Suomen tietoturvaklusterin (FISC) ry:n lausunto

Vahvasta sähköisestä tunnistamisesta ja sähköisestä allekirjoituksista annetun lain muuttamisesta

Lausuntopyyntö LVM/1518/03/2014

Finnish Information Security Cluster

LAUSUNTO

31. lokakuuta 2014

Johdanto

FISC on suomalaisten tietoturvayritysten muodostama teollisuusklusteri ja siihen kuuluu kaikki merkittävät alan yritykset sekä VTT. Moni klusterin jäsen toimii tunnistamis-, käyttövaltuus- ja identiteetin hallintaan liittyvällä alueella. Suomessa on näillä alueilla yksi maailman parhaista osaamiskeskittymistä. Tietoturvaklusterin näkemyksen mukaan Suomen kansallisten tunnistusratkaisujen sekä markkinoiden kehittäminen on tärkeää ja yhtenä tukipilarina tälle on siihen sovelias lainsäädäntö.

Suomi on ollut sähköisen asioinnin osalta pitkälle kehittynyt maa, verkkopankkien käyttöaste ovat korkealla, sähköisen maksamisen onnistuu lähes kaikkialla joka on johtanut turvallisen sähköisen maksamisen korkeaan käyttöasteeseen. Julkiset palvelut ovat varsin pitkälle kehitettyjä ja Suomessa voi mm. perustaa yrityksen kokonaan verkossa ja hoitaa lähes kaiken veroasioinnin käymättä fyysisesti verovirastoissa..

Sähköinen tunnistaminen on toteutettu eri markkinoilla hyvin eri tavoin. Useissa maissa vahva sähköinen tunnistaminen on edennyt pankkitoiminnan ja maksamisen toimiessa vetureina laajentuen sitten muihin sähköisiin asiointipalveluihin. Vaihtoehtoisia tapoja tälle ovat olleet operaattorivetoiset palvelumallit joista on esimerkkinä Turkki tai julkisen vallan rakentamat palvelumallit joista on esimerkkinä Viro.

Sähköisen tunnistamisen haasteena on roolien, vastuiden, liiketoiminnan ja teknisten ratkaisujen tasapainoinen yhteensovittaminen niin, että ne noudattavat liiketoiminnallisia lainalaisuuksia. Liiketoimintaperusteiden puuttuminen niiden toimijoiden kannalta jotka joutuvat ottamaan vastuita ja kustannuksia on ollut lähes poikkeuksetta suurin este laajamuotoisten tunnistuspalvelurakenteiden syntymiselle. Teknologiat sen sijaan mahdollistavat lukuisia eri toimintatapoja.

Lähtökohtaisesti sähköisessä tunnistamisessa mahdollistetaan hyvin erityyppisiä liiketoiminnallisia ja asiointiin liittyviä tapahtumia, joiden arvoa on mahdotonta yhteismitallistaa. Tunnistus voi liittyä arvokkaan kaupan toteutumisen kahden osapuolen välillä tai se voi olla pelkkä varmistus esimerkiksi blogikirjoituksen tekijästä ennen kirjoituksen julkaisua. Mikäli näissä toimenpiteissä toteutuu identiteetin väärinkäytös, ovat vaikutukset taloudelliselta merkitykseltään hyvin erilaisia.. Tämä heijastuu myös vastuukysymyksiin.

Suomessa tällä hetkellä tarjottavat sähköiset palvelut ovat edistyksellisiä. Nykyinen lainsäädäntö on mahdollistanut näiden palveluiden syntymisen. Jo olemassa olevilla sähköisillä tunnistamisilla on aikaansaatu satojen miljoonien eurojen säästöjä julkisella sektorilla sekä jopa miljardien eurojen säästöjä yksityisissä palveluissa. Suomessa käytetään laajasti vahvaa tunnistamista lähes kymmenessä tuhannessa verkkokaupassa ja palvelussa.. Näihin palvelurakenteisiin tehdyt nykyiset tunnistusratkaisuinvestoinnit ovat useiden satojen miljoonien eurojen arvoisia. Kaikki näihin olemassa oleviin järjestelmiin tehtävät muutokset ovat kustannusvaikutuksiltaan merkittäviä.
Julkisella sektorilla tehdään noin 30 miljoonaa vahvaa sähköistä tunnistusta vuodessa.

