Fujitsu Finland Oy:n lausunto koskien Liikenne- ja viestintäministeriön ”Lausuntopyyntöä vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain sekä eräiden siihen liittyvien lakien muuttamisesta” (Dnro LVM/2005/03/2015)

Kiitämme mahdollisuudesta kertoa mielipiteemme lakiluonnoksesta liittyen sähköiseen tunnistamiseen ja allekirjoituksiin.

Yleistä

Sähköinen tunnistaminen on kehittymässä eteenpäin yli kymmenen vuoden pysähtyneestä tilasta, mutta nyt kaikki ehdotetut kehityssuunnat eivät edistä digitalisaation tai sähköisen asioinnin tavoitteita. Tähän asti vahva tunnistaminen on yli 98%:sti perustunut pankkitunnuksiin, eikä merkittävää asemaa saavuttaneita uusia tunnistusmenetelmiä tai –välineitä ole tullut markkinoille.

Samalla sähköisen allekirjoituksen ratkaisut ovat säilyneet lähinnä kokeilujen asteella, eikä lähitulevaisuudessa ole odotettavissa ainakaan kansallisella tasolla etenemistä tässä asiassa. Yritykset sen sijaa ovat omassa toiminnassaan oman kokemuksemme mukaan kiinnostuneita etenemään ainakin kokeiluihin, jotta ne pääsisivät ajasta ja paikasta riippumattomaan sopimiseen asiakkaidensa kanssa eli juuri tilanteeseen, joka sähköisellä allekirjoituksella saavutettaisiin.

KaPA-ohjelmassa on toteutettu VRK:n toimesta KaPA-arkkitehtuurin mukainen julkishallinnon tunnistuksen välityspalvelu korvaamaan Vetuma-palvelun. Samalla ollaan siirtymässä arkkitehtuuriin, jossa sähköisen palvelun tarjoaja tekee sopimuksen yhden tai useamman tunnistuksen välityspalvelun kanssa ja vastaavasti tunnistusvälinepalvelut tekevät sopimuksen todennäköisesti kaikkien tunnistusvälityspalveluiden kanssa. Tämä helpottaa teoriassa uusien tunnistusvälinepalveluiden markkinoille tuloa, mutta sopimusongelmaa on liioiteltu.

Tunnistustoimintaa hallinnoimaan on luotu Luottamusverkosto, jonka jäseniksi kaikkien vahvoja tunnistuspalveluita tarjoavien osapuolten on liityttävä. Liikenne- ja Viestintäministeriö ohjaa luottamusverkon toimintaa ja osaltaan antaa määräyksiä tunnistuspalveluissa ja allekirjoituksissa noudatettavista käytännöistä. Luottamusverkosto ohjaa ja kehittää omaa toimintaansa tunnistuksen ja allekirjoitusten lain ja LVM käytäntöjen puitteissa. EU:n eIDAS säädökset tulevat suoraan voimaan EU-tasolta ja Suomen lainsäädäntöä on harmonisoitava monilta osin eIDAS:n vaikutuksesta.

Suuri osa esitetyistä muutoksista eri lakeihin on yhteensopivuuden kannalta pakollisia. Haluaisimme kuitenkin painottaa eri lainkohtien vaikutusta vahvan tunnistamisen ja allekirjoitusten kehittymiseen ja käytön laajenemiseen.

Vahvan tunnistamisen markkina

Vahva tunnistaminen jakautuu kolmeen eri segmenttiin: Julkishallinnon palvelut, pankki- ja vakuutusalan palvelut ja muut yksityissektorin palvelut.

