

19.11.2015

Dnro:  
1194/04/2015

kirjaamo@lvm.fi

Lausuntopyyntönne, asia LVM/992/03/2015

## Viestintäviraston lausunto luonnoksesta valtioneuvoston asetukseksi vahvan sähköisen tunnistuspalvelun tarjoajien luottamusverkostosta

Liikenne- ja viestintäministeriö on pyytänyt Viestintävirastolta lausuntoa luonnoksesta valtioneuvoston asetukseksi vahvan sähköisen tunnistuspalvelun tarjoajien luottamusverkostosta.

Viestintävirasto on ollut mukana lausuntopyynnössä mainitussa hallintamallityöryhmässä, joka on avustanut asetusluonnoksen ja muiden luottamusverkoston toiminnan kannalta tarvittavien asiapapereiden valmistelussa.

### Keskeiset huomiot luonnoksesta

Asetus tulee tarkentamaan tunnistuslain 12 a §:aa ja asetuksen sisältö on olennainen luottamusverkoston toimivuuden kannalta.

Viestintävirasto näkee luonnoksen sisällön vastaavan niitä periaatteita, jotka hallintamalliryhmässä ovat olleet esillä.

Viestintävirasto ehdottaa kuitenkin, että asetukseen lisättäisiin luottamusverkoston hallinnollisena käytäntönä säännös yhteistoimintaryhmästä, jotta nykyiset ja tulevat toimijat sitoutetaan yhteissäätelyyn ja sen tuloksiin. Tästä on uusi pykäläehdotus lausunnon lopussa.

Viestintävirasto on tarkastellut asetusluonnosta suhteessa tunnistuslain säännöksiin ja suhteessa luonnosvaiheessa oleviin luottamusverkoston käytännesääntöihin. Virasto haluaa tuoda asetuksen ja tunnistuslain muutosten valmistelun tueksi esille seuraavia havaintoja sääntelyn yksityiskohdista:

### 2 § Määritelmät

Viestintävirasto pitää tärkeänä sitä, että *tunnistusvälineen tarjoaja* ja *tunnistuksen välityspalvelun tarjoaja* määritellään säädännössä erikseen, sillä näiden roolissa ja velvoitteissa on perustellusti eroja. Määritelmät olisi siksi toivottavaa lisätä tai siirtää lakiin, kun sen muutosta valmistellaan. Molemmat roolit

kattava yläkäsite *tunnistuspalveluntarjoaja* on nyt määritelty lain tasolla.

*Tekninen rajapinta* -termiä käytetään asetuksessa ja myös se olisi hyvä määritellä säädännössä. Määritelmä voisi olla esimerkiksi seuraava: toimijoiden välisen tiedonsiirron määrittelyt ja toteutukset.

Asetuksessa voisi harkita käytettäväksi vahvan sähköisen tunnistamisen palveluja EU-tasolla sääntelevän Eidas-asetuksen (EU) 910/2014 termejä *henkilön tunnistetieto* ja *luottava osapuoli*.

### **3 § Luottamusverkoston tekniset rajapinnat**

Viestintävirasto katsoo, että 1 momentin kohdassa 1 todettu *tunnistusvälineiden tarjoajien välinen rajapinta* eli ensitunnistamisen ketjuttamiseen tarvittava rajapinta kuuluu lähtökohtaisesti asetuksen piiriin, sillä sähköisten tunnistusvälineiden helpompi myöntäminen ja luominen luo osaltaan edellytyksiä tunnistuspalveluita tarjoavien ja niitä hyödyntävien toimijoiden väliselle toiminnalle.

Edelleen Viestintävirasto katsoo, että 1 momentin kohdassa 2 tunnistuksen *välityspalveluntarjoajan ja tunnistuspalvelua hyödyntävän toimijan* välinen rajapinta kuuluu asetuksen piiriin ainakin siltä osin, että tässä rajapinnassa tarvitaan valmiutta vähimmäistunnistetietojen välittämiseen.

Yleisesti Viestintävirasto korostaa teknisten rajapintojen sääntelyssä sitä, että sääntelyn tarkoitus on vakioida ja määritellä toimintaa vain siltä osin ja sillä tarkkuudella, että toimijoiden välinen sopiminen aidosti helpottuisi käytännössä, mutta toisaalta myös siten, että edistetään kilpailua vahvistamalla neuvotteluasemaltaan heikompien sopijaosapuolten asemaa. Määrittelyjen ratkaisujen lisäksi tai sijaan on aina mahdollista sopia muistakin toteutuksista.

