25.11.2015

Kirjaamo@lvm.fi

Liikenne- ja viestintäministeriö

Viite: Lausuntopyyntö LVM/992/03/2015

Prof-Tel Oy:n lausunto: Luonnos valtioneuvoston asetukseksi vahvan sähköisen tunnistus-palvelun tarjoajien luottamusverkostosta

Liikenne- ja viestintäministeriö on pyytänyt Prof-Tel Oy:ltä lausuntoa luonnoksesta valtioneuvoston asetukseksi vahvan sähköisen tunnistuspalvelun tarjoajien luottamus-verkostosta.

Prof-Tel Oy ei ole ollut aktiivisesti mukana nimenomaisesti tätä nyt lausuntoa koskevia asioita selvittävässä hallintamallityöryhmässä. Prof-Tel Oy on kuitenkin seurannut kyseistä työtä. Prof-Tel Oy on sen sijaan ollut aikoinaan kehittämässä Suomen mobiili-varmennepalvelua. Mobiilivarmennepalvelussa on toteutettu toimiva ja kansainvälisten standardien mukainen luottamusverkosto mobiiliympäristöön. Ks. erikseen kohta 4 jäljempänä.

Prof-Tel Oy kiittää mahdollisuudesta lausua näkemyksensä ja toteaa lausuntonaan ja näkemyksenään seuraavaa:

1. Yleistä

1.1 Aikaisempi lausunto

Prof-Tel Oy on aikaisemmin antanut lausunnon vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksesta annetun lain muuttamiseksi sekä lakiin lisättävän luottamusverkoston ohjeiksi annettavasta valtioneuvoston asetusluonnoksesta (lausunto 7.10.2014, LVM/1518/03/2014). Nuo lausutut asiat mm. luottamusverkoston osalta pätevät sinänsä edelleen eikä niitä enää tässä toisteta.

1.2 Luottamusverkoston selkeys

Erilaisia vahvoja tunnistamisvälineitä ja -palveluita tarjoavien yritysten ja niiden välisen luottamusverkoston (federointi, Circle of Trust (CoT)) varaan rakennetun vahvan sähköisen tunnistamisen tulee olla niin teknisesti ja toiminnallisesti kuin hallinnollisilta vastuiltaan ja vaatimuksiltaankin hyvin määritelty ja yksiselitteinen. Tätä vaatimusta edellyttää näkemyksemme mukaan jo se, että tunnistuslaki voi toimia viranomais-roolissa suoritettaessa oikeustoimia. Oikeustoimien lainvoimaisuutta pitää pystyä auditoimaan myös jälkikäteen.

Vaatimukset koskisivat eri toimijoiden keskinäisten sopimisten mahdollistamiseksi tunnistamisen peruspalvelujen toiminnallisia ja teknisiä minimi vaatimuksia. Lisä-vaatimuksista (esim. laajennukset) voisi sopia kahdenkeskisesti niin haluttaessa.

Mainittu periaate ohjaa mm. määritelmien selkiyttämisessä ja nykyisten tunnistusvälineiden (kansalaisvarmenne, mobiilivarmenne, Tupas-varmenne) ja assertio-rajapintavaatimusten (Saml2, OpenId) määrittelemisessä tekniikoiden ja toimijoiden välillä sekä kehitystä uusille toimijoille ja uusille tekniikoille.

Vaatimukset tulisi määritellä asetustasolla tai sopia asetuksessa määrittelyperiaatteista (määrittelyvastuu, työryhmät, aikataulut, laatutasot). Joka tapauksessa vaatimukset tulisi olla hyvin määritelty ja dokumentoitu sekä auditoitu.

2. Asetusluonnos

2 § Määritelmät

Määritelmiä tulisi selkeyttää ja pitää ne lain tasolla. Asetuksessa tulisi käyttää pääsääntöisesti vain laissa annettuja määritelmiä. Tässä tulisi harkita huomioitavaksi myös EU-direktiivien kehitys (eIDAS) ja pyrkiä käyttämään samoja määritelmiä.

Sama toimija voi esiintyä myös useissa rooleissa (esimerkiksi tunnistusvälineen tarjoaja, tunnistuksen välityspalvelun tarjoaja). Tämä tulisi huomioida määritelmissä.

Tulisi myös määritellä tunnistuspalvelun peruspalvelut siinä vaiheessa kun luottamusverkoston rajapintoja määritellään.