Julkishallinto	Julkishallinnon tunnistustapahtumien määrä vuonna oli 2015 Vetuman osalta noin 31 miljoonaa tunnistusta. Tässä merkittävimpänä oli Kela, jonka palvelut vastasivat noin 70% kaikista Vetuma-tapahtumista. Veron ja TEM:n ottaminen mukaan lisää tunnistusten määrää ehkä 10 miljoonalla vuodessa ja palveluiden digitalisoinnin kautta tunnistusten määrä on kasvamassa tasaisesti.
Pankki- ja vakuutus	Eri lähteiden mukaan kansalaisten pankki- ja vakuutusalan tunnistuksia on luokkaa 400 miljoonaa vuodessa. Tämä määrä ei ole laskemassa tulevina vuosina.
Muu yksityissektori	Yksityissektorilla ei ole ollut juurikaan tarvetta vahvalle henkilön tunnistamiselle. Verkkokaupankäynnissä myyjälle riittää tieto, että käyttäjällä on voimassa oleva pankki- tai luottokortti, Paypal-tili tai muu maksuväline, eikä henkilön tarkka identiteetti ole niin tärkeä. Yksityisen puolen terveydenhuollon palveluihin voi olla tarvetta tunnistautua vahvasti, mutta muuten vahvan tunnistautumisen markkina on yksityissektorissa pieni, eikä merkittävää kasvua ole odotettavissa. Vasta sähköisen allekirjoituksen yleistyessä alkaa vahvan tunnistamisen määrä kasvaa.

Markkinoiden koon pienuuden vuoksi ennustamme, että yksityiselle puolelle ilmestyy tunnistuksenvälityspalveluita vain muutamia.

Tunnistusvälinepalveluiden yksityiset markkinat tulevat kasvamaan julkihallinnon digitalisaation edetessä tasaisesti, mutta kasvupotentiaali on silti Suomen kokoisessa markkinassa rajallinen, johtuen muun muassa jo olemassa olevista laajalti käytössä olevista ratkaisuista.

Ennustamme tunnistusmarkkinoiden jakautuvan julkihallinnon tunnistuksiin ja nykyisten toimijoiden tunnistuksiin ja vastaavasti erilaisiin tunnistusvälineisiin. Tältä pohjalta koko vahvan tunnistuksen tavoiteltavissa olevat markkinat ovat varsin pienet, eivätkä ne tule mahdollistamaan kannattavaa liiketoimintaa ainakaan monelle toimijalle. Korkeat hallinnointimaksut (47 §) ja Väestötietojärjestelmän kyselyt (7 §) kuormittavat liiketoimintaa entisestään. Mikäli kaavaillun lain tavoitteena on yksityisen puolen ratkaisuiden kehittyminen, ovat tällaiset maksut omiaan vähentämään potentiaalista kilpailua jo ennestään rajatuilla markkinoilla. Tästä syystä ehdotamme, että poistetaan laista tunnistuspalveluiden hallinnointiin (47 §) ja jatkuvaan tunnistuspalvelutoimintaan (olemassa olon tarkistus 7§ ja 7a §) liittyvät maksut.

Ehdotuksemme: **Poistetaan laista tunnistuspalveluiden hallinnointiin (47 §) ja jatkuvaan tunnistuspalvelutoimintaan (olemassaolon tarkistus 7§ ja 7a §) liittyvät maksut.**

Tietoturvan ja tunnistuspalveluiden saatavuuden takaaminen

Tunnistuspalveluiden tietotekninen luotettavuus on ratkaisevassa asemassa erilaisten digitaalisiin palveluihin liittyvien tapahtumien ja luottamuksellisten tietojen suojaamisessa ja luottamuksen ylläpitämisessä. Kansalaisten luottamus palveluiden tietoturvallisuuteen on keskeisimpiä edellytyksiä palveluiden käytön yleistymiselle. Toisaalta yhä useamman yhteiskunnan palvelun käytettävyys edellyttää vuoden jokaisena päivänä, ympäri vuorokauden saatavissa olevia tunnistuspalveluita. Tunnistuspalveluiden toimivuus on kyettävä takaamaan myös kuormahuippujen aikana (esimerkiksi äänestykset, opiskelupaikkojen haku, veroilmoitusten jättö, jne.).

Riittävän luotettavuuden varmistamiseksi on kaikkien tunnistuspalveluiden kehitys- ja käyttövaiheissa noudatettava korkeita tietoturvavaatimuksia ja palveluiden koko elinkaari on auditoitava asianmukaisesti. Tämä menettely on jo käytössä esimerkiksi Vetuma-palvelussa, eikä tätä vaatimustasoa voi ainakaan alentaa missään uusissa tunnistuspalveluissa, oli ne toteuttanut Väestörekisterikeskus tai joku muu toimija.

