

Microsoftin lausunto hallituksen esityksen luonnokseen vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain muuttamisesta

Microsoft Oy kiittää mahdollisuudesta lausua valtiovarainministeriön ja liikenne- ja viestintäministeriön yhteistyönä valmistelemasta muutoskokonaisuudesta vahvasta sähköisestä tunnistamisesta annettuun lakiin ja tähän liittyvästä valtioneuvoston asetuksesta.

Yleisenä huomiona voidaan todeta, että kaikilla sähköisten palveluiden käyttäjillä on useita sähköisiä identiteettejä ja näin tulee olemaan myös jatkossa. Eri toimijat valitsevat palveluihinsa ratkaisut tasapainottaen tunnistamisen helppoutta ja turvallisuutta tarpeidensa mukaan. Tarpeeseen nähden turhan vahvojen tunnistamisratkaisujen käyttö ei tue tietoyhteiskuntakehitystä. Suositeltavampaa olisi tarjota helppokäyttöisiä palveluita, joissa käyttäjältä edellytetään toimenpiteen oikeusvaikutuksen kannalta riittävää sähköisen tunnistamisen tasoa.

Yhteenveto

- Esitysluonnoksen ytimenä oleva luottamusverkosto on nykyaikainen ja järkevä tapa kehittää vahvan tunnistamisen markkinan toimintaa.
- Esityksessä ei ole selvitetty kattavasti mahdollisuutta luottamusverkoston luomiseen muilla keinoin kuin läinsäädännöllä.
- Esityksessä ei kuvata eikä oteta riittävästi huomioon nykytilannetta, esimerkiksi kansainvälisiä vahvan sähköisen tunnistuksen tarjoajia ja maksupalvelujen tarjoajia.
- Muutosesityksellä ei välttämättä saavuteta esitettyjä tavoitteita.
- Esitysluonnoksen toteuttaminen loisi teknisen riskikeskittymän ja viranomaisille uusia tehtäviä, joita ei ole otettu huomioon arvioitaessa esityksen vaikutuksia.
- Esityksen kielelliseen selkeyteen ja väärintulkintojen vaaran vähentämiseen on syytä kiinnittää huomiota.
- Parempaan lopputulokseen päästäisiin muuttamalla lakia vasta asiaa koskevan EU-asetuksen yksityiskohtien työstämisen jälkeen.

Muutosesityksellä on hyvä tarkoitus

Esitysluonnoksella tavoitellaan

- 1) jokaiselle kansalaiselle mahdollisuutta sähköisesti todennettuun henkilöllisyyteen ja sen käyttöön,
- 2) vahvaan sähköiseen tunnistamiseen perustuvan palvelutuotannon kehittymistä ja
- 3) sähköisen tunnistamisen markkinaehtoista kehittymistä.
- 4) uusien tunnistamisvälineiden käyttöönoton helpottamista

Vahvalla sähköisellä tunnistusvälineellä tulisi kyetä asioimaan kaikissa niissä yksityisen sektorin palveluissa, joissa vahva tunnistaminen on välttämätöntä ja kaikissa julkisen sektorin tuottamissa palveluissa. Tavoitteena näyttää itse asiassa olevan tietoturvallisuuden parantaminen siirtymällä käyttämään nykyistä vahvempia tunnistamisen ratkaisuja. Tavoitteet ovat kannatettavia.

Tavoitteisiin pyritään säätämällä tunnistuspalvelujen tarjoajien luottamusverkostosta ja pakollisesta tunnistamistietojen välittämisestä luottamusverkostoon kuuluvien toimijoiden kesken. Sähköisten palvelujen tuottajan ja palvelujen käyttäjän tarvitsisi ainakin periaatteessa tehdä sopimus vain yhden toimijan kanssa. Sähköisten palvelujen tuottaja kuitenkin edelleen voisi itse määritellä mitä tunnistuspalveluita hyväksyy.

Periaatetasolla on puutteita

Luonnoksessa ei käsitellä eräitä tärkeitä periaatteita, kuten sitä, että tunnistamisen vahvuuden tulisi olla suhteellista verrattuna suoritettavan toimenpiteen oikeusvaikutuksiin tai yksityisyydensuojan säilyttämiseen välttämällä tarpeetonta tunnistautumista.

