30.10.2014

Dnro:
1194/04/2014

kirjaamo@lvm.fi
markus.rahkola@vm.fi
olli-pekka.rissanen@vm.fi

Lausuntopyyntönne, asia LVM/1518/03/2014

Viestintäviraston lausunto vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain muutosehdotuksesta ja valtioneuvoston asetusluonnoksesta

Liikenne- ja viestintäministeriö on pyytänyt Viestintävirastolta lausuntoa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain muutosehdotuksesta (jatkossa "tunnistuslaki"). Lain nojalla on tarkoitus antaa myös valtioneuvoston asetus (jatkossa "asetus"), jonka luonnoksesta on myös pyydetty lausuntoa.

Keskeiset huomiot ehdotuksista

Viestintävirasto pitää tärkeänä ehdotettujen säädösmuutosten tavoitteen - toimivan kansallisen sähköisen tunnistamisratkaisun - toteuttamista. On myös tarkoituksenmukaista jo tässä vaiheessa ryhtyä viemään sähköisen tunnistamisen toimintaympäristöä sellaiseen suuntaan, että ns. eIDAS -asetuksessa[1] edellytetty sähköisen tunnistamisen menetelmien rajat ylittävä vastavuoroinen tunnustaminen olisi mahdollista toteuttaa asetuksen aikataulua noudattaen.

Tunnistuslailla on suuri merkitys sähköisen asioinnin turvallisuuden varmistamisessa. Lailla säänneltyihin vahvan sähköisen tunnistamisen palveluihin luotetaan yhä enenevässä määrin taloudellisesti ja toisaalta yksityisyyden suojan kannalta merkittävissä asiointitilanteissa kuten vaikkapa kiinteistön kaupassa ja terveydenhuollon tietoihin pääsyssä. Vahvan sähköisen tunnistamisen palveluihin kohdistuvan luottamuksen johdosta niiden sääntelyssä on kiinnitettävä erityistä huomiota etenkin käsitteiden ymmärrettävyyteen sekä palveluiden luotettavuuden ja turvallisuuden kannalta keskeisiin vaatimuksiin.

Yleisenä havaintona tunnistuslain ja asetuksen osalta on nähtävissä haasteet, joita uuden toimintaympäristön (luottamusverkoston) luominen ja sen proaktiivinen sääntely asettavat lainsäätäjälle. Sekä tunnistuslain että asetuksen sisällössä on epätarkkuuksia sen suhteen, keihin ja mihin

1 Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla.

luottamusverkoston rajapintoihin säännöksiä sovellettaisiin, miten nämä rajapinnat toteutettaisiin ja mihin esimerkiksi Viestintäviraston ohjaus ja -valvontatoiminta kohdistuisi.

Luottamusverkoston toiminnan sääntelyä on tarkoitus tarkentaa alemman asteisilla säännöksillä kuten asetuksella ja mahdollisesti sitäkin alemman asteisilla normeilla. On kuitenkin tärkeää, että jo tunnistuslain sisällöstä voidaan selvästi päätellä, mitä asioita sääntely koskee ja mitkä jäävät sen ulkopuolelle. Myös henkilötietojen käsittelyn ja tietoturvallisuusvaatimusten reunaehtojen sekä valvontaviranomaisen olennaisten tehtävien tulisi riittävällä tarkkuudella käydä ilmi jo laista.

Luottamusverkoston toimintaperiaatteet eivät kaikilta osin käy ilmi tunnistuslaista tai asetuksesta. Yksi merkittävä kysymys harkittaessa säädännön sisältöä on, kuinka käytännössä toteutetaan se, että sähköisen palvelun tarjoajan ei tarvitsisi tehdä sopimusta kuin yhden tunnistuspalvelun tarjoajan kanssa voidakseen tarjota palveluitaan kaikkien tunnistuspalvelun tarjoajien käyttäjille.

Viestintävirasto olettaa lausunnossaan, että tarkoitus ei ole rakentaa luottamusverkostolle mitään erillistä keskuslaitetta, joka välittäisi tunnistuspyyntöjä ja tunnistussanomia keskitetysti, vaan että pyynnöt liikkuvat suoraan tunnistuspalvelun tarjoajalta toiselle joskin tietysti riittävällä tasolla suojattuna.

> Yksinkertaistettu esimerkki Viestintäviraston oletusten perusteella:
>
> Nordea Pankki Suomi Oyj:n (Nordea) myöntämän tunnistusvälineen haltija tulee sähköisen palvelun sivustolle, joka käyttää Elisa Oyj:n tunnistuspalvelua. Käyttäjä siirtyy ensin Elisa Oyj:n tunnistuspalveluun, jossa hänelle avautuu mahdollisuus päästä edelleen Nordean tunnistuspalveluun. Käyttäjä tunnistautuu Nordean tunnistuspalvelussa, josta tunnistustapahtumaa koskeva tunnistussanoma lähetetään Elisalle, joka välittää sen edellä mainittuun sähköiseen palveluun, johon asiakas haluaa tunnistautua.