Palveluntarjoajan on myös kyettävä osoittamaan riittävät ja uskottavat resurssit ja osaaminen tietoturva- ja saatavuuskriittisten palveluiden tuottamisessa. Näin ollen ehdotamme, että tunnistuspalveluiden koko elinkaaren osalta on noudatettava Vahti korotettu-tason (tai vastaavia) tietoturvavaatimuksia.

Ehdotuksemme: **Tunnistuspalveluiden koko elinkaaren osalta on noudatettava Vahti korotettu-tason (tai vastaavia) tietoturvavaatimuksia.**

Uusien tunnistusvälineiden markkinoille tulo

Suomen vahvan tunnistamisen markkinoille ei ole tullut useaan vuoteen yhtään uutta tunnistusvälinettä, viimeisin oli operaattoreiden yhdessä tuoma mobiilivarmenne vuosia sitten. Uuden tunnistusvälinepalvelun on liiketoiminnan aikaan saamiseksi (1) ensin investoitava ilman ensimmäistäkään asiakasta ensin palvelua tuottavan järjestelmän kehittämiseen ja saamiseen tietoturvatasoltaan normien mukaiseksi, (2) solmittava sopimukset välityspalveluiden kanssa, (3) markkinoitava palvelua kiinnostuksen herättämiseksi, (4) saatava myytyä tunnistusvälineet asiakkaille, ottamalla käyttäjiä palveluun ketjuttamalla olemassa olevista tunnistusmenetelmistä tai suorittamalla ensitunnistus ja (5) sitten odotettava palvelun käytön kasvamista.

Jos tunnistusvälineen hakemisessa ensitunnistus tehdään tunnistuspalvelun tiloissa, joutuu asiakas vastaamaan matka- ja matka-aikakuluista, sillä palveluntarjoajan liiketoimintamalli ei näitä kestä. Jos taas palveluun rekisteröinti tehdään ketjuttamalla, syntyy nykyisen lain mukaan tunnistusvälineen tarjoajalle vastuu mahdollisesta tunnistuksen virheellisyydestä suhteessa vahingon kärsineeseen (17 §). Tämä mahdollinen vahingonkorvausvastuu muodostuu erittäin vaikeasti käsiteltäväksi ongelmaksi. Tunnistusväline-palvelun tarjoajalla ei ole mahdollisuutta arvioida ketjutukseen sisältyvää riskiä, koska tietoa koko ensitunnistuksen ja sen jälkeen tehtyjen ketjutusten vaiheista ei tällä hetkellä saa mistään.

Tällä hetkellä vaikuttaa siltä, että vastuu tunnistukseen liittyvästä toiminnasta määräytyy eri tavoin eri kohdissa tunnistautumisketjua. Vaihtoehtoja on ainakin kolme: (1) henkilödokumentin myöntäjä, (2) ensitunnistaja ja (3) aiempaan tunnistukseen luottava ketjuttaja. Edellä mainitun 17§:n sisältämä vastuusäännös kohdistuu ainoastaan viimeiseen eli aiempaan tunnistukseen luottavaan ketjuttajaan. Ensitunnistajan vastuusta ei nimittäin ole vastaavankaltaista säännöstä.

Tässä on esimerkki kohtaan sisältyvästä vahingonkorvausvastuun ongelmasta.

> Ajatelleen tilanne, jossa henkilö saa rikollisin keinoin haltuunsa väärän henkilödokumentin (esimerkiksi passin) ja avaa sillä pankin tiskillä pankkitilin ja nostaa lainan. Vastuu määräytyy tällöin mm. yleisten vahingonkorvaus- ja rikosoikeudellisten sääntöjen mukaisesti.
>
> Jos henkilö hankkii samoilla (väärillä) henkilödokumenteilla sähköisen tunnisteen tunnistusvälipalveluntarjoajalta (ensitunnistaja), ei tämä tunnistusvälineen tarjoaja joudu tunnistuslain perusteella erityiseen korvausvastuuseen virheelliseen henkilödokumenttiin perustuvasta ensitunnistuksesta johtuvasta vahingosta, kunhan on toiminut huolellisesti.
>
> Mikäli kuitenkin sama henkilö ketjuttaa ensimmäisen tunnistusvälineen (, joka on siis edelleen hankittu väärin henkilödokumentein,) toisen tunnistusvälineentarjoajan sähköiseen tunnisteeseen, joutuu jälkimmäinen tunnistusvälineen ketjuttaja 17 §:n mukaiseen vahingonkorvausvastuuseen.