Käsillä oleva sähköisen tunnistamislain valmisteluvaihe on toteutettu kovalla kiireellä. Työn alkuvaiheessa valmistelutyön perusteena olivat markkinoiden epätoimivuus, tunnistamisen kustannukset julkisissa palveluissa sekä eräiden käyttäjäryhmien rajautuminen palveluiden ulkopuolelle. Nämä syyt ovat kuitenkin osoittautuneet taloudellisesti varsin pieniksi ja kokonaisuuden kannalta vähämerkityksisiksi..

Nyt markkinoilla olevien ratkaisujen merkittävin epäkohta on tunnistamiseen liittyvä sopimusrakenne joka edellyttää erillistä kahden välistä sopimusta osapuolten välillä. Tämä on tunnistamista hyödyntävälle palvelutarjoajalle merkittävä taloudellinen rasite. Yhtenä merkittävänä esteenä on ollut myös tunnistuspalveluiden laskuttaminen, pieniä tapahtumasummia on ollut pankeissa lähes mahdotonta tai hyvin vaikea laskuttaa. Prosesseja ja toimintatapoja on vaikea saada pienille esim. senttilaskutuksille sopiviksi ja taloudellisesti kannattaviksi. Koska sopimuskäytäntöä ei ole digitalisoitu ja automatisoitu, niin niihin liittyvät prosessit ovat olleet vaivalloisia ja kustannustehottomia..

Operaattorit ovat luoneet erillisen luottamusverkon, jossa sopimalla yhden operaattorin kanssa tunnistuspalvelusta, kolmannelle osapuolelle mahdollistetaan kaikkien operaattoreiden asiakkaiden tunnistaminen. Tämä ratkaisu on ollut tarjolla markkinoilla jo vuodesta 2007, mutta käyttö ei ole laajentunut merkittävästi. Alussa rajoitteena pidettiin verkon kuuluvuutta erityisesti sisätiloissa sekä matkapuhelintunnistukseen soveltuvien liittymien rajallista tilaajamäärää. Käyttö ei ole näidenkään esiteiden poistuttua kuitenkaan laajentunut.

Tunnistamisen markkinaosuudet ovat tällä hetkellä jakautuneet niin, että kolmen suurimman pankin asiakkaat muodostavat lähes 80% koko vahvan tunnistamisen tapahtumista, joten vahvaa tunnistamista vaativa sähköisen asioinnin kehittäminen on riippuvasta näiden pankkien mukanaolosta. Nykyinen pankkien tarjoama salasanalista ei ole sovelias vaihtoehto tabletti ja älypuhelimien käytön sekä niiden mahdollistaman mobiliteetin kasvaessa. Nykyratkaisu ei siis ole kehityksen kannalta riittävä, ja pankkienkin tulee kehittää tunnistusratkaisuaan jo omienkin palvelutarpeiden ajanmukaistamiseksi.

Aiemmat yritykset kehittää yhteistä tunnistusratkaisua eivät ole onnistuneet.
Yksi syy on vahvan sähköisen tunnistamisen rajallinen tarve. Vahvan tunnistamisen käyttötarpeet ovat keskittyneet pääosin maksamisen ja pankkiasioinnin ympärille. Vahvaan tunnistamiseen ei myöskään ole ollut uusia, käyttäjäystävällisiä ja kustannustehokkaita palveluita joista vahvaa tunnistusta olisi ollut saatavilla.

Yksityisellä sektorilla, markkinoilla olevat käyttäjille helpot kevyet tunnistustavat ovat sen sijaan erittäin laajasti käytössä. Vahvan ja kevyen tunnistamisen tarpeen rajaaminen sekä myös yhteensovittaminen on haaste. Nyt esitetyssä lainsäädännössä ei ole otettu mitenkään huomioon eritasoisten tunnistustapojen palveluita ja porrastuksen hyödyntämistä palveluissa. Vahvan tunnistamisen tasomääritelmät sekä erityyppisten porrastusvaihtoehtojen hyödyntämiseen liittyvät mahdollisuudet olisi tullut ottaa huomioon lakia suunniteltaessa.

Ruotsissa on kokeiltu BankID:n ympärille rakennettuja luottamusverkostoja viisitoista vuotta. Siellä sähköinen asiointi ei ole yhtä laajasti levinnyttä kuin Suomessa rakenteiden teknisten monimutkaisuuksien takia. BankId testasi myös pankkien ja operaattoreiden välistä luottamusverkkoyhteistyötä johon rakennettiin kiinteät hinnoittelumallit sekä erilliset säännöllisesti toteutettavat auditointitavat. Tässä mallissa epäonnistuttiin, sillä säätelemällä hintoja, rakentamalla vaatimuksia ja kustannuksia sekä luomalla velvollisuuksia liiketoimintaosapuolille, luotiin ekosysteemi joka ei toiminut yksityisillä markkinoilla.

