan tulkintamuistion muodossa eikä esimerkiksi määräyksellä.

- **Muistioon on lisätty selvennys oikeudellisesta luonteesta suhteessa säännöksiin ja eräitä linjauksia on muutettu yleispiirteisemmäksi.**

Käyttäjien oikeudet

KKV ja pankkisektori esittivät jokseenkin vastakkaiset näkemykset siitä, onko merkityksellistä selkeyttää käyttäjille, milloin nämä käyttävät vahvaa tunnistusta ja milloin rekisteröimätöntä tunnistusta.

KKV piti tärkeänä, että huolehditaan muistioluonnoksessa kuvatulla tavalla välineiden riittävästä eriyttämisestä ja sopimusehtojen selkeydestä. Kuluttajille ei tunnistusvälinettä käytettäessä saa jäädä epäselväksi se, onko kyseessä heikko vai lailla säännelty vahva tunnistaminen. Kuten muistioluonnoksessa kuvataan, vahvan ja heikon tunnistusmenetelmän toteutuksessa on syytä huomioida tunnistustavan erottuminen käyttäjän havaittavissa olevista piirteistä ja käyttäjän oikeuksien toteutuminen. Erot heikon ja vahvan tunnistuksen palveluissa on voitava hahmottaa niihin sovellettavista ehdoista. Heikon ja vahvan tunnistuksen ehdot eivät muutoinkaan saa luoda epäselvyyttä sen suhteen, mihin kuluttajat sitoutuvat ehdot hyväksyessään.

Finanssiala ja OP puolestaan katsoivat, että tunnistusmenetelmän tasolla ja muistioluonnoksen mukaisella eriyttämisellä ei ole merkitystä käyttäjille. Käyttäjille on tärkeintä helppous ja käyttäjän luottamus perustuu palveluntarjoajaan eikä tunnistuspalvelun vahvaan statukseen. Tällä perusteella katsottiin, että vahvan ja rekisteröimättömän tunnistusmenetelmän

erottamisella ja tunnistamisen tasolla ei olisi käyttäjälle merkitystä. Tunnistuksen vahvuuden katsottiin olevan tunnistukseen luottavan osapuolen, ei käyttäjän intressissä.

- Virasto toteaa, että arviot keskimääräisen käyttäjän kiinnostuksesta tunnistuspalvelun statukseen voivat olla relevantteja, mutta tämä oikeastaan vain korostaa informointitarvetta tunnistuspalvelusta. Käyttäjän on voitava helposti havaita, mitä tunnistusta käyttää ja mitkä sen ehdot ovat.

OP:n ja Finanssiala katsoivat, että käyttäjän näkökulmasta on parempi käyttää vahvan sähköisen tunnistusvälineen myöntäjän prosesseja sekä teknologioita vähemmillä tunnistamisen elementeillä tai kontrolleilla kuin kehittää erilaisia ratkaisuja ja jakaa käyttäjille monia eri tunnuksia tai käyttää vain matalalla tasolla toimivia yleiskäyttöisiä tunnistusvälineitä. OP:n lausunnossa kiinnitettiin huomiota siihen, että eriyttäminen voi aiheuttaa epäselvyyttä esimerkiksi tunnistusvälineen sulkemisessa.

- Tulkintamuistion tarkoitus on selkeyttää sitä, millä reunaehdoilla samasta järjestelmästä voidaan tuottaa myös matalamman tason tunnistusmenetelmiä.

- **Sulkemista ja elinkaaren hallintaa koskevaa kohtaa on selvennetty**. Eriyttämisestä on huolehdittava, jos vahvassa ja rekisteröimättömässä tunnistuksessa käytetään eri menettelyjä.

Termi heikko tunnistus

Avaintecin lausunnossa kritisoitiin termin heikko tunnistus käyttämistä.

- Virasto on samaa mieltä siitä, että sanassa on tarpeeton arvolataus ja muistion määritelmässä onkin erityisesti tuotu esille, että kysymys on rekisteröitymisestä ja valvonnasta eikä tunnistuksen laadusta. Termin matala haasteena virasto pitää sitä, että se viittaa eIDAS-asetukseen alimpaan varmuustasoon, jonka toteuttamisesta ei niin ikään voi olla objektiivista tietoa.