Millä perusteella sähköisen tunnistusvälineen ketjuttaminen voi muodostaa tällaisen koventuneen vahingonkorvausvastuun?

Tämä on todellinen ongelma, jonka juurisyy voi johtua inhimillisestä virheestä henkilödokumentin myöntämisessä, virheestä tietojärjestelmässä tai käyttäjän rikollisesta toiminnasta. Mielestämme tunnistusketjua ja siihen liittyviä vastuukysymyksiä tulisi tarkastella kokonaisuutena.

Ongelmaa saataisiin lievennettyä, mutta ei kokonaan poistettua, esimerkiksi seuraavilla toimenpiteillä:

1. Valtio perustaa ajantasaisen rekisterin, jonne tallennetaan: a) kaikkien myönnettyjen henkilödokumenttien tiedot ja b) kaikkien varastettujen tai hukkuneiden henkilödokumenttien tiedot. Tunnistusvälinepalveluiden tarjoajat voisivat tarkistaa palvelusta ensitunnistusvaiheessa ja ketjutusten yhteydessä henkilödokumenttien voimassa olon.
2. Valtio perustaa ajantasaisen rekisterin jonne tunnistuspalvelut päivittävät tapahtumatiedot kaikista ensitunnistamiseen perustuneista sähköisen tunnistusvälineen myöntämistapahtumista ja kaikista tunnistusvälineiden ketjutustapahtumista. Tämän rekisterin perusteella tunnistuspalvelun toimittaja voisi arvioida tunnistusvälineen ketjuttamiseen liittyviä riskejä. Edelleen, näillä kahdella rekisterillä olisi erityisesti merkitystä loppukäyttäjän (eli käytännössä kansalaisen) tunnistukseen

liittyvässä kontrollissa. Henkilö voisi siten esimerkiksi poliisilta tiedustelemalla saada selville kaikki häneen identiteetilleen myönnetyt henkilödokumentit ja niiden avulla saadut tunnistusvälineet.

3. Poistetaan yksiselitteinen tunnistusvälineiden aiempaan tunnistukseen luottavan ketjuttajan vahingonkorvausvastuu laista ja luodaan yhtenäinen koko vastuuketjun huomioiva vastuumalli.

Ehdotuksemme: **Valtio perustaa 1) rekisterin henkilödokumenttien käyttökelpoisuuden tarkastamiseksi, 2) rekisterin sähköisten tunnistusvälineiden myöntämisten tapahtumien tarkastamiseksi ja 3) poistaa laista tunnistusvälineen ketjuttamisen vahingonkorvausvastuun (17 §) ja luodaan yhtenäinen koko vastuuketjun huomioiva vastuumalli.**

Dynaaminen todentamistekijä

Tunnistamisen todentamistekijät kohdassa (8 b §) mainitaan, että jokaisessa tunnistamistapahtumassa on oltava mukana tapahtumakohtaisesti muuttuva todentamistekijä.

> ”Jokaisessa tunnistusmenetelmässä on käytettävä sellaista dynaamista todentamistekijää, joka voidaan muuttaa jokaisessa uudessa henkilön ja hänen henkilöllisyytensä varmentavan järjestelmän välillä tapahtuvassa todentamistapahtumassa.”

Jos kyseessä on fyysisen käyttäjän erilainen vaste jokaiseen tunnistamistapahtumaan, tarkoittaa se monessa tapauksessa PIN:n vaihtumista tapahtumasta toiseen. Tällainen ominaisuus korttitunnistuksessa (HST-kortti, organisaatiokortti, terveydenhuollon ammattilaisen kortti) ei toteudu nykyisissä korteissa ja on vaikeaa toteuttaa vaikka kortinkäsittelyä muutettaisiin uusiin PKI-korttitoteutuksiin. Sama ongelma saattaa koskea operaattoreiden liikkeelle laskemia mobiilivarmenteita.

Ehdotuksemme: **Poistetaan vaatimus (8 b §) dynaamisesta tunnistustekijästä PKI-kortin osalta laista.**

Kunnioittavasti

Helsingissä 22.2.2016

Fujitsu Finland Oy:n psta

_____ _____