Lausunto

FISC ry kiittää mahdollisuudesta lausua hallituksen esityksestä vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain muuttamisesta ja valtioneuvoston asetuksesta.

Nyt tehty lakiehdotus esittää uuden vaihtoehdon tunnistamisluottamusverkoista. Luottamusverkkoihin liittyminen on vapaaehtoista. Verkoston jäsenellä on kuitenkin lukuisia velvoitteita. Velvoitteet koskevat teknisiä ja kaupallisia asioita. Nämä vaatimukset ja määritykset muodostavat luottamusverkossa toimijoille huomattavia taloudellisia riskejä. Teknisesti luodaan yhteensopivuuteen auditointeihin ja testauksiin merkittäviä rasitteita, joiden kustannusvaikutuksia ylitoimialarajojen mahdotonta arvioida. Lisäksi eIDAS turvatasojen määrittely asettaa huomattavasti epävarmuutta. Laki pyritään asettamaan nyt voimaan vaikka eIDAS työ on pahasti vielä kesken.

Luottamusverkolle asettaan laissa hintasäännöstely, jolla rajoitetaan verkon jäsenten väliset tunnistustapahtumat enimmillään 1 sentin hintaisiksi. Tämä aiheuttaa jo teknisesti ja kaupallisesti haasteita laskutuksen ja tunnistustransaktioiden hallinnan kautta, joissa kulut muodostuvat korkeammiksi kuin taloudelliset hyödyt. Tunnistusverkossa on oltava luotettava tapa todentaa luottamusverkon yli menevät tapahtuma, joten teknisesti on oltava kattava järjestelmä logitukselle ja raportoinnille. Tästä aiheutuu huomattavat lisäkustannukset. Luottamusverkossa on myös velvoite VTJ-järjestelmän käytöstä jokaisen tapahtuman yhteydessä aiheuttaen teknistä ja kaupallista rasitetta.
Laki rajaa myös luottamusverkossa ensitunnistamiseen liittyviä hintarajoituksia, jotka toimivat yhtenä liiketoimintaa rajoittavana tekijänä luottamusverkon jäsenille.

Tehdyn lakiehdotus suurin uhkakuvana on se, että esimerkiksi suuret pankit eivät osallistu luottamusverkon toimintaan. Näin ajaudutaan tilanteeseen jossa vahvaksi tunnistamiseksi on joko hyväksyttävä pankkien TUPAS-tunnistus myös tulevaisuudessa jotta ihmiset eivät palaa fyysisesti valtion virastojen tiskeille. Mikäli pankit eivät ole mukana ja jää luottamusverkolle käyttökohteita pankki- ja maksamismaailman ulkopuolelta hyvin vähän. Jos tämä hyvinkin realistinen uhkakuva toteutuu, jää luotu laki malliksi kuinka julkisten palveluiden vahvaksi sähköiseksi tunnistamiseksi. Tällöin luottamusverkon toimijoille jäisi vain hyvin pieni liiketoimintakenttä operoitavaksi.

Liiketoiminnallisesti laissa esitetty hintasäännöstely johtaa tunnistustapahtumien tapahtumamaksujen keräämiseen lopulta suoraan kansalaisilta.

Yksityisellä palvelusektorilla ei oteta uusia teknisiä palvelurajapintoja helposti käyttöön korkeiden integraatiokustannusten takia. Taloudelliset hyödyt hintasäännöstelystä eivät ole yksityiselle sektorille kovin merkittäviä. Yksittäisen tunnistustapahtumahinta ei ole merkittävä tekijä palveluissa, joissa asiakkaat asioivat vahvasti tunnistaen vain muutamia kertoja vuodessa.

Yksityisellä sektorilla pankki- ja maksupalvelut ovat ainoastaan vahvaa tunnistamista laajasti vaativia sektoreita, joissa tapahtumahinnalla voi olla suuremmin merkitystä. Muissa palveluissa kevyemmät ja palvelukohtaiset tunnistusratkaisut ovat usein riittäviä lähes kaikkien sähköistenasiointipalveluiden toteuttamiselle.