Nykytilan kuvauksesta puuttuu olennaisia seikkoja

Esitysluonnoksessa ei ole kuvattu sähköisten palveluiden kirjoa riittävästi eritellen eikä nykytilannetta ole kaikilta osin kuvattu kattavasti. Nykytilan osalta todetaan, että *verkkokaupoissa, erilaisilla keskustelupalstoilla ja vastaavilla käytetään tapauskohtaisia ratkaisuja ja yleisesti heikkoa sähköistä tunnistamista*, siis käyttäjätunnusta ja salasanaa sekä käyttäjän itsensä antamia henkilötietoja.

Vahva tunnistaminen verkkokaupassa ei ole välttämätöntä toisin kuin esityksessä esitetään. Verkkokaupoissa käytetään useita erilaisia maksutapoja ja vain osassa näistä käytetään vahvaa sähköistä tunnistusta. Maksutavan ja sen edellyttämän tunnistamisen aiheuttamien kustannusten optimointi on osa verkkokaupan riskienhallintaa. Verkkomaksuna maksettaessa maksaja tunnistautuu vahvasti verkkopankissa. Näin toimitaan nykyaikaisen tietoturvaparadigman mukaisesti, vain välttämätön suojataan ja se suojataan riittävän hyvin.

Esitysluonnoksessa ei oteta huomioon sitä, että verkkomaksamiseen, verkkokauppojen syntymisen helpottamiseen ja sopimusten hallintaan on syntynyt palveluja, kuten Klarna, Suomen Verkkomaksut ja CheckOut. Näitä käyttävät useat verkkokaupat. Huomiota kiinnittää se, että näiltä palvelutuottajilta ei ole pyydetty lausuntoja. Pienyritys tarvitsee siis yhden sopimuksen verkkokauppaansa varten ja markkinoilla on kilpailua. Tältä osin esitysluonnoksen perusteluissa esitetyt tiedot eivät näyttäisi pitävän paikkaansa.

Erilaisilla keskustelupalstoilla ja vastaavilla käytetään esitysluonnoksen mukaan yleisesti heikkoja sähköisiä tunnisteita. Monissa tapauksissa tämä on myös palvelun käyttäjien intressi. Luonnoksessa ei mainita eikä käsitellä sitä, että monissa tapauksissa verkkosivustot tarjoavat myös mahdollisuuden käyttää vahvaa sähköistä tunnistautumista, mikäli käyttäjä kokee sellaisen aiheelliseksi. Tällaista mahdollisuutta tarjoavat ainakin Facebook, Google ja Microsoft. Kaikkien näiden kaksivaiheinen tunnistus täyttää lain mukaiset vahvan sähköisen tunnistautumisen tunnusmerkit ja kunkin ympärille on syntynyt suuri kansainvälisten palvelujen verkosto käyttämään tunnistautumispalvelua.

Vahva tunnistautuminen on välttämätöntä yksityisen sektorin palveluissa vain lain niin edellyttäessä. Kaikissa tällaisissa sähköisissä palveluissa (vakuutuspalvelut, pankkipalvelut, sijoituspalvelut, telepalveluiden hankinta) käytetään jo vahvaa tunnistautumista, joten tavoite on siltä osin toteutunut.

On toki huomattava, että joillakin toimialoilla, kuten energiatoimialalla, väärinkäytösten määrä on niin vähäinen, että ei ole katsottu tähän mennessä laajasti tarpeelliseksi toteuttaa vahvaa tunnistautumista sähköisissä palveluissa, esimerkiksi solmittaessa sähköisistä sopimuksista verkkopalvelussa. Energiatoimialan käytäntö onkin yhdenmukainen fyysisessä ja digitaalisessa maailmassa.

Esitysluonnoksen pedanttinen tulkinta saattaa vaarantaa yksityisyydensuojan

”Vahvalla sähköisellä tunnistusvälineellä tulisi kyetä asioimaan ... kaikissa julkisen sektorin tuottamissa palveluissa.” Virkkeestä jää satunnaiselle lukijalle helposti sellainen mielikuva, että kaikissa julkisen sektorin palveluissa tavoitellaan vahvaa tunnistautumista. On valitettavaa, että luonnoksesta puuttuu maininta siitä, että monissa palveluissa tulee voida asioida tunnistautumatta, mikä on yksityisyydensuojan ja oikeusturvan toteutumisen kannalta välttämätöntä. Nykyisten tunnistusvälineiden käytön laajentaminen kaikkiin julkisiin palveluihin esimerkiksi opetussektorille aiheuttaisi todennäköisesti ylimääräisiä tarpeettomia kustannuksia sekä julkiselle toimijoille että tunnistuspalveluiden tarjoajille. Nykyiset tunnistautumisvälineet eivät välttämättä myöskään sovellu käytettäväksi palveluissa, joissa kirjautumistapahtumia voi tapahtua käyttäjää kohti useita päivässä.