Lausuntopyynnössä on pyydetty lausujia selkeästi erottamaan toisistaan tunnistuslaista ja asetuksesta annettavat lausunnot. Edellä todetut seikat huomioon ottaen erottaminen ei kaikilta osin ole mahdollista. Kyseessä on sääntelykokonaisuus, jonka osalta tulisi vielä harkita millä tasolla esimerkiksi asetuksessa nyt olevista tietoturvallisuusvelvoitteista ja valvontaviranomaisen toimivallasta on säädettävä myös laissa. Toisaalta lainsäädännön tasolla tehtävät rajaukset vaikuttavat asetuksen lopulliseen sisältöön. On myös nähtävissä mahdollinen tarve myös eräiden toistaiseksi huomiotta jääneiden kysymysten (esimerkiksi luottamusverkoston tietojen salassapito ja perusteet tietojen luovuttamiselle) täsmentämiselle laissa.

Viestintävirasto haluaa lausunnossaan kiinnittää liikenne- ja viestintäministeriön huomion erityisesti seuraaviin myöhemmin yksityiskohtaisemmin kuvattaviin asiakokonaisuuksiin:

1. Viestintäviraston tehtävien tarkoituksenmukaisuus, oikeasuhtaisuus, ohjauksen ja valvonnan keinot sekä taloudelliset ja henkilöresurssit

2. Lain yksikäsitteisyys ja vaatimusten asettaminen lain tasolla

3. Hintasäänteln tarkoitus ja keinot

Viestintäviraston tehtävien tarkoituksenmukaisuus, oikeasuhtaisuus, ohjauksen ja valvonnan keinot sekä taloudelliset ja henkilöresurssit

Viestintäviraston tehtäviin ei ole ehdotettu tunnistuslaissa muutoksia. Asetuksessa on ehdotettu Viestintävirastolle merkittäviä lisätehtäviä, joiden tulisi riittävällä tasolla käydä ilmi tunnistuslaista. Lisäksi ehdotettujen tehtävien sisältöä tulisi sekä keventää että täsmentää. Muun muassa luottamusverkoston hallinnointiin ja tekniseen määrittelyyn liittyvien tehtävien hoitamisessa olisi arvioita huolella, minkä tahon tehtäviin nämä olisi tarkoituksenmukaisinta sisällyttää.

Luottamusverkoston yhteistyösopimuksen hallinta

Asetuksen 1 §:n mukaan:

> "*Luottamusverkoston jäsenet sitoutuvat toimimaan yhteistyössä ja sopivat erikseen yhteistyön toteuttamisesta. Yhteistyösopimuksen hallinnasta vastaa Viestintävirasto. Yhteistyösopimuksen liitteinä on oltava jokaisen sopimukseen liittyneen toimijan tunnistuspalvelun kuvaus sekä siihen liittyvät turvallisuuskäytäntöjen kuvaukset.*
>
> *Luottamusverkostoon kuuluvan toimijan vahvoilla sähköisillä tunnistusvälineillä on voitava tehdä muiden tunnistusvälineiden liikkeellelaskijoiden tunnistusvälineiden rekisteröinnin yhteydessä hakijan sähköinen ensitunnistaminen, eikä hyödynnettävän tunnistusvälineen liikkeellelaskija voi erikseen estää oman välineensä hyödyntämistä tunnistustapahtumassa.*"

Asetuksen 3 §:n mukaan:

> "*Jokainen Viestintäviraston rekisteröimä tunnistuspalvelun tarjoaja on velvoitettu toimittamaan osana palvelun rekisteröintiä tunnistuspalvelun turvallisuuskäytännöt (esim. varmennepolitiikka) sekä ylläpitämään ja kehittämään niitä. Turvallisuuskäytäntöjen kuvaukset liitetään yhteistyösopimuksen liitteiksi.*
> […]
> *Yhteistyösopimuksessa kuvataan loppukäyttäjien palvelusopimusten yleiset ehdot. Luottamusverkostoon kuuluva tunnistuspalvelun tarjoaja vastaa suhteessa muihin luottamusverkostoon kuuluviin tunnistuspalveluiden tarjoajiin omista asiakkaistaan, näiden kanssa tekemistä sopimuksistaan, asiakkaille tarjoamistaan tunnistuspalveluista sekä näihin liittyvistä vahingonkorvausvaatimuksista.*"

Tunnistuslain uuden määritelmän mukaan luottamusverkostoon kuuluvat tunnistuspalvelun tarjoajien lisäksi sähköisen palvelun tarjoajat sekä tunnistuspalveluiden käyttäjät/tunnistusvälineiden haltijat. Ilmeisesti on kuitenkin tarkoitus velvoittaa yhteistyöhön ainoastaan tunnistuspalvelun tarjoajat. Mahdollisesti yhteistoimintaa ja säädettyjä toimintamalleja sekä rajapintoja yms. noudattamista koskevien velvoitteiden tulisi olla laissa ja niiden tulisi kohdistua ainoastaan tunnistuspalvelun tarjoajiin - ei muihin luottamusverkoston jäseniin.

Mikäli katsotaan tarkoituksenmukaiseksi, että Viestintävirasto toimii tunnistuspalvelun tarjoajien luottamusverkoston sääntöjen laatijana ja niiden noudattamisen valvojana, olisi sopimusta tarkoituksenmukaisempi instrumentti velvoittava määräys (tunnistuspalvelujen tietoturvallisuudesta ja luottamusverkoston toiminnasta tms.). Sen sijaan että sopimusehdot olisivat yhteistyösopimuksen liitteitä, Viestintävirastolle ilmoitettaviin tietoihin (lain 10 §) tulisi tarvittaessa täsmentää, että myös loppukäyttäjien (sähköisen palvelun tarjoajat ja tunnistusvälineiden haltijat)

palvelusopimusten yleiset ehdot tulee toimittaa Viestintävirastolle. Viestintävirasto arvioi, onko luottamusverkosto kuvattu niissä siten kuin siitä on laissa, asetuksessa ja Viestintäviraston määräyksessä säädetty.

