Liikenne- ja viestintäministeriölle

IKI ry:n lausunto laista sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista

Viite: Lausuntopyyntö 5.11.2008 (1862/30/2008)

Internet-käyttäjät ikuisesti IKI ry

IKI ry

Internet käyttäjät ikuisesti - IKI ry on yhdistys joka pyrkii edistämään sähköisen viestinnän edellytyksiä Suomessa. IKI ry:llä on yli 18.000 jäsentä.

Lisätietoja IKI ry:stä: <http://www.iki.fi>

Yleistä

Se, että tästä asiasta tehdään lakia varsinkin virallisiin ja tärkeisiin kaupallisiin palveluihin tunnistautumisen piirissä on hyvä asia. Myös erittely tunnistamiseen ja allekirjoituksiin on järkevä.

Pakottavaa vai vapaaehtoista lainsäädäntöä?

Lakiehdotusta voi tulkita ainakin kahdella tavalla:
1) tarkoitus on kontrolloida kaikkea sähköistä tunnistusta joka täyttää vahvan tunnistamisen tunnusmerkit,
2) tarkoitus on kontrolloida vain niitä jotka vapaaehtoisesti tekevät ilmoituksen ja haluavat käyttää nimeä "vahva sähköinen tunnistaminen".

Perusteluissa mainitaan "heikko tunnistaminen" mutta ei huomioida sitä, että monet palvelut joissa nykyään käytetään heikkoa tunnistusta ovat siirtymässä tai luultavasti lähitulevaisuudessa siirtyvät tunnistamiseen joka on teknisesti vastaava kuin lakiehdotuksen vahva tunnistaminen. Tulevatko ne tällöin lain piiriin? Ovatko tällä hetkellä käytetyt teknisesti vahvaa tunnistamista vastaavat järjestelyt (näistä enemmän alla) tarkoitettu olemaan lain piirissä?

Jos tarkoitus on 1) pakottava kontrolli, silloin lakiehdotuksen teksti tuo lain määräysten piiriin sellaisiakin toimintamalleja joista ei ole järkevää määrätä noin raskaita maksu- ja vastuuseuraamuksia. Alla esimerkkejä tällaisista ratkaisuista.

Jos tarkoitus on 2) vapaaehtoinen kontrolli, silloin on mahdollista että
- poislukien muutamat nykyiset suuret toimijat, muut tunnistamispalveluiden tarjoajat eivät ilmoittaudu lain piiriin välttääkseen suuret maksut ja vastuut, vaikka heidän tarjoamansa palvelu olisikin käytännössä "vahvaa tunnistamista" vastaava.
- Jos kuitenkin vain lain mukainen vahvan tunnistamisen tarjoajan palvelu kelpaa tiettyihin erityisen tärkeisiin palveluihin (viranomaiset, pankit, ym) silloin laki saavuttaa kuitenkin keskeiset tavoitteensa ilman että häiritään liikaa muuta tunnistusta verkossa.

Mielestämme tämä perusasia pitäisi erittäin selvästi ilmaista itse lain tekstissä ettei jää tulkinnanvarausta aluetta.

Sähköisen tunnistamisen ja allekirjoitusten kenttä on monimuotoisempi kuin lakiehdotuksen näkökulma

Lakiehdotus lähestyy tunnistamis- ja allekirjoitusasiaa lähinnä suurten pankkien, operaattoreiden, viranomaisten sekä virallisten ja tärkeiden kaupallisten palveluiden näkökulmasta. Tämä näkyy mm. suurina maksuina tahoille jotka katsotaan "vahvan sähköisen tunnistamispalvelun tarjoajiksi".

Käytössä ja tulossa käyttöön on kuitenkin myös hyvin erityyppisiä teknisesti vahvoja tunnistautumis ja allekirjoitusratkaisuja jotka perustuvat mm. ei-kaupallisiin ja verkostopohjaisiin toimintamalleihin.

Lakiehdotus nykymuodossaan saattaisi estää ja haitata tällaisten uusien ja toimivien tunnistautumismallien käyttöönottoa ja siten huonontaisi kansalaisten tietoturvatilannetta, kilpailutilannetta sekä tietoturva-alan innovointia Suomessa.