- **Muistiossa on korvattu ilmaus heikko tunnistus ilmauksella rekisteröimätön tunnistusmenetelmä.**

PSD2

Pankkien edustajien lausunnoissa tuotiin esille, että pankkitunnistuksen tärkein sääntely perustuu PSD2:een ja että maksupalveluiden vahvan tunnistuksen vaatimukset tulevat komission teknisestä sääntelystandardista ja EBA:n ja Finanssivalvonnan tulkinnoista. Kysyttiin, onko muistioon tarkoituksenmukaista lisätä viittaukset ja mahdolliset uudet tulkinnat koskien maksupalvelulain ja tunnistuslain *vastuusäännösten suhdetta* liittyen rekisteröimättömään/heikkoon sähköiseen tunnistukseen. Liikenne- ja viestintäviraston ja Finanssivalvonnan tulkintayhteistyötä toivottiin.

Yhdessä lausunnossa katsottiin, että maksupalvelulaki tulee sovellettavaksi tunnistuslain sijaan, kun tunnistusvälineitä käytetään maksupalvelun käyttötarkoituksessa. Edelleen lausuttiin, että tahtotilana ei voi olla, että Suomessa ruvetaan kehittämään dedikoituja tunnistusvälineitä pelkästään PSD2:n mukaisten maksujen hyväksyntää varten.

- **Virasto on lisännyt muistioon maininnan PSD2-sääntelystä.**

- Teknisiä tai vastuusäännösten yhteensovittamiskysymyksiä ei valitettavasti pystytä käsittelemään tässä muistiossa tarkemmin, vaan se tehdään mahdollisuuksien mukaan muissa yhteyksissä. Lausunnoissa on nostettu esiin korttimaksamisen rajapinta ja vastuusäännökset. Muutoin lausunnoissa ei ole tuotu esille vaatimuksia, joiden yhteensovittamiseen linjaukset voisivat liittyä.

- Liikenne- ja viestintävirasto ja Finanssivalvonta ovat tarkastelleet teknisiä vaatimuksia vuonna 2018 siitä lähtökohdasta, että lainsäädäntöjä sovelletaan rinnakkain ja eroavuuksien kohdalla tulee täyttää kulloinkin tiukemman tai tarkemman sääntelyn vaatimukset. Virasto toteaa, että molempien sääntelyjen ja EU-tason tulkinnan kehittyessä

tulee uusia ratkaistavia yhteensovittamiskysymyksiä, jotka edellyttävät valvovien viranomaisten yhteistyötä.

- **Viraston ohjaus- ja valvontatoiminnan tavoitteena on, että samaa tunnistusmenetelmää voi käyttää sekä yleiskäyttöisenä että PSD2-alan tunnistusvälineenä.**

Todentamistekijät ja salaisuudet

Muistioluonnoksen yksityiskohtaisista linjauksista pidettiin epätarkoituksenmukaisena sitä, että vahvassa ja heikossa tunnistusmenetelmässä tulisi käyttää eri salasanaa. Tätä perusteltiin palveluntarjoamisessa saadulla kokemuksella siitä, että vaatimus eri salasanojen muistamisesta aiheuttaa haittoja, jotka ylittävät eriyttämisen mahdolliset hyödyt. Vertailukohtana viitattiin siihen, että maksukorteissa käytetään ongelmitta samaa salasanaa debit- ja credit-käytössä.

- **Virasto on muuttanut lausuntojen perusteella linjausta todentamistekijöiden eriyttämisestä tulkintamuistiossa.**

- **Virasto on lisäksi arvioinut kryptografisten salaisuuksien eriyttämistä ja lieventänyt luonnoksessa esittämäänsä tulkintaa.**

Ensitunnistaminen

Muistion varsinaisen aiheen lisäksi lausunnoissa korostettiin etäensitunnistamisen vaatimusten määrittelyn tarvetta.

- Etäensitunnistamisen arviointivaatimusten tarkentaminen on tästä tulkintamuistiosa erillinen tehtävä.

- Tulkintamuistiossa on kuitenkin esitetty linjauksia siitä, mitä on huomioitava korotettaessa rekisteröimätön tunnistusmenetelmä vahvaksi.

Muuta

Lausunnoissa esitettiin tekstiin yksittäisiä tarkennustoivomuksia ja -ehdotuksia.

- **Virasto on tarkentanut muistion sanamuotoja.**

Lausunnoissa toivottiin virastolta toimia käyttäjien ymmärryksen lisäämiseksi mm. tunnistamisen ja sähköisen allekirjoituksen eroista sekä muidenkin sähköisten palveluiden kuin vahvan sähköisen tunnistuksen sähköisten esilletuomista ja edistämistä.

- **Virasto kiittää näiden asioiden esille nostamisesta ja huomioi nämä asiat mahdollisuuksiensa ja toimivaltansa mukaan muissa yhteyksissä**