Mitä tulee tunnistuspalvelun kuvaukseen ja turvallisuuskäytäntöihin, tulisi harkita, riittäisikö että Viestintävirasto laatii toiminnallisia ja turvallisuusvaatimuksia koskevan määräyksen liitteineen ja valvoo, että kaikki noudattavat sitä. Vai onko välttämätöntä, että toimijat jakavat nämä tiedot toisilleen varmistuakseen muiden toimijoiden toiminnan lainmukaisuudesta. Riippuen palvelunkuvausten ja turvallisuuskäytäntöjen tasosta, ne voivat olla liikesalaisuuksia tai palvelun turvallisuuden kannalta salassa pidettäviä tietoja, joita toimijat eivät välttämättä halua jakaa toisilleen ja niiden joutuminen vääriin käsiin voi myös vaarantaa tunnistuspalveluiden ja luottamusverkoston tietoturvallisuuden. (Salassapitoa on käsitelty myös jäljempänä erikseen.)

Ehdotus:

Viestintävirasto ehdottaa, että luovutaan yhteistyösopimuksen käsitteestä ainakin viranomaisen valvontainstrumenttina. Verkoston toimintaperiaatteista ja mahdollisista turvallisuusvaatimuksista voitaisiin säätää valtioneuvoston asetuksella ja tarkemmin Viestintäviraston määräyksellä. Lakiin tarvittaisiin määräyksenantovaltuus.

Mikäli tunnistuspalveluiden ja luottamusverkoston toimintaperiaatteet ja turvallisuusvaatimukset on kuvattu riittävällä tasolla laissa ja alemmanasteisissa säännöksissä, ei välttämättä ole tarpeen laatia mallisopimusehtoja eri asiakasrajapintoihin taikka vaatia toimijoita jakamaan tarkkaa kuvausta palveluistaan tai niiden turvallisuuskäytännöistä keskenään.

Lakiin tulisi tarkentaa velvollisuus toimittaa Viestintävirastolle aloitusilmoituksen yhteydessä selvitys siitä, kuinka toimija toteuttaa luottamusverkostoa (ja tietysti sen omaa palvelua) koskevat vaatimukset mukaan lukien tiedot loppukäyttäjien kanssa tehtävien sopimusten ehdoista. Osittain nämä tiedot sisältyvät jo 10 §:ssä lueteltuihin tietoihin. Mikäli jäljempänä mainittu auditointi tehdään, voidaan selvitys antaa ainakin osittain auditointiraportin muodossa.

Viestintäviraston määräys ei luonnollisesti sulje pois toimialan mahdollisuutta sopia asioista ja esimerkiksi itsesääntelyllä laatia yhteisiä mallisopimuslausekkeita tms. kilpailulainsäädännön reunaehdot huomioon ottaen.

Luottamusverkoston teknisten rajapintakuvausten laatiminen ja rajapinnan hyödyntämiseen liittyvän dokumentaation yhteiskäytön valvonta

Asetuksen 3 §:stä voi päätellä, että olisi mahdollisesti tarkoitus, että Viestintävirasto laatii tekniset rajapintakuvaukset tunnistuspalveluiden luottamusverkostoon. Viestintävirasto on ymmärtänyt, että mainitut rajapintakuvaukset koskisivat nimenomaan ja ainoastaan tunnistuspalveluiden välisiä rajapintoja ja että ns. asiakasrajapinnat tunnistusvälineiden haltijoihin ja sähköisiin palveluntarjoajiin eivät kuuluisi kuvausten piiriin. Lisäksi Viestintävirasto on ymmärtänyt, että

rajapintakuvaukset tarkoittaisivat sen määrittelemistä, mitä tietoa siirtyy ja keiden välillä kussakin tilanteessa.

Ehdotus:

Viestintävirasto ehdottaa, että luovutaan rajapintakuvauksen ja sen hyödyntämiseen liittyvän dokumentaation käsitteestä ainakin viranomaisen ohjaus- ja valvontainstrumenttina.

Mikäli on ehdottoman välttämätöntä, että viranomainen laatii tekniset rajapintakuvaukset, tulee laissa riittävällä tasolla määritellä, mitä rajapintoja määritelmät koskevat, mitä henkilötietoja niissä siirtyy ja keiden välillä. Lisäksi määräyksenantovaltuuden koskien rajapintoja tulisi olla laissa. Eri tilanteina tietosisällön suhteen voitaneen pitää ainakin tunnistusvälineen hakijan tunnistamisen rajapintaa ja toisaalta "tavallista" tunnistuspyyntöä ja vastaussanomaa.

Tekniset rajapintakuvaukset voisivat ainakin yksityiskohtaisella ohjelmistokielen tasolla olla viittauksia mahdollisiin valmiisiin standardeihin[2].