Esimerkkejä ei-kaupallisista ja erilaisista tunnistautumis- ja allekirjoitusjärjestelmistä

PGP

PGP on jo pitkään käytössä ollut vahva tunnistus-, allekirjoitus- ja salausjärjestelmä joka perustuu luottamusverkostoihin ("Web of trust") mikä on hyvin erilainen "viralliseen" keskitettyyn avainten hallintamalliin verrattuna. PGP on jo pitkään ollut sähköpostiliikenteen de-facto salaus- ja allekirjoitusratkaisu.

PGP:n mallissa on yksilöiden tekemien varmenteiden lisäksi myös organisaatioita jotka eri turvatasoja noudattaen varmentavat käyttäjien avaimia, eli toiminta ei tältäkään osin ole keskitettyä.

Lakiehdotusta voi tulkita niin että PGP-avaimia varmentava taho (allekirjoittaja) katsottaisiin "vahvan sähköisen tunnistamispalvelun tarjoajaksi". PGP täyttää sopivasti varmennettuna lakiehdotuksessa mainitut vahvan tunnistuksen vaatimukset.

Lisätietoja: <http://en.wikipedia.org/wiki/Pretty_Good_Privacy>.

PGP:tä käytetään jo esimerkiksi kaupallisiin allekirjoitusta vastaaviin palveluihin kansainvälisestikin, esimerkiksi Sveitsissä toimivan Joker.com internet-domain-rekisteröintipalvelu hyväksyy PGP-allekirjoitetut (tunnistetut) viestit asiakkaalta sopimus- ja kaupallisten asioiden suorittamiseksi automaattisesti ilman muita tarkistuksia.
Lisätietoja:
<https://joker.com/faq/content/41/159/en/how-does-the-pgp_gpg_mailinterface-work.html>

IKI PGP CA -toiminta

IKI ry on pyrkinyt edistämään viestinnän luotettavuutta ja tietoturvaa edistämällä PGP:n käyttöä sähköpostiviestinnän yhteydessä, käytännössä tarjoamalla luonnollisten henkilöiden (tunnistettujen IKI ry:n jäsenten) PGP-avainten varmentamista (allekirjoittamista) jo yli kymmenen vuoden ajan, vuodesta 1998 alkaen.

Tämä tarkoittaa että kaikki PGP:n käyttäjät voivat melko hyvin luottaa iki-jäsenten PGP-allekirjoituksiin jos niissä on IKI PGP CA:n allekirjoitus. IKI ry:tä pidetään varsin luotettavana tahona tällaisissa asioissa. Toiminta ei ole yhteisön sisäistä vaan kattaa kaikki PGP-käyttäjät. Kaikki tämä on tehty vapaaehtoistyönä ilman kaupallisia tavoitteita.

Lisätietoja:
- IKI PGP CA -toiminnan julkistaminen yhdistyksen jäsenlehdessä 13.2.1998
  <http://www.iki.fi/iki/ikitotuus-6.html#IKIPGPCA>
- IKI PGP CA:n ohjesääntö ja toiminnan tarkat tiedot
  <http://www.iki.fi/iki/avaimenhaltija/avaimenhaltija-ohje.html>.

IKI PGP CA-ohjesääntöä on pidetty esimerkillisenä tällaisen vapaaehtoistoiminnan ohjeistuksena.

OpenID

OpenID on yleistyvä "single sign on" -ratkaisu internetissä joka on suunniteltu vartavasten niin että tunnistautumispalvelua voi tarjota kuka tahansa. OpenID:tä käytetään esimerkiksi monien "vähemmän turvakriittisten" www-palveluiden ja blogien tunnistautumis- ja rekisteröintiratkaisuna. Teknisesti se on kuitenkin sopivasti toteutettuna yhtä vahva kuin lakiehdotuksessa mainittu "vahva sähköinen tunnistautuminen".