Kun julkisen hallinnon sähköinen palvelu hakee väestötietojärjestelmästä tai muusta rekisteristä asiakkaan tietoja helpottaakseen asiointia ja vähentääkseen asiakkaan hallinnollista taakkaa, vahva sähköinen tunnistautuminen on välttämätöntä. Palveluita tulisi kuitenkin voida käyttää tunnistautumattakin silloin kun se palvelun luonteen vuoksi on mahdollista.

Julkishallinnon tunnistamiseen liittyvien sopimusten hallinta korostuu

Esitysluonnoksessa tuodaan seitsemään kertaan esiin, että julkishallinto joutuu hallinnoimaan kohtuuttoman paljon sopimuksia tunnistuspalveluiden tarjoajien kanssa. Näitä sopimuksia on esitysluonnoksen mukaan noin 1 500. Tällä tarkoitettaneen vetuma-palveluun liittyvien organisaatioiden tekemiä sopimuksia, joissa valtiovarainministeriö on jollakin tavalla osallisena.

On luonnollista että vetuma-palvelun käyttöönottovaiheessa sopimusten solmimisen osuus on korostunut työtehtävissä. Yhden sopimuksen käsittelyn työmäärä lienee muutamista tunneista korkeintaan muutamiin päiviin. Sopimusten hallinnan työkustannukset lienevät joitakin satoja tuhansia euroja vuodessa. Toiminnan tehokkuutta voidaan parantaa ja kustannuksia vähentää hallinnon prosessien kehittämisellä ja tarkoituksenmukaisilla sopimusjärjestelyillä. Siihen ei tarvita lain muutosta.

... mutta tavoitteita ei tällä esityksellä saavuteta

Esityksellä ei luoda kaikille kansalaisille mahdollisuutta sähköisesti todennettuun henkilöllisyyteen henkilöllisyyteen. Esitys ei takaa luottokelvottomien, vähävaraisten tai kansalaisuudettomien henkilöiden mahdollisuutta käyttää vahvaa tunnistamista vaativia palveluita kohtuukustannuksin.

Runsaasta 400 miljoonasta vuosittaisesta pankkitunnistein tehdystä tunnistustapahtumasta ja muutamista kymmenistä tuhansista mobiilitunnisteella tai HST-kortilla tehdystä tunnistustapahtumasta yli 85 % on finanssipalveluihin tunnistautumiseen ja pankkimaksamiseen liittyviä tapahtumia. Julkisen hallinnon palveluihin tunnistaudutaan vuosittain vajaa 20 miljoonaa kertaa.

Mikäli esitysluonnoksesta tulee laki, lain voimaantulon jälkeen edelleenkin kukin pankki voi edelleen hyväksyä vain omat pankkitunnisteensa. Tunnistustapahtumista on edelleen yli 85 % pankkitunnistein tehtyjä finanssipalveluihin tunnistautumisia. Markkina ei muutu.

Parantaako esitysluonnos mahdollisuuksia kehittää vahvaan sähköiseen tunnistamiseen perustuvien palvelujen tuotantoa. Parantaa, mutta samaan tulokseen voitaisiin päästä ilman lakimuutostakin.

Esitysluonnoksen toteuttaminen loisi uuden riskikeskittymän

Esitysluonnoksen 7§ vaatimus jokaisen tunnistustapahtuman varmistamisesta Väestörekisterikeskuksen palvelusta voi johtaa siihen, että ko. palvelun vikatilanne tai palvelunestohyökkäys voi lamaannuttaa kaiken vahvan sähköisen tunnistamisen koko Suomessa. Tällaisen yksittäisen loogisen ja teknisen yhdyspisteen määrittäminen yhteiskunnan kriittiselle infrastruktuurille ei ole suositeltavaa. Esitysluonnos luo viranomaisille uusia tehtäviä, mutta vaikutusarviossa niitä ei oteta huomioon

Vahvan sähköisen tunnistamisen palvelut ovat pääsääntöisesti yksityisen sektorin tuottamia palveluja. Tässä esityksessä viranomaisille luodaan uusia tehtäviä, joiden toteuttaminen voi aiheuttaa nykyisille toimijoille uusia kustannuksia.