Tiettyä järjestelmää koskeviin teknisiin rajapintakuvauksiin liittyy myös tietoturvallisuusnäkökulma. Mitä yksityiskohtaisemmalle tasolle kuvaukset viedään, sitä helpommin niiden avulla on mahdollisuus pyrkiä hyödyntämään palveluiden mahdollisia haavoittuvuuksia - varsinkin jos myös edellisessä jaksossa kuvatut tunnistuspalvelun tarjoajien luottamusverkoston ja yksittäisten palveluiden turvallisuuskäytännöt ovat kovin yksityiskohtaisesti tiedossa. Tästä syystä, olivatpa kuvaukset ja käytännöt tms. kenen hyvänsä hallussa ja ylläpidossa, tulisi tunnistuspalvelun tarjoajille säätää salassapitovelvollisuus koskien mainittuja tietoja. Valvontaviranomaisen tulisi voida saada tiedot. (Salassapitoa on käsitelty myös jäljempänä erikseen.)

Tunnistuspalvelun tarjoajien auditoinnin yksityiskohtaisten vaatimusten laatiminen ja auditointi

Asetuksen 3 §:n mukaan

> "*Luottamusverkoston kaikki jäsenet ovat velvoitettuja esittämään auditointiraportin, joka ei ole yli kuusi kuukautta vanha, osana Viestintävirastolle tehtävää ilmoitusta ennen yleisölle tarjottavan vahvan sähköisen tunnistustoiminnan aloittamista. Auditoinnin voi suorittaa Viestintävirasto tai sen hyväksymä toimija. Viestintävirasto antaa teknisillä ohjeilla auditoinnin yksityiskohtaiset vaatimukset.*"

Auditointivaatimukset voisivat koostua edellä selostetusta Viestintäviraston teknisestä määräyksestä ja sen mahdollisista tarkentavista liitteistä, kuten luottamusverkoston tekninen rajapintamäärittely, auditointivaatimukset ja yleinen kuvaus vaatimustenmukaisuuden täyttymisen toteamisesta. eIDAS asetuksen johdosta on laadittu ETSIssä luottamuspalvelun tarjoajien vaatimustenmukaisuuden arviointia koskevia dokumentteja, joita voitaisiin mahdollisesti soveltuvin osain hyödyntää auditointivaatimuksia laadittaessa. Myös komission tunnistuspalvelujen turvatasoja koskevat vaatimukset on otettava huomioon. Viime kädessä yksityiskohtaisina vaatimuksina voitaisiin

2 Rajapintakuvaukset näyttävät olevan standardipohjaisia: esim. SAML v2.0 on kuvattu: http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.html

käyttää VAHTIa tai KATAKRI III:sta. Riippuen siitä, missä määrin vaatimusten julkistaminen voi vaarantaa tunnistuspalveluiden ja/tai luottamusverkoston tietoturvallisuuden, on vaatimusten mahdollisesti oltava osittain salassa pidettäviä siten, että ne voidaan luovuttaa vain tietyin edellytyksin siten kuin viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 13 §:n 2 momentissa säädetään. (Salassapitoa on käsitelty myös jäljempänä erikseen.)

Mikäli kaikki luottamusverkoston tunnistuspalvelun tarjoajat on auditoitava, tulisi tämän velvoitteen käydä ilmi laista, sillä siitä aiheutuu toimijoille vähäistä suurempia kustannuksia.[3] Lakiin on myös otettava viittaus arviointitoimintaa koskevaan lakeihin[4] siten, että on selvää, ketkä arviointeja suorittavat ja millä perusteella.

Viestintäviraston osalta on selvennettävä, että Viestintävirasto tekisi viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain mukaisen auditoinnin ja perisi mainitun lain mukaiset maksut, vaikka mainitun lain piiriin ei kuulu yksityisten yhteisöjen auditointi ilman yhteisön toiminnan viranomaiskytkentää. Lisäksi lakiviittauksin ja lain perusteluissa on selvennettävä, että sekä Viestintävirasto että tietoturvallisuuden arviointilaitokset perivät auditoinnista maksun siten kuin arviointitoimintaa koskevissa laeissa tai niiden nojalla säädetään tai erikseen sovitaan.[5]

Palvelukuvausten, turvallisuuskäytäntöjen/-vaatimusten ja teknisten rajapintakuvausten salassapidosta

Kaikki tunnistuspalvelun tarjoajat tarvinnevat tarkat kuvaukset luottamusverkon toiminnasta, tietoturvallisuudesta ja teknisistä rajapinnoista. Riippumatta siitä, pitääkö näitä tarkkoja kuvauksia yllä Viestintävirasto esimerkiksi määräyksen liitteinä tai palveluntarjoajat itsesääntelynä, on varmistettava, etteivät palveluntarjoamisen turvallisuuden kannalta kriittiset tiedot päädy julkisuuteen.

Tunnistuspalvelun tarjoajien osalta tulisi tarvittaessa säätää mainittujen tietojen suojaamisesta, käsittelyoikeuksista, luovuttamisesta sekä salassapidosta (mukaan lukien vaitiolo-/salassapitovelvollisuuden laiminlyönnin rangaistusseuraamuksista). Lisäksi tulisi ratkaista, millä edellytyksillä ja missä vaiheessa näitä tietoja luovutetaan toimintaa aloittavalle tai muulle tunnistuspalvelun tarjoajalle, jota ei ole vielä auditoitu. Tulisiko esimerkiksi velvoittaa nykyiset toimijat sekä tulevaisuudessa tunnistuspalvelun aloitusilmoitusta tekevät yhteisöt taustatarkistuksiin ja/tai esiauditointiin ennen tietojen luovuttamista. Tietojen luovuttaminen/luottamusverkostoon liittyminen voitaisiin mahdollisesti myös kytkeä siihen, että palveluntarjoajasta on tehty yritysturvallisuusselvitys siten kuin turvallisuusselvityslain 5 luvussa säädetään.