3 § Luottamusverkoston tekniset rajapinnat

Tekniset rajapinnat tulisi määritellä edellä kohdan 1 periaatteiden mukaisesti selkeästi ja etukäteen erikseen määriteltyjen tunnistuspalveluiden perusvaatimusten pohjalta eri CoT-toimijoiden välillä (vrt. esim. Suomen mobiilivarmennepalvelu, ks. kohta 4/liite). Rajapintavaatimusten tulisi perustua kansainvälisiin standardeihin ja niistä Suomen oloihin sovittuihin profiileihin (vrt. edelleen mobiilivarmennepalvelun FiCom-määrittelyt).

Tunnistaminen (proof of identity) toimii monien erilaisten turva- ja oikeustoimien (allekirjoitus, auktorisointi, sopimukset, sertifiointi, äänestykset, jne) ensiaskeleena ja senkin vuoksi olisi tärkeää, että ”oikeustoimiarkkitehtuuri” olisi selkeä ja että se mahdollistaisi jäsennellyn roadmapin toteutettaessa sähköisiä palveluja ja niiden oikeustoimia.

Prof-Tel Oy kannattaa selkeitä määrittelyitä eikä jättäisi toteutusta pelkästään toteuttajien implementaatioiden varaan. Tämä periaate lisäisi myös kilpailua ja läpinäkyvyyttä.

Viestintävirasto olisi oikea paikka tehdä määrittelyt.

4 § Luottamusverkoston hallinnolliset vastuut

Prof-Tel Oy kannattaa asetusluonnoksen sisältöä sellaisenaan.

5 § Luottamusverkoston hallinnolliset käytännöt

Prof-Tel Oy kannattaa asetusluonnoksen sisältöä sellaisenaan.

Prof-Tel Oy, Långhagintie 32, 02480 Kirkkonummi
045-6700 447, esa.kerttula@proftel.fi, www.proftel.fi

3. Yhteenveto

Prof-Tel Oy pitää valtioneuvoston asetusluonnosta vahvan sähköisen tunnistuspalvelun tarjoajien luottamusverkostosta (tunnistuslaki laki 617/2009, 12 a §) tarkoituksenmukaisena ja kannatettavana. Prof-Tel Oy näkee, että määrittelyissä ja teknisissä rajapinnoissa toimittaisiin selkeiden periaatteiden mukaisesti kuten edellä kohdassa 1 ja 2 on ehdotettu.

Ystävällisin terveisin

Esa Kerttula, Dr.
Prof-Tel Oy

4. Liite
Suomen mobiilivarmennepalvelun kuvaus kansainvälisessä tiedelehdessä

Prof-Tel Oy (allekirjoittanut) on tehnyt johtavaan kansainväliseen peer-reviewed tiedelehteen, *Journal of Network and Computer Applications*, artikkelin mikä kuvaa Suomen mobiilivarmennepalvelun ominaisuuksia, standardeja, käytettävyyttä ja palvelun tehokkuutta. Koska tuore artikkeli liittyy keskeisesti lausuntopyynnön asioihin muun muassa luottamusverkoston ja standardien osalta, allekirjoittanut rohkenee liittää oheen tiedot artikkelista kiinnostuneille. Prof-Tel Oy on konsultoinut Suomen mobiilivarmennepalvelun kehittämistä muutama vuosi sitten. Oheinen artikkeli syntyi osin työn tuloksista ja varmennepalvelun teknisestä dokumentaatiosta operaattoreiden (TeliaSonera, Elisa, DNA) ja FiComin sekä alan suomalaisen teollisuuden myötävaikutuksella.

Artikkeli
A novel federated strong mobile signature service—The Finnish case

Abstract
This paper describes the legal framework, architecture with standards and signature services of the new public Finnish federated strong mobile signature scheme. Mobile signatures are used, for example, for user identification and authentication, the message authentication, non-repudiation of transactions and verifying the information integrity. The service is based on mobile PKI and on the federation of security assertions using ETSI MSS standards. The service provider needs an agreement only with one operator. Then all services in the Circle of Trust may request authentication and digital signing from user even if a service provider has made an agreement with other competing operator than the home operator of the user. The signature service platform is extremely secure using strong two-factor and two-channel model. All personal security credentials are stored and the crypto-operations run in the mobile operator's tamper-proof secure element, UICC. The Finnish mobile signature service fulfils the strong identification in the Finnish 'Identification' Act. The service platform offers potentially to millions of Finnish citizens and the participating Finnish businesses convenient to use and trusted signature services on various service channels for applications hosted on the premises or in the cloud. Signature services can be used also abroad where SMS services are provided and where user's operator has a roaming agreement.