Koko lakiesitys vahvasta tunnistamista perustuu arvioihin, joissa sähköinen vahva tunnistaminen tarjoaisi merkittävää liiketoimintaa, ja että tunnistamiseen olisi

palvelurakenteiden arvoketjussa käytettävissä huomattavasti pääomia. Tälle olettamalle ei ole kuitenkaan lähitulevaisuudessa perusteita ja tunnistaminen on kuitenkin palvelurakenteissa vain pieni toiminnallisuus joka on vain oltava kunnossa.

Lakiesityksessä säädetään Viestintäviraston toiminnasta joka asetuksella ottaa yksin vallan markkinoiden säännöstelylle. Viestintävirasto voi vapaasti halutessaan muuttaa hintoja ja teknisiä vaatimuksia ulottaen vaikutukset kaikille luottamusverkkoon kuuluville. **Tämä on huomattava ennalta arvaamaton liiketoimintariski kaikille luottamusverkkoon liittyville.** Hinnoittelu luottamusverkostossa tulisi rakentua luottamusverkon jäsenten väliseen sisäinen päätökseen. Lisäksi luottamusverkoston liiketoimintamallit tulisi jättää verkoston itsensä määriteltäväksi. Viestintäviraston toiminta voisi keskittyä ainoastaan teknisten laatuvaatimusten toteutumiseen sekä luottamusverkoston virallisen jäsenrekisterin ylläpitämiseen.

Laki määrittelee VTJ-järjestelmästä uuden tunnistusveromekanismin markkinoille ja siitä voi muodostua myös tekninen pullonkaula käytettävyydelle. VTJ:n rooli on tulkittavissa uutena tunnistusverotuksena luottamusverkonjäsenille. **VTJ-käyttö tulisi olla jokaisen tunnistuspalvelua tuottavalle täysin ilmaista ja sen käyttö tulisi olla kullekin jäsenelle tarvepohjaista, se voisi olla määrällisesti tehtävä kerran puolessa vuodessa varmistaakseen tietojen ajantasaisuus.**

Vastustamme vahvasti laissa kuvattuja tapoja joilla julkinen sektori tulee tämän lain puitteissa osaksi kilpailemaan omilla proxy-ratkaisulla yksityisen sektorin vastaavien palveluiden kanssa ja samalla lisäämällä työpaikkoja julkiselle sektorille.

Lakiesityksessä on hyvä se, että siinä puretaan vahvan tunnistamisen ketjuttamisen rajoitteet. Vastuurakenteet olivat rajoitteena uusien palveluiden syntymiselle ja erityisesti uusien tunnistusvälineiden markkinoille tuomiselle. Nyt esitetty laki ehdotus ketjuttamisesta on markkinoille sopivampi tapa hallita vastuita.

Suositukset jatkotoimille

Vahva sähköinen tunnistaminen voisi parhaimmillaan olla Suomelle keskeinen kilpailukykytekijä, jonka avulla liiketoimintojen digitalisoituminen ja julkiset digitaaliset palvelut saisivat tärkeän rakennuspalikan, jota muualla ei vielä ole. Lakitasolla voidaan vaikuttaa ainakin seuraaviin vahvan sähköisen tunnistamisen edellytyksiin:

1. Vapaa kilpailu
2. Kustannukset
3. Kehityksen jatkuminen Suomessa.

Lakitasolla tulisi varmistaa, että uudet tarjokkaat voivat toteuttaa ratkaisunsa yhteensopivina olemassa olevien toimijoiden kanssa, jotta integroinnit palveluntuottajiin olisivat mahdollisimman helppoja. Jos uusia luottamusverkostoja muodostetaan, myös niiden kanssa pitäisi voida mahdollisimman helposti toteuttaa yhteensopivuus, vaikka ei olisi verkoston jäsen.

Tällä hetkellä ensitunnistuksen hankaluus ja kalleus on huomattava kustannuksia nostava tekijä. Lakiehdotuksen ajatus ensitunnistuksen tekemisestä ketjuttamalla olemassa olevia

tunnistusvälineitä on ehdottomasti kannatettava edellyttäen että vastuurakenteet osapuolten välillä ovat selkeitä. Lisäksi tulisi huolehtia, että jatkuvan tunnistuksen kustannukset eivät karkaa käsistä. Siksi suhtaudumme kielteisesti esimerkiksi lakiehdotuksen VTJ-kyselyn pakollisuuteen.

Laki- tai asetustasolla ei kuitenkaan tulisi määrätä hintoja eri tapahtumille tai toimijoiden välille. Oleellista on, että tunnistuspalvelujen tarjoajat kohtelevat kaikkia sidosryhmiä samalla tavalla eli että esimerkiksi tunnistamisen ja sen ketjuttamisen hinnat ovat kaikille toimijoille samat.