3 Toimijoiden tulisi myös pystyä ottamaan tulemat kulut huomioon budjetoinnissaan.
4 Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011) ja laki tietoturvallisuuden arviointilaitoksista (1405/2011).
5 Viestintäviraston maksuista on säädetty viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain 12 §:n mukaisesti tarkemmin asetuksella. Tietoturvallisuuden arviointilaitokset perivät arvioinnista toimeksiantajan kanssa tekemänsä sopimuksen mukaisen, liiketaloudellisin perustein määrittelemänsä maksun.

Luottamusverkoston turvallisuusvaatimusten ja rajapintakuvausten paljastuminen ei vielä välittömästi johtaisi jokaisen yksittäisen tunnistuspalvelun tarjoajan palveluiden vaarantumiseen. Viestintäviraston näkemyksen mukaan ei tulisi kasvattaa palveluihin kohdistuvaa riskiä velvoittamalla tunnistuspalvelun tarjoajat jakamaan tarkkaa tietoa omaan palvelunsa kohdistuvien tietoturvallisuusvaatimusten toteuttamisesta muille kuin valvontaviranomaiselle. Mikäli palveluntarjoajat auditoidaan, ei myöskään pitäisi olla perustetta epäillä tietoturvallisuudelle asetettujen vaatimusten täyttymistä.

Viestintäviraston resurssit

Riippumatta siitä, mikä taho ja millä tasolla, laatii luottamusverkoston toiminnan edellyttämät vaatimus- ja rajapintamäärittelyt, on annettu aikataulu (vuoden 2016 alussa valmis) todella tiukka. Mikäli vaatimusmäärittelyjen jälkeen on tehtävä auditointeja, tarvitaan edelleen lisää aikaa. Ottaen huomioon luottamusverkoston toiminnan kriittisyys ei myöskään voida ajatella, että se otettaisiin tuotantokäyttöön ilman perusteellista testausta.

Viestintäviraston tuotot tunnistuspalveluiden tarjoajien valvontamaksuista ovat tällä hetkellä n. 156 000 euroa vuodessa (+laatuvarmentajan valvontamaksu 40 000). Olemassa olevilla resursseilla ei pystytä suorittamaan kaavailtuja uusia tehtäviä, joiden suorittamiseen oletettavasti ei riittäisi edes 6 henkilön työpanos, mikäli tehtävien pitäisi olla tehtyinä vuodessa. [6]

Ehdotus:

Jotta luottamusverkoston edellyttämät hallinnolliset ja tekniset kuvaukset ja yksityiskohtaiset vaatimukset olisi mahdollista saada valmiiksi ennen luottamusverkoston toiminnan alkamista, tulisi luottamusverkoston toiminta, toimijat, verkoston rajapinnat sekä Viestintäviraston tehtävät kuvata selkeästi laissa ja mahdollisesti asetuksessa. Lisäksi tulisi harkita, kuinka kevyillä vaatimuksilla luottamusverkosto voidaan toteuttaa.

Ottaen huomioon, että tunnistuspalvelun tarjoajien valvontamaksut kattavat tällä hetkellä noin yhden henkilötyövuoden panoksen, tulee Viestintävirastolle osoittaa lisää taloudellisia ja henkilöresursseja luottamusverkoston toiminnallisten ja tietoturvavaatimusten, teknisten rajapintakuvausten sekä yksityiskohtaisten auditointikriteerien laatimiselle. Myös eIDAS asetuksen nojalla annettavien tarkempien vaatimusten laadinta ja siihen liittyvän standardointityön seuranta vievät paljon henkilötyöaikaa. On syytä huomata, että auditoinneista saatavilla maksuilla katetaan ainoastaan auditoinneista aiheutuvat kustannukset - ei mainittujen vaatimusmäärittelyjen laatimisen kustannuksia.

Viestintäviraston arvio tarpeellisista lisähenkilöresursseista on 5 henkilötyövuotta (nykyisen yhden lisäksi) niin kauan kuin vaatimusten

6 Vertailutietona voidaan mainita, että Viestintäviraston käynnissä olevan verkkotunnusprojektin toteuttamiseen menee melkein 3 vuotta 6 - 10 miestyövuoden panoksella. Projektien erilaisuudesta huolimatta tätä voitaneen pitää jonkinlaisena vertailukohteena.

laadinta ja muu siirtymävaihe on suoritettu. Tämänkin jälkeen tarvitaan enemmän henkilötyövuosia kuin nyt ottaen huomioon viraston kasvava rooli palveluntarjoajien ja luottamusverkoston valvonnassa sekä eIDAS asetuksesta seuraavat lisätehtävät. Siirtymäkauden jälkeenkin tarvitaan arviolta kolme henkilöä (kaksi enemmän kuin nyt) suorittamaan tunnistuspalvelujen ohjaus- ja valvontatehtävää sekä auditointeja.