Tarkemmat määrittelytarpeet koskevat Viestintäviraston käsityksen mukaan tällä hetkellä 1 momentin kohdan 2 mukaista *tunnistusvälineen tarjoajan ja tunnistuksen välityspalvelun* välistä rajapintaa. Muita rajapintoja koskevat lain ja asetuksen yleiset vaatimukset.

Asetusluonnoksen 3 §:n 3 momentissa säädetään teknisen rajapinnan vaatimukseksi standardinmukaisuus. Viestintävirasto ehdottaa tässä vielä huomioitavaksi sen, että yleisesti käytetyistä standardeista on niiden määrittelyjen avoimuuden takia välttämätöntä laatia standardin puitteissa *kansalliset määrittelyt*, jotka aidosti helpottavat ja edesauttavat luottamusverkoston toimijoiden välistä yhteentoimivuutta ja sopimista.

Lisäksi Viestintävirasto ehdottaa harkittavaksi, että asetuksessa tai ainakin sen perusteluissa näkyisi myös hallintamallityöryhmän valmistelussa muodostettu näkemys: *välineen tarjoajalle* riittää valmius yhteen määriteltyyn rajapintaan, mutta tunnis-

tuksen *välityspalvelun tarjoajalla* tulee olla valmius käyttää tarvittaessa kaikkia.

Edellä todetut asiat voisi tarkentaa asetuksessa 3 §:n 3 momentissa seuraavasti

*Luottamusverkostoon kuuluvan tunnistusvälineen tarjoajan on tarjottava luottamusverkoston edellä 1 momentin kohdassa 2 tarkoitettussa rajapinnassa vähintään yhtä yleisesti käytettyyn standardiin pohjautuvan kansallisen määrittelyn mukaista teknistä rajapintaa ja tunnistuksen välityspalvelun tarjoajalla tulee olla valmius tarjota (niitä) kaikkia (yleisesti käytettyyn standardiin pohjautuvan kansallisen määrittelyn mukaisia teknisiä rajapintoja).*

Viestintävirasto toivoo, että perustelumuiotiossa mainittaisiin se, että Viestintävirasto laatii esimerkiksi teknisellä määräyksellä tarkoituksenmukaisella tarkkuustasolla OpenId Connect- ja SAML-standardeista kansalliset profiilit yhteistyössä toimialan kanssa ja että kansallisesti määritetyt rajapintoja tulee olemaan tämän hetkisen tiedon mukaan enintään kolme.

Myös TUPAS -toteutusta olisi hyvä käsitellä perusteluissa vaihtoehtona, koska hallintamallityöryhmän valmistelutyössä on päädytty siihen, että myös se pyrittäisiin huomioimaan lain ja asetuksen tavoitteet täyttävänä rajapintana.

Edellä käsitellyt tarkennukset 3 momentissa koskisivat vain välineen tarjoajan ja välityspalvelun tarjoajan välistä rajapintaa. Jos asetuksessa harkitaan tarpeelliseksi varautua mahdollisiin tuleviin määrittelytarpeisiin muiden rajapintojen osalta, niiden määrittelyjen tulisi pohjautua vastaavasti yleisesti käytettyihin standardeihin tai hyviin käytäntöihin.

#### **4 § Luottamusverkoston hallinnolliset vastuut**

Viestintävirasto pitää 4 §:n 1 momenttiin koottuja yhteistoimintavastuun piiriin kuuluvia asioita oikeaan osuneina ja tärkeinä luottamusverkoston toimivuuden kannalta. Ilmaus "vastaa omalta osaltaan" tuo esille sen, että kaikki veloitteet eivät toiminnan luonteen takia ole relevantteja kaikkien toimijoiden kannalta.

Viestintävirasto käy seuraavassa lyhyesti läpi eri kohdat siitä näkökulmasta, miten niiden voi tulevassa asetuksen valvonnassa arvioida niveltävän tunnistuslain velvoitteisiin.

**Kohdassa 1** todettu **tunnistetietojen välittäminen** on koko verkoston toiminnan tarkoitus ja sen voi nähdä täydentävän tunnistuslain 12 a §:n 2 momentista seuraavaa yleistä veloitetta tarjota välinettä tai välitystä luottamusverkostossa.