Tällä hetkellä kehitys vahvan tunnistamisen alueella Suomessa on pysähtynyt yli 10 vuotta sitten kehitetyn Tupas-tunnistamisen tasolle. Yksi käytännön este Tupaksen kehittymiselle on kilpailulainsäädäntö. Suuri markkinaosuus ei mahdollista uusien versioiden tekemistä verkoston toimijoiden kesken, vaan verkosto pitäisi hajottaa ja toimijoiden tehdä omat uudet ratkaisunsa. Tämä ei ole kansantaloudellisesti järkevää. Tämä pitäisi ottaa huomioon lakiehdotuksessa, jotta Tupaksesta voidaan kehittää uusi, nykyaikainen versio yhteistyössä kaikkien alan toimijoiden kanssa. Samalla voidaan edistää muiden luottamusverkostojen syntymistä sen rinnalle, esimerkiksi valtion toteuttama luottamusverkosto on ehdottomasti kannatettava asia, mikäli sillä lisätään vapaata kilpailua markkinoilla. Rinnakkaisissa verkostoissa on huolehdittava siitä, että verkostot voivat teknisesti toimia yhteensopivasti.

Nyt laadittu lakiesitys muokkaa markkinoita ja toimintatapoja aivan liian radikaalisti. EU:ssa eIDAS säädökset tulevat kuitenkin vaikuttamaan erittäin laajasti kansalliseen toimintaan. Ennen kuin eIDAS vaatimukset ovat vahvistettu, ei lakiin tulisi tehdä muita muutoksia kuin vahvan tunnistamisen ketjuttamisen liittyvät muutokset.

Nyt suunniteltuja uudistuksia ja niiden mahdollisia markkinavaikutuksia tulisi tutkia ja arvioida laajemmin. Lakiehdotuksen mukaista toimintaa voisi testata nyt rajoitettuna pienimuotoisena pilot-mallina. Saatuja tuloksia yhdessä lopullisten eIDAS vaatimusten kanssa voisi soveltaa tulevassa lopullisessa tunnistamiseen liittyvässä lain säädännössä.

Lainsäädännössä tulisi erityisesti keskittyä Suomen kilpailukyvyn parantamiseen ja sähköisen asioinnin edistämiseksi. Nyt tulisi hakea laajemmin paremmin keinoja joilla todellisuudessa saataisiin markkinat toimimaan joustavammin ja luomaan uusia palveluita edistäen lopulta yhteiskunnan digitaalisuutta. Nämä tavoitteet jäävät tässä laki esityksessä kokonaan toteutumatta. Suomessa ei kannattasi lähteä luomaan hyvin monimutkaista kokonaisuutta sähköisen tunnistamisen markkinoista. Meillä ei ole yksikertaisesti varaa ylimääräiseen byrokratiaan. Jo nyt meneillään ollut lainsäädäntötyö on hidastanut tai jopa pysäyttänyt markkinakehityksen kokonaan vahvan tunnistamisen sekä siihen liitettyjen palveluiden osalta. Lakiesityksessä suunnitellaan rakenteita, joista on osaksi jo näyttöä muilta markkinoilta epätoimivuudesta. Lisäksi laki luo valtiohallintoon uusia hallinnollisia rakenteita sekä lukuisia uusia prosesseja, joilla kasvatetaan yhteiskunnallisia kustannuksia, rasitteita palvelutuottajille sekä kustannuksia palveluita käyttäville. Tämä lisää verorasitteita yhteiskunnallisesti valtiokeskeisen hallinnoin ja valvonnan kautta kun pitäisi kulkea päinvastaiseen suuntaan purkaen näitä rakenteita.

Nyt esitetty laki tulee oletettavasti jakamaan markkinat kahtia, kuten on tapahtunut esimerkiksi sähköisessä laskutuksessa, jossa on käytännössä erillinen pankkiverkko sekä sähköisenlaskutuksen operaattoriverkko toimien erillään toisistaan. Kahtia jakautuminen ei helpota markkinoita vaan kasvattaa kustannuksia koko maan sähköisten palveluiden kehitykselle nyt ja tulevaisuudessa.

FISC Finnish Information Security Cluster

Lisätietoja

Toiminnanjohtaja Juha Remes, juha.remes@cyberlab.fi

sekä

Hallituksen puheenjohtaja Timo Kotilainen, timo.kotilainen@cyberlab.fi