Viestintävirastolle ollaan myös määrittämässä sellaisia uusia tehtäviä, joihin sillä ei ainakaan nyt ole resursseja. Näiden uusien tehtävien resurssointi ja rahoitus olisi syytä kuvata esityksen taloudellisissa vaikutuksissa, koska tehtävät ovat luonteeltaan pysyviä.

Esityksessä todetaan, että varmennustapahtuman olisi tarkoitus olla maksuton. Korkean käytävyyden tietoturvallisten palvelujen tuottaminen aiheuttaa aina merkittäviä kustannuksia. Esityksestä olisi käytävä ilmi kuinka tällainen palvelu resursoidaan ja rahoitetaan.

Esityksessä ei oteta kantaa, ei myöskään asetusluonnoksessa, Väestörekisterikeskuksen palveluiden palvelutason määrittämiseen. Ilman palvelutasolupausta kaupallisten toimijoiden on vaikea sitoutua käyttämään palvelua. Palvelutason tulee lisäksi olla sellainen että kaupallisten toimijoiden on mahdollista taloudellisesti järkevästi täyttää omat palvelulupauksensa.

EU-asetuksen voimaantulon vaikutuksia ei oteta riittävästi huomioon

Tunnistamispalveluja koskevan EU-asetuksen toimeenpano on käynnissä ja vaatimukset tarkentuvat kesään 2015 mennessä. Vaikka esitysluonnoksessa on todettu, että sen ja EU-asetuksen välillä ei ole päällekkäisyyksiä ja että aikataulut on sovitettu yhteen. Asetuksen implementointi tulee aiheuttamaan nykyisille tunnistuspalveluiden tuottajille joka tapauksessa kustannuksia. Kokonaisuuden kannalta saattaisi olla tarkoituksenmukaisempaa keskittyä nyt osallistumaan aktiivisesti Suomen tavoitteiden saavuttamiseen ja muuttaa kansallista lainsäädäntöä vasta kun EU-asetuksen kaikki yksityiskohdat ovat tiedossa. Tällä tavoin vältettäisiin tarpeettomien kustannuksien syntymistä tunnistuspalveluiden tarjoajille. Vaarana on se, että vahvan sähköisen kustannusten noustessa kynnys niiden käyttöönottoon kohoaa entisestään.

Kieliasua kannattaisi hioa väärinkäsitysten vaaran vähentämiseksi

Luonnoksessa on useissa kohdin yhdistelty samaan kappaleeseen asioista, joilla ei ole keskenään tosiasiallista yhteyttä. Satunnainen tottumaton lukija yhdistelee mielessään asiat helposti yhteenkuuluviksi. Paremmen sääntelyn ohjelman tavoitteiden mukaisesti esitysluonnoksen kieliasua tulisi selkeyttää ja korjata kohdat, joissa väärin tulkintojen vaara on ilmeinen. Tällaisia ovat muun muassa:

- Sivulla 4 julkisen hallinnon sopimusten määrän ja pienyritysten aseman rinnastaminen
”Valtiovarainministeriössä on arvioitu, että näitä sopimuksia on tehty noin 1500, joista suurin osa

eri pankkiryhmien kanssa. Pienille yksityisen sektorin toimijoille koituu kohtuuttomia kustannuksia tällaisesta määrästä sopimuksia.”

- Sivulla 9 julkisen hallinnon kustannusten ja verkkopankkitunnistusten kokonaismäärän esittäminen *”Julkisen hallinnon sähköisissä palveluissa käytettyjen tunnistuspalveluiden yhteenlaskettu kustannus on tapahtumamääristä riippuen noin 4-6 miljoonaa euroa vuodessa. Verkkopankkisopimuksia on noin 5,5 miljoonaa ja verkkopankkitunnistuksia noin 400 miljoonaa vuodessa.”*
- Sivulla 14 taloudellisissa vaikutuksissa on kustannuksina esitetty sekä pankkien saamia maksuja että pankkien maksamia maksuja

Lisäksi tekstissä on ristiriitaisuuksia, esimerkiksi:

- Sivuilla 3 ja 4 todetaan että *”Henkilökorttiin liitettyä kansalaisvarmennetta on mahdollista käyttää osassa julkisen hallinnon palveluita.”* ja *”Julkisen sektorin tuottamiin sähköisiin asiointipalveluihin on mahdollista tunnistautua kaikilla Viestintävirastoon ilmoittautuneiden vahvan sähköisen tunnistuspalvelun tarjoajien tunnistusvälineillä.”* Jompikumpi näistä virkkeistä ei pidä paikkaansa.