Luottamusverkoston toiminnan käynnistäminen ei näyttäisi olevan mahdollista annetulla aikataululla, vaikka mainitut resurssit saataisiin. Henkilöiden palkkaamiseen ja/tai mahdolliseen perehdyttämiseen, vaatimusten laatimiseen, niiden toteuttamiseen, verkoston testaamiseen ja toimijoiden arviointiin tarvitaan lisää aikaa.

Mikäli Viestintävirastolle kaavaillut tehtävät edellyttävät julkisen hankinnan tekemistä (järjestelmän tai konsultoinnin hankinta), vie hankinnan tekeminen oman aikansa ja edellyttää myös taloudellisia lisäresursseja.

Lain yksikäsitteisyys ja vaatimusten asettaminen lain tasolla

Luottamusverkoston käsite

Viestintävirasto ehdottaa, että lain perusteluista (yleisperustelut ja 2 §:n 14 kohta sekä 12 a §) poistetaan maininnat koskien sitä, että sähköisen palvelun tarjoaja voisi valita, mihin tunnistuspalveluihin luottaa. Valintaa ei ainakaan tulisi voida tehdä ja samalla liittyä osittain käyttämään luottamusverkostoa. Mikäli verkostoon tehdään määrittelemätön määrä sähköisen palveluiden tarjoajien valinnoista riippuvia "estoja" vaarantaa se todennäköisesti palvelun toimivuutta ja tuo merkittävästi lisähaasteita teknisten rajapintamäärittelyiden laatimiseen.

Mahdollinen vaihtoehto on antaa sellaiselle sähköisen palvelun tarjoajalle, joka ei halua käyttää kuin tiettyjä tunnistuspalveluja, mahdollisuus tehdä valinta sopimalla palvelusta vain kunkin haluamansa tunnistuspalvelun tarjoajan kanssa erikseen, mikäli tunnistuspalvelun tarjoaja haluaa tarjota ns. "erillispalvelua". Näiden erillispalveluiden toteutusten osalta tunnistuspalvelun tarjoajat eivät olisi osa luottamusverkostoa paitsi 17 §:n 4 momentin osalta, mikäli ne käyttävät jonkin toisen tunnistuspalvelun tarjoajan tunnistusvälinettä tunnistusvälineen hakijan tunnistamisessa. Tämä vaihtoehto edellyttäisi mainintaa lakiin, että tunnistuspalvelun tarjoaja voi tarjota myös sellaista palvelua, jossa ei välitetä edelleen toisen palveluntarjoajan tunnistussanomia.

Lienee tarkoitus, että tunnistuspalvelun tarjoajat saavat toteuttaa asiakasrajapintansa (käyttäjiin ja sähköisiin palveluihin nähden) omalla tavallaan kunhan noudattavat palvelun turvallisuutta koskevia vaatimuksia. Suuri osa lisävaatimuksista tulee siten koskemaan tunnistuspalvelun tarjoajien välistä luottamusverkostoa. Mainituista syistä voisi olla tarpeen joko muuttaa Luottamusverkoston määritelmää tai määritellä erikseen tunnistuspalvelun tarjoajien välinen luottamusverkosto.

Eri rajapintojen määrittely

Viestintäviraston käsityksen mukaan tunnistuspalvelun tarjoajien luottamusverkoston teknisissä rajapinnoissa on karkeasti arvioituna kahdenlaisia tapahtumia:

1. Tunnistusvälineen hakijan tunnistaminen tunnistusvälinettä haettaessa (17 § 4 mom)

2. Yksittäisen tunnistustapahtuman toteuttaminen (12 a § 3 mom)

Nämä tilanteet olisi hyvä määritellä selkeästi lain tasolla erikseen ja kuvata laissa (ei vain perusteluissa) ainakin ylätasolla ne tiedot, jotka siirretään näissä tilanteissa tunnistuspalvelun tarjoajien välillä.

Sähköisiä allekirjoituksia tarjoava varmentaja (6 ja 7 §)

"Sähköisiä allekirjoituksia tarjoava varmentaja" on mainittu tunnistuslain 6 ja 7 §:issä. Tätä toimijaa ei ole määritelty missään ja silti sille on säädetty oikeuksia ja velvollisuuksia. Viestintäviraston näkemyksen mukaan pitäisi joko määritellä "sähköisiä allekirjoituksia tarjoava varmentaja" tai poistaa ilmaus 6 ja 7 §:istä.

Jos ilmaisulla on tarkoitettu laatuvarmenteita tarjoavaa varmentajaa, tulisi se sanoa selvästi laissa. Jos taas on tarkoitettu sitä, että tunnistuspalvelun tarjoajalla on oikeus käsitellä mainittuja tietoja myös niissä tapauksissa, joissa tunnistusvälineellä tehdään allekirjoituksia (lain 4 §), tulisi asian käydä selvemmin ilmi lainsäädännöstä.

Tunnistamista koskevien tietojen säilyttäminen 17 § 4 mom ja 24 §

Tunnistuslain 17 § 4 momentin perustelut ovat osittain ristiriidassa lain 24 §:n kanssa, jonka mukaan on säilytettävä tiedot ensitunnistamisen tekemisessä käytetyistä asiakirjoista.