Lakiehdotusta voi tulkita niin, että OpenID-tunnistamispalvelun tarjoaminen olisi lain mukaista "vahvan sähköisen tunnistamispalvelun tarjoamista". OpenID on sopivasti toteutettuna käytännössä pankkitunnistamista vastaava teknisesti. Ei kuitenkaan olisi järkevää näin raskaalla lainsäädännöllä, maksuilla ja velvoitteilla estää esimerkiksi OpenID-tunnistautumispalvelun tarjoamista käyttäjille jotta he voivat sillä tunnistautua tai rekisteröityä esim. sekalaisiin www- ja blog-palveluihin.

Lisätietoja: <http://en.wikipedia.org/wiki/OpenID>.

CA-cert

CA-cert on yhteisöllinen ja verkkoluottamukseen perustuva sertifikaattien varmennusjärjestelmä joka toimii maailmanlaajuisesti. CA-cert varmantejia ("assurer") toimii myös Suomessa. CA-certin henkilöllisyystarkistus vastaa suunnilleen laissa mainitun ensitunnistuksen vaatimuksia.

Lisätietoja: <http://en.wikipedia.org/wiki/CAcert.org>

Ehdotuksia lakiehdotuksen parantamiseksi

Uusien ratkaisujen käyttöönottoa ei tulisi estää liian laaja-alaisella lailla. Ei-kaupallisten toimijoiden toimintamahdollisuudet ja erilaisten ei-virallisten palveluiden tunnistautumistarpeet ja ratkaisut pitäisi olla selvästi sallittuja ilman suuria maksuja tai raskaita velvoitteita.

Laissa tulisi hyvin selkeästi esittää rajaukset siitä mikä toiminta ei kuulu lain piiriin, koska vahingollinen innovaatioita ja käyttöönottoa estävä vaikutus ulottuu myös lain tulkinnanvaraiselle alueelle.

Tunnistautumisen käyttötarkoitus ja teknologinen ratkaisu pitäisi huomioida toisistaan erillisinä asioina.

Tunnistamisessa ja allekirjoituksissa tietoturvatarpeita on monenlaisia ja monen tasoisia laissa ajateltujen virallisten tarpeiden lisäksi. Laissa pitäisi huomioida selkeämmin nämä eri tasoiset tunnistautumistarpeet: Esimerkiksi viranomaisten ja pankkien tunnistautumistarpeet ovat korkeampia kuin jonkin www-blog-palvelun, vaikka teknisesti tunnistautumistekniikat ovat tai tulevat pian olemaan käytännössä samanlaisia.

Jos tulkintamahdollisuuksia jää siitä mikä toiminta kuuluu lain piiriin, se käytännössä haittaa tai estää ei-kaupallisten ja muiden uusien innovatiivisten ratkaisujen käyttöönoton ja saattaa

huonoimmassa tapauksessa johtaa kartelli- tai monipolitilanteisiin ja niihin liittyviin ongelmiin.

Mielestämme kansalaisten tietoturva on niin tärkeä asia ettei pidä estää innovaatiota ja joustavia toimintamahdollisuuksia eri ympäristöissä ja eri tarpeisiin rajaamalla liian tarkasti tai estämällä lailla erilaisten ratkaisujen käyttöä.

Ehdotetuista maksuista -- edistävätkö ne tärkeitä tietoturvatavoitteita?

Ehdotetussa muodossa lain voi tulkita koskevan myös monia sellaisia tahoja mitä sen ei selvästi pitäisi kattaa, mm. tässä lausunnossa mainittuja tapauksia.

Ei-kaupallisilla tai epävirallisilla toimijoilla ei ole käytännössä mahdollisuuksia lain mainitsemiin suuriin vuosittaisiin maksuihin ja muihin vaatimuksiin.

Maksut saattavat myös motivoida lain piiriin kuuluvia tai lain tulkinnanvaraisella alueella olevia toimijoita pyrkimään välttämään joutumasta lain piiriin, mikä ei ole hyvä asia tietoturvaratkaisujen käyttöönoton kannalta.

