

Anne Mäenpää

19.2.2016

**Liikenne- ja viestintäministeriölle**

Lausuntopyyntö: LVM/2005/03/2015

**VAHVASTA SÄHKÖISESTÄ TUNNISTAMISESTA JA SÄHKÖISISTÄ ALLEKIRJOITUKSISTA ANNETUN LAIN SEKÄ ERÄIDEN SIIHEN LIITTYVIEN LAKIEN MUUTTAMINEN**

Oy Samlink Ab:lta on pyydetty lausuntoa yllä mainitussa asiassa. Esitämme lausuntonamme seuraavaa.

Taustaksi tuomme esille, että Oy Samlink Ab toimii teknisenä toimittajana n. 80 %:lle nykyisistä rekisteröityneistä vahvan sähköisen tunnistuspalvelun tarjoajista (pankkeja) ja kauttamme kulkee yli 100 miljoonaa tunnistustapahtumaa vuosittain.

Vuosittaisista pankkitunnuksilla tehtävistä tunnistuksista noin 95 % kohdistuu pankkien omien palveluiden käyttöön ja vain noin 5 % tunnistautumisiin muiden asiointipalveluiden tarjoajien palveluihin.

**Yleistä**

Näkemyksemme mukaan lainsäädäntömuutokset tähtäävät, jos eivät kokonaan, niin ainakin valtaosaltaan puhtaasti julkisen hallinnon palveluiden tarpeiden täyttämisen varmistamiseen. Yksityisen sektorin palveluntarjoajien, kuten tunnistuspalveluiden tarjoajina toimivien pankkien, tarpeet eivät näyttäisi tulevan erityisen hyvin otetuiksi huomioon.

Pankkialan toimijoiden osalta on myös otettava huomioon se, että on ensiarvoisen tärkeitä varmistaa lainsäädännön yhdenmukaisuus ja ristiriidattomuus laajasti niin, että pankit pystyvät täyttämään eri valvontaviranomaisten määräyksistä johtuvat velvoitteet ilman riskiä siitä, että jonkin määräyksen noudattaminen johtaa toisen määräyksen rikkomiseen.

Pidämme tärkeänä sitä, että jatkossakin kunkin yksityisen sektorin asiointipalveluiden tarjoajan tulisi voida päättää itse niistä sähköisistä tunnistusvälineistä, jotka se hyväksyy omissa palveluissaan. Toimijoiden kannalta on lisäksi olennaista, että pankkitunnuksista ja Tupas-tunnistuspalvelua voidaan tarjota ja hyödyntää myös luottamusverkostosta riippumatta.

Tärkeää on myös se, ettei jää epäselväksi jokaisen sähköisen tunnistusvälineen tarjoajan oma päätösvalta siitä ilmoitetaanko sen sähköisen tunnistamisen järjestelmä EU:n komissiolle vai ei. Rajat ylittävään palvelun tarjoamiseen ei tule sääntelyllä kaikkia toimijoita pakottaa.

Anne Mäenpää

19.2.2016

### **Tunnistusvälineen hakemisen ketjuttamisen rajaaminen**

Väärinkäytösmahdollisuuksien välttämiseksi, esim. identiteettivarkauksista aiheutuvat ongelmatilanteet, olisi tärkeää, ettei ketjuttaminen olisi rajattomasti mahdollista. Tunnistusvälineen haltijan oikeusturvanäkökohtia tulisi painottaa selkeämmin jo suoraan sääntelyssä eikä näin tärkeitä asioita tulisi jättää puhtaasti toimijoiden välisiin sopimuksiin ratkaistaviksi.

Tärkeää olisi, että tunnistusvälineen haltijalle luotaisiin keino mm. estää uusien tunnistusvälineiden luonti. Lisäksi turvallisuutta lisäävä tekijä voisi olla se, että sähköisellä ensitunnistamisella luotu uusi sähköinen tunnistusväline olisi heikompi tasoinen kunnes tunnistusvälineen haltijan henkilökohtainen ensitunnistus on tehty.

Ketjuttamiseen liittyen pitäisi varmistaa, että tunnistamistapahtumissa välitetään mm. riittävät tiedot käyttäjän ensitunnistamisesta ja siitä miten se on tehty, fyysisesti vai sähköisesti (ketjutuksen seuranta). Lisäksi palveluntarjoajalle on tärkeää saada tiedot tunnistusvälineestä, jotta on mahdollista päättää, onko käytettävä tunnistusväline sellainen, jonka palveluntarjoaja hyväksyy.