Viestintäviraston näkemyksen mukaan voisi olla hyvä siirtää tiedot ns. ensitunnistamisen ketjutuksesta siinä rajapinnassa, jossa tunnistusvälineen hakija tunnistetaan käyttämällä vahvan sähköisen tunnistamisen tunnistusvälinettä. Mahdollisten tunnistamisessa ilmenneiden ongelmien selvittämiseksi jokaisen tunnistuspalveluntarjoajan tulisi myös säilyttää koko ketjua koskeva tieto. Vähintäänkin pitää säilyttää tieto siitä, kenen myöntämällä tunnistusvälineellä hakija on tunnistettu. Tämä edellyttää muutoksia lain 24 §:ään.

Edellä mainitulla on kytkös myös siihen vaatimukseen, että aina kun hakija tunnistetaan olemassa olevalla sähköisen tunnistamisen välineellä, korvauksen saa ensitunnistamisen tekijä (17 § 4 mom). Tällöin lienee oltava tiedossa, mikä taho ensitunnistamisen on tehnyt.

Hallintopakkokeinot ja ilmoitusvelvollisuudet

Hallintopakkokeinona lain perusteluissa on viitattu vain lain 45 §:ään. Myös lain 12 §:n 2 mom (toiminnan kieltämismahdollisuus) tulisi nostaa esille.

Lisäksi tulisi harkita, pitäisikö Viestintävirastolla olla mahdollisuus määrätä tunnistuspalvelun tarjoajan toiminta keskeytettäväksi siten, että määräys olisi heti täytäntöönpanokelpoinen. Tätä keskeyttämismääräystä käytettäisiin tilanteessa, jossa tunnistuspalvelun tarjoajan toiminta

vaarantaa tunnistamisen luotettavuuden tai koko luottamusverkoston toiminnan.

Mahdollisesti lakiin (16 §) tulisi myös lisätä velvollisuus kertoa toisille tunnistuspalveluntarjoajille, jos tunnistuspalvelun tarjoaja on toiminnallaan vaarantanut luottamusverkoston turvallisuuden. Lisäksi tulisi harkita VML 131 §:ää vastaavaa velvoitetta kytkeä irti oma tai toisen palvelu luottamusverkostosta. Viestintävirasto voisi tarvittaessa velvoittaa irtikytkemiseen.

Voimaantulo ja siirtymäsäännökset

Siirtymäsäännöksessä on otettu huomioon ainoastaan lain 12 a §. Viestintäviraston käsityksen mukaan kaikki ehdotetut muutokset (luottamusverkoston määritelmä, 6,7 ja 17 §:n muutokset sekä uusi 12 a §) tulisivat noudatettavaksi vasta sitten kun luottamusverkoston toiminta alkaa.

Hintasääntelyn tarkoitus ja keinot

Ensitunnistamisen tekijän kohtuullinen korvaus

Tunnistuslain 17 §:n 4 momenttiin ehdotetaan seuraavaa:

> *Olemassa olevan vahvan sähköisen tunnistusvälineen avulla on voitava hakea vahvaa sähköistä tunnistusvälinettä. Edellä 2 momentissa tarkoitetun henkilökohtaisen ensitunnistuksen tehnyt tunnistuspalvelun tarjoaja on oikeutettu kohtuulliseen korvaukseen. Aiempaan ensitunnistukseen luottava vahvan sähköisen tunnistuspalvelun tarjoaja vastaa mahdollisesta ensitunnistuksen virheellisyydestä suhteessa vahingon kärsineeseen.*

Säännöksen yksityiskohtaisissa perusteluissa todetaan, että "*kohtuullisen korvauksen enimmäismääränä voitaisiin pitää 15 prosenttia kulloinkin voimassa olevan poliisin palveluhinnaston mukaisesta henkilön tunnistamisen hinnasta. Esimerkiksi vuoden 2014 poliisin palveluhinnaston mukaisesti sähköisesti tehdyn ensitunnistuksen enimmäiskorvaus olisi 6,45 euroa.*"

Perusteluissa ei mainita syitä hintasääntelylle eli sitä, miksi hinnasta pitäisi ylipäätään säätää lailla. Syyt tulisi perustella, koska hintasääntely on poikkeus normaalitilanteeseen, jossa jokainen määrittelee mahdolliset maksut ja muut ehdot sopimusperusteisesti.

Itse säännöksen mukaan ensitunnistamisen tehnyt tunnistuspalvelun tarjoaja on oikeutettu kohtuulliseen korvaukseen. Säännöksessä ei täsmennetä, mistä korvaus maksetaan ja mikä taho maksun suorittaa. Nämä asiat olisi syytä täsmentää laissa. Lisäksi voisi selventää, tuleeko ensitunnistamisen tarjoamisesta jotain muita kuluja, esim. yhteyksien luomisesta, ensitunnistamiseen liittyvän sopimuksen tekemisestä vai aiheutuuko pelkästään kertaluontoisia kuluja kustakin tunnistustapahtumasta.