**Kohdassa 2** todettu **tekniset rajapinnat, niiden toimivuus ja saatavilla olo** täydentävät tunnistuslain 12 a §:n 2 momentin yhteentoimivuutta, mutta koskevat yhteentoimivuuden li-

säksi myös palvelun laatua ja saatavuutta, joista laissa ei ole varsinaisia vaatimuksia. Jos laadulle nähtäisiin tarpeelliseksi asettaa joltain osin vaatimuksia, asiasta tulisi Viestintäviraston arvion mukaan säätää laissa. Viestintävirastolla ei sinänsä ole kantaa siihen, säännelläkö laatua vai jääkö se sopimuksilla sovittavaksi asiaksi. Tällä on vaikutusta siihen, voidaanko asiaan puuttua virhetilanteessa viranomaisvalvonnalla vai ratkais-taanko asia sopimuksen perusteella.

**Kohdassa 3** todettu **teknisen rajapinnan dokumentaation** yhteiskäyttö täydentää Viestintäviraston käsityksen mukaan tunnistuslain 12 a §:n edellyttämiä hallinnollisia käytäntöjä, jotka mahdollistavat sopimusten tekemisen. Jos toimijat käyttävät jotain luottamusverkoston vähimmäisvalikoimaan kuulu-vaa yleistä rajapintaa, Viestintäviraston laatimat määrittelyt ovat julkisia ja tämä asetuksen kohta koskee yrityksen omia tarkempia määrittelyjä. Jos käytetään muuta rajapintaa, yrityk-sen määrittely voi kattaa suuremman osan yritysten välisen tiedonsiirron järjestämisessä tarvittavista tiedoista.

**Kohdassa 4** mainitun **veloituksen teknisen oikeellisuuden** voi nähdä täydentävän tunnistuslain 12 a §:n 3 momentin hin-tasäätelyä, mutta muutoin tekninen oikeellisuus on nähtävä osaksi laatua, jota käsitellään 2 kohdassa.

**Kohdassa 5** todettu **häiriötilanteiden tiedonvaihto ja sel-vittäminen** liittyvät tunnistuslain 12 a §:n 2 momentin edellyt-tämiin hallinnollisiin käytäntöihin yhteentoimivuuden mahdollis-tamiseksi, mutta selvittämisestä ja tiedonvaihdosta ei ole tun-nistuslaissa ei ole varsinaisia vaatimuksia.

Lain 24 §:ssä säädetyt tunnistustapahtumaa ja tunnistusvä-linettä koskevat tiedon tallennusvelvollisuudet liittyvät toimijoi-den kyvykkyyteen selvittää joitain häiriöitä.

Lain 16 §:ssä säädetään tällä hetkellä tunnistuspalveluntarjo-ajan velvollisuudesta ilmoittaa palveluntarjoajille, tunnistusväli-neiden haltijoille ja Viestintävirastolle palvelun tietoturvaan kohdistuvista merkittävistä uhkista ja häiriöistä. Viestintäviras-ton näkemyksen mukaan 16 §:n velvollisuutta olisi tarpeellista laajentaa koskemaan myös luottamusverkoston jäseniä ja il-moituskynnyksen tulisi olla matala ja aikataulun nopea luotta-musverkoston jäsenten välillä ja virastolle. Viestintävirasto nä-kee omaksi roolikseen seurata tietoturvallisuuden tilannetta luottamusverkostossa ja analysoida häiriöitä ja uhkia sekä ohja-ta tarvittaessa tietoturvallisuutta edistäviä käytäntöjä. Virasto katsoo kuitenkin, että operatiivinen 24/7 -luonteinen tiedon-vaihto- ja selvitystyö kuuluu yritysten vastuulle.

Viestintävirasto kiinnittää 5 kohdan yhteydessä huomiota sii-hen, että sääntelyssä olisi vielä hyvä selkeyttää velvoitteita eri-laisissa häiriötilanteissa. Häiriöiksi katsottavat tai koettavat ti-lanteet voivat koskea kolmea eri perustilannetta: 1) muutosti-lanteet tai huoltokatkot, 2) vikatilanteista ja kapasiteettiongel-mista johtuvat katkot (toimivuus ja laatu) ja 3) tietoturvauhkut ja -häiriöt. Tunnistustoiminnassa erityisiä häiriöitä ovat lisäksi

tunnisteet, jotka on annettu väärälle henkilölle. Nämä voidaan joko katsoa tietoturvahäiriöiksi, koska ne vaarantavat tiedon luottamuksellisuutta tai käsitellä omana häiriötyyppinä.