### **Tunnistusvälineen haltijan yksilöinti – sähköinen asiointitunnus (SATU)**

Haluamme nostaa esille myös sen, että niin sääntelyssä kuin teknisissä ratkaisuissa tulisi huolehtia siitä, että henkilötunnuksen sijasta mahdollistettaisiin yksiselitteisesti sähköisen asiointitunnuksen käyttäminen. SATU on neutraalimpi yksilöintitieto toisin kuin HETU, joka kertoo henkilöstä muitakin henkilötietoja ja jonka käyttö tästä syystä on monissa yhteyksissä koettu ongelmalliseksi.

### **Dynaaminen todentamistekijä – nykyisestä poikkeava vaatimus tunnistusmenetelmälle (tunnistusvälineelle)**

Perustuen siihen, mitä EU-asetukseen (EU) N:o 910/2014 liittyvässä täytäntöönpanoasetuksessa (EU) 2015/1502 todetaan, ehdotetaan todentamismenetelmässä aina käytettävän dynaamista todentamistekijää (lakiehdotuksen 8 a § (tai 8 b §) 2 mom.). Tämä on selkeästi aivan uusi vaatimus tunnistusvälineelle. Vaatimuksesta saattaa seurata se, että tiukasti tulkiten nykyisten pankkitunnusten ei voitaisi katsoa täyttävän korotetun varmuustason vaatimuksia, toisin kuin aiemmin on todettu. Tällä saattaa olla merkittäviä seurausvaikutuksia syntyvän luottamusverkoston laajuudelle. Toivottavaa olisi, että vaatimuksen merkitystä avattaisiin perusteluissa nykyistä enemmän ja selkeämmin.

### **Auditointivaatimukset ja aikataulu**

Lakiehdotuksessa esitetään vahvan sähköisen tunnistuspalvelun tarjoajalle velvollisuutta osoittaa tunnistuspalvelunsa vaatimustenmukaisuus sekä toimittaa

Anne Mäenpää

19.2.2016

arviointikertomus suoritetusta riippumattomasta tunnistuspalvelun arvioinnista Viestintävirastolle vuoden 2016 loppuun mennessä.

Arviointiperusteiden ja -vaatimusten tarkempi määrittäminen ja dokumentointi Viestintävirastossa, jolle määräystenantovalta ehdotetaan kuuluvaksi, on vielä kesken.

Korostamme sitä, että sekä auditointi- että tietoturva-vaatimusten tulee perustua yleisiin kansainvälisiin standardeihin ja käytäntöihin.

Avoinna olevia asioita ovat lisäksi mm. yksityiskohdat, joiden perusteella voitaisiin arvioida syntyviä kustannuksia sekä menettelyjä, jos toimijat muodostavat yhteenliittymän tai käyttävät samaa teknistä toimittajaa. Samoin päätökset ja kuvaukset tarvittavista teknisistä rajapinnoista ovat auki.

Niiden tietojen perusteella, jotka vaatimuksista tällä hetkellä on käytettävissä, voidaan olettaa, että toimijoille aiheutuvat kustannukset tulevat olemaan merkittäviä toisin kuin ehdotuksessa annetaan ymmärtää. Vielä avoinna olevien yksityiskohtien vuoksi kustannusten tarkempi analysointi ei kuitenkaan ole mahdollista.

Haluamme korostaa, että kun otetaan huomioon, että perustavaa laatua olevat yksityiskohdat eivät ole tiedossa, myöskään ehdotettua aikataulua ei voi pitää realistisena. Luottamusverkostoon kuulumisen mahdollistaminen edellyttää joka tapauksessa teknisiä muutoksia sekä sähköisen tunnistuspalvelun vaatimustenmukaisuusarviointien suorittamista.

Pidämme tärkeänä, että aikataulu olisi järkevässä suhteessa siihen, milloin lopulliset tekniset rajapintavaatimukset ja lopulliset auditointivaatimukset ovat toimijoiden käytettävissä.

OY SAMLINK AB

Jari Pirhonen  
Turvallisuusjohtaja

Anne Mäenpää  
Lakimies