Säännöksessä käytetään ilmaisua "kohtuullinen korvaus". Perusteluissa kerrotaan toisaalta, mitä kohtuullisuuden arvioinnissa voidaan ottaa

huomioon ja toisaalta esitetään euromääräisesti, mitä on pidettävä kohtuullisena korvauksena. Olisi syytä valita jompikumpi lähestymistapa. Mikäli valitaan euromääräinen hinta, se pitäisi viedä lakitasolle ja perusteluissa perustella miksi juuri siihen on päädytty. Jos taas perustellaan mitä kohtuullisuuden arvioinnissa on otettava huomioon, tulisi miettiä miten kohtuullisuuden kriteerit suhtautuvat euromäärän esittämiseen - tai kannattaako euromääriä mainita. Pitkäkestoisten hinnoittelua koskevien oikeudenkäyntien välttämiseksi Viestintävirasto kannattaa (mikäli hintasääntelyyn päädytään) enimmäishinnasta säätämistä mahdollisimman tarkasti siten, että sääntely on lain tasolla eikä ainoastaan perusteluissa.

Jos perusteluissa ja/tai laissa todetaan, että hinta voi olla 15 % poliisin palveluhinnaston mukaisesta henkilön tunnistamisesta, pitäisi tarkemmin perustella sitä, miksi näitä kahta hintaa ylipäätään voidaan pitää vertailukelpoisina. Poliisi kuitenkin perii maksun suoraan tunnistettavalta (ja nimenomaan henkilökohtaisesta tunnistamisesta). Tunnistuslaissa olisi kyse sähköisestä tapahtumasta kahden tunnistuspalvelun tarjoajan välillä. Nyt ainoat perusteluissa todetut seikat liittyvät siihen, että sähköinen ensitunnistaminen voidaan tehdä monta kertaa ja että ensitunnistaminen on tehty ensisijaisesti muuta kuin tunnistuspalvelun tarjontaa varten.

Toisaalta perusteluissa viitataan nykyisten ensitunnistajien esittämiin kustannuksiin kohtuullisuuden arvioimiseksi. Jää epäselväksi, onko näiltäkin osin kyse edelleen poliisin hinnaston mukaan määräytyvän hinnan perusteluista vai siitä, mitä kohtuullisen hinnan arvioinnissa otettaisiin huomioon ja voiko tilanne tältä osin muuttua.

Tunnistustapahtuman korvaus

Tunnistuslain 12 a §:ään ehdotetaan seuraavaa:

> *Sähköisen tunnistuspalvelun tarjoajan lähettäessä sähköiseen tunnistusvälineeseen liittyvää tietoa toiselle sähköisen tunnistuspalvelun tarjoajalle edelleen välitettäväksi, välitettävästä tunnistetiedosta **tulee** suorittaa lähettäjälle korvaus.*
>
> [...]
>
> *Luottamusverkoston hallinnollisista käytännöistä, teknisistä rajapinnoista, vastuista sekä tunnistuspalvelujen tarjoajien välillä lähetettävistä tunnistetietietojen korvauksista säädetään tarkemmin valtioneuvoston asetuksella.*

Asetuksen 2 §:ssä säädettäisiin siirtohinnoittelun osalta seuraavaa:

> *Sähköisen tunnistuspalvelun tarjoajan lähettäessä sähköiseen tunnisteeseen liittyvää tietoa toiselle sähköisen tunnistuspalvelun tarjoajalle edelleen välitettäväksi, välitettävästä tunnistetiedosta **voidaan** suorittaa lähettäjälle korvaus. Välitettävästä tunnistetiedosta perittävä korvaus voi olla enintään 1 sentti.*
>
> *Tunnistuspalveluiden tarjoajat voivat keskinäisellä sopimuksella sopia myös alemmasta hinnasta tai hinnoittelusta, joka mahdollistaa tapahtumamääristä riippumattoman korvauksen. Keskimääräinen korvaus välitettävästä tunnistetiedosta ei saa kuitenkaan ylittää edellä mainittua tapahtumakohtaista 1 momentissa säädettyä enimmäiskorvausta.*

Korvausta välitettävistä tunnistetiedoista ei voida periä tunnistustapahtumista, jotka ovat Euroopan parlamentin ja neuvoston asetuksen (eu) n:o 910/2014 sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla mukaisia rajat ylittäviä tunnistustapahtumia.

Tunnistuspalvelun tarjoaja, joka edelleen välittää toisen tunnistuspalvelun tarjoajan tunnistamia loppukäyttäjien tietoja, maksaa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain 12 a §:n 2 momentissa säädetyn korvauksen loppukäyttäjän tunnistaneelle tunnistuspalvelun tarjoajalle. Jos tunnistuspalvelun tarjoaja toimii tunnistusvälineiden jakelijana ja tunnistustapahtumia välittävänä toimijana, ei sisäistä korvausta välitettävistä tunnistetiedoista tarvitse suorittaa.

Tunnistustapahtumaan liittyvästä tunnistamisesta maksettavan korvauksen kohdalla pätee myös edellisessä jaksossa todettu koskien hintasääntelyn syiden selvittämistä sekä sääntelyn lain tasolle saattamista.

Lopuksi

Viestintäviraston arvion mukaan sekä tunnistuslain että asetuksen säännöksiä on täsmennettävä luottamusverkoston toimintaympäristön selkeyttämiseksi. Erityistä huomiota on kiinnitettävä Viestintäviraston tehtävien tarkoituksenmukaisuuteen ja siihen, että toimivallasta ja sen reunaehdoista on riittävällä tarkkuudella säädetty lain tasolla. Lisäksi tulee huolehtia siitä, että valvovalla viranomaisella on riittävästi resursseja ja aikaa tehtävänsä suorittamiseksi.