Mainitut summat ovat samaa kokoluokkaa kuin tyypillisen start-up-yrityksen koko alkupääoma jolloin tämän alan start-uppeja voisi olla vaikea perustaa Suomeen mikä ei edistä Suomen teknologista kehitystä. Suomessa on kansainvälisesti kovan tason osaamista tästä aihepiiristä eikä sen piirissä syntyvää uutta innovatiivista yritystoimintaa tulisi haitata.

Ei ole myöskään järkevää säätää lakeja joissa on vaatimuksia jotka johtavat muiden kuin suurten kaupallisten toimijoiden palveluiden sijoittamiseen Suomen tai EU:n ulkopuolelle, koska tällöin kokonaistilanne kansalaisten käyttämien palveluiden tietoturvan osalta voi jopa huonontua.

Tilannetta voi myös verrata sähköisiin passeihin ja niiden käyttöönottoon. Vaikka CA-rekisteri (ICAO Public Key Directory) on olemassa, suurin osa maista ei ole ilmoittanut avaimiaan sinne koska siitä otetaan suuri maksu. Lopputuloksena on se että sähköisten passien turvallisuus ei ole yhtään parempi kuin normaalin paperisen passin, koska sähköistä allekirjoitusta ei voida tarkistaa kaikkialla... Ylisuurella maksulla on siis estetty halutun tietoturvan toteutuminen käytännössä.
Viite: ICAO PDK

Kustannukset syntyvät nähtävästi kokonaan siitä että "Viestintävirasto joutuu pitämään yllä vahvaa sähköistä tunnistamista koskevaa tietotaitoaan jatkuvasti sekä vastaamaan vahvaa sähköistä tunnistamista käyttävien palveluntarjoajien sekä tunnistamisvälineiden haltijoiden mahdollisiin yhteydenottoihin". Tämän tietouden ylläpitoon käytettävä rahamäärä ei suinkaan kasva vaikka tunnistamispalvelun tarjoajien määrä kasvaisi.

Teknisiä ja muita kommentteja

Sivulla 14: "Julkinen ja yksityinen avain liittyvät toisiinsa monimutkaisen matemaattisen yhtälön kautta siten, että julkisesta avaimesta ei voi käytännössä johtaa yksityistä tai päinvastoin.". Tämä ei tarkkaan ottaen pidä paikkansa koska useimmissa julkisen avaimen menetelmissä yksityisestä avaimesta voi triviaalisti johtaa julkisen avaimen.

Sivulla 60 kohta "20§" allekirjoituksen luomisesta. Mielestämme olisi hyvä mahdollistaa se, että käyttäjä voi halutessaan itse luoda oman PKI-avainparinsa jonka julkisen puoliskon vahvan tunnistamisen palvelun tarjoaja sitten varmentaa. Vain näin voidaan täydellisesti varmistua siitä ettei avaimen salainen puolisko ole kenenkään muun kuin käyttäjän omassa hallinnassa. Avainten luontipaikka voi muodostua liian houkuttelevaksi kohteeksi rikollisille jos salainen puolisko avaimista on edes hetken jossain keskitetyssä paikassa.

Lausuntopyynnöistä ja valmistelusta

Pyydämme jatkossa toimittamaan vastaavissa internettiin, internet-viestintään, -valvontaan ja -tietoturvaan liittyvissä asioissa lausuntopyynnön suoraan myös Internet-käyttäjät ikuisesti IKI ry:lle. IKI ry on myös valmis ja sopiva taho osallistumaan tulevaisuudessa vastaavien asioiden valmisteluun.

Helsingissä 1.12.2008,

Hannu Aronsson
Puheenjohtaja
Internet-käyttäjät ikuisesti IKI ry

Yhteystiedot

Internet-käyttäjät ikuisesti IKI ry:
Osoite: c/o Hannu Aronsson, Lahnaruohontie 7 A 12, 00200 Helsinki
Sähköposti: iki-hallitus@iki.fi
Nettisivut: www.iki.fi

Hannu Aronsson:
Osoite: Lahnaruohontie 7 A 12, 00200 Helsinki
Puhelin: 040 500 6242
Sähköposti: haa@iki.fi