Asetusehdotuksen 4 §:n 1 momentin 5 kohdassa käsitellään häiriöiden selvittämistä. Koska tunnustuslaissa ei tällä hetkellä säädetä häiriöiden selvittämisen yhteistoiminnasta ja koska asetusehdotus jättää avoimeksi sen, mitä häiriötilanteita selvittämisvelvollisuus koskee, Viestintävirasto ehdottaa asiaa selvennettäväksi sekä asetuksessa että tulevassa lainmuutoksessa.

Viestintävirasto arvioi tärkeimmäksi tietoturvahäiriöiden ja identiteetin väärinkäytösten selvittämisen ja ehdottaa niiden huomioimista myös lain valmistelussa.

Laatuhäiriöiden selvittäminen voi muiden laatuasioiden tapaan olla sopimusasia (, joskin välityspalveluiden tekninen riippuvuus välineen myöntäjien palvelun jatkuvasta saatavuudesta on hyvä tunnistaa harkinnassa.) Muutos-, huolto- ja vikatilanteissa lakiin voisi harkita yleistä velvollisuutta huomioida ja minimoida vaikutukset muihin toimijoihin luottamusverkostossa ja velvollisuutta tiedottaa näistä tilanteista.

**Kohdassa 6** todettu **sopimusten laatiminen ja ylläpito** liitetään perustelumuiistiossa tunnustuslain 12 a §:n 4 momentin velvoitteeseen, jonka mukaan tunnistuspalveluntarjoajat vastaavat yhteistyössä teknisten rajapintojen ja hallinnollisten käytäntöjen yhteentoimivuudesta. Viestintävirasto ehdottaa kaikkia toimijoita koskevien sopimuskäytäntöjen osalta seuraavassa kohdassa kuvattua täydennystä asetukseen. Virasto ehdottaa myös harkittavaksi, että tässä 6 kohdassa viitattaisiin yhteissäätelyn mukaisten sopimuskäytäntöjen toteuttamiseen osaltaan kahdenvälisissä sopimuksissa luottamusverkoston toimijoiden välillä.

### **§ Luottamusverkoston hallinnolliset käytännöt**

Hallintamallityöryhmän valmistelutyössä on päädytty siihen, että siltä osin kun verkoston toiminnasta ei ole tarpeen säätää, yhteisistä käytännöistä huolehdittaisiin jatkossa yhteissäätelyllä Viestintäviraston vetämässä työryhmässä.

Asetusehdotuksen 4 §:ssä huomioidaan hyvin yhteistoiminnan aiheita, mutta toimintatapa ja sitoutuminen yhteistoimintaan jää avoimeksi. Tunnustuslain 12 a §:n 4 momentissa todetaan, että tunnistuspalveluntarjoajat vastaavat yhteistyössä teknisten rajapintojen ja hallinnollisten käytäntöjen yhteentoimivuudesta. Viestintävirasto ehdottaa, että sitoutuminen yhteissäätelyyn ja siinä laadittaviin käytänteisiin huomioitaisiin asetuksessa. Tämä olisi myös markkinoille tulijoiden kannalta selkeää ja avointa.

Luottamusverkoston hallinnolliset käytännöt voisi säätää asetuksessa kuvaamalla suunnitellun yhteissäätelyryhmän tehtävät seuraavaan tapaan

*Viestintävirasto voi asettaa luottamusverkoston yhteistoimintaryhmän, jossa voivat olla edustettuina luottamusverkoston jäsenet ja viranomaiset, jotka ohjaavat ja valvovat luottamusverkoston toimintaa sekä muut toimijat, joiden osallistuminen katsotaan tarkoituksenmukaiseksi.*

*Luottamusverkoston yhteistoimintaryhmän tehtävänä on valmistella luottamusverkoston toimintaan liittyviä ohjeita ja sopimusmalleja, vaihtaa tietoa luottamusverkoston toimintaan liittyvistä kysymyksistä ja seurata toimialan kehitystä, joka vaikuttaa luottamusverkoston toimintaan.*

Viestintävirasto pitää sinänsä suunniteltua yhteissäätelymallia tarkoituksenmukaisena ja korostaa sitä, että viraston asetukseen kirjattavaksi ehdottama malli sallii joustavasti myös sen, että yritysten rooli kasvaa yhteistoiminnassa ja vähentää lähtötilanteen viranomaisvetoisuutta sitä mukaa, kun yritysten valmius ja intressit tähän lisääntyvät.



Jarmo Ilme  
Pääjohtajan sijaisena  
Viestintävirasto



Anne Lohtander  
Lakimies  
Viestintävirasto