



16.5.2014

Kansallinen tunnistusmalli - taustamuistio

1 Johdanto

Hallituksen rakennepoliittinen ohjelma (29.8.2013) talouden kasvuedellytysten vahvistamiseksi ja julkisen talouden kestävyysvajeen umpeen kuromiseksi sisältää mm. ICT:n hyödyntämistä koskevia hankkeita. Rakennepoliittisen ohjelman mukaan (kohta 2.11) ”Toteutetaan viipymättä kansallinen sähköinen palveluväylä ja sähköinen tunnistautuminen kustannustehokkaasti sekä Viron yhteistyömahdollisuudet täysimääräisesti hyödyntäen” sekä (kohta 3.9.3) ”Palvelurakenteita ja toimintoja uudistetaan sekä keskushallinnossa että aluehallinnossa valtionhallinnon tuottavuuden ja vaikuttavuuden parantamiseksi”.

Talouspoliittinen ministerivaliokunta linjasi 19.11.2013, että osana kansallisen palveluarkkitehtuurin toteutusta tulee toteuttaa kansallinen sähköinen tunnistusmalli, jossa valtio takaa kansalaisen sähköisen identiteetin ja jossa tunnistusvälineitä voidaan tuottaa markkinaehtoisesti. Kansallisen sähköisen tunnistusratkaisun malli koostuu valtion ja yksityisten toimijoiden muodostamasta kokonaisuudesta, joka tarjoaa kansalaisille sähköisen identiteetin, sekä sen käyttämiseksi kansalaisille tarjottavat tunnistusvälineet ja -palvelut.

Tässä työssä on tarkoitus keskittyä luomaan kansalaisen tunnistamiseen liittyvä malli. Sen kanssa rinnakkaisia tehtäviä tulevat olemaan roolien mukainen valtuutus sekä toisen puolesta asiointi. Näistä on tarkoitus käynnistää erilliset hankkeet tai yksi hanke. Niissä ei luoda erillistä tunnistusratkaisua, vaan tunnistaminen tulee pohjautumaan tässä luotuihin ratkaisuihin.

Lisäksi erillinen tarkastelun kohde on virkamiesten ja ammattiryhmien tunnistaminen, joka tällä hetkellä perustuu erillisiin kortteihin esimerkiksi terveydenhuollossa ja sisäisessä turvallisuudessa.

2 Nykytilan kuvaus

Vahvoja sähköisiä tunnistusvälineitä vaativien sähköisten palveluiden markkinat ovat jakaantuneet pääasiassa kolmen palvelusektorin kesken: pankki- ja vakuutuspalvelut, julkisen hallinnon palvelut sekä muut yksityi-



set palvelut. Näistä volyymeiltaan merkittävimmät ovat pankki- ja vakuutussektorin sekä julkisen hallinnon tarjoamat sähköiset palvelut.

Sähköisiä tunnistuspalveluita tuottavat tällä hetkellä pankit, mobiilioperaattorit ja Väestörekisterikeskus.

Pankkitunnisteilla on merkittävin markkinaosuus käyttäjäpeitossa ja tapahutumamäärissä. Mobiilioperaattoreiden tuottama mobiilivarmenne ja Väestörekisterikeskuksen tuottama henkilökorttiin liitetty kansalaisvarmenne eivät toistaiseksi ole saavuttaneet kokonaisuudessa merkittävää markkina-asemaa. Mobiilivarmenteella on mahdollista asioida lähes kaikissa palveluissa pankkipalveluita lukuun ottamatta. Sähköinen tunnistaminen itsessään ei ole merkittävä palvelukerros, mutta sen avulla on mahdollista rakentaa monipuolisia ja personoituja sähköisiä palveluita.

Arjen tietoyhteiskunnan neuvottelukunnan yhteydessä vuosina 2008-2009 tehtiin valtioneuvoston periaatepäätös ja kansalliset linjaukset sähköisestä tunnistamisesta. Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä al-lekirjoituksista (617/2009) tuli voimaan 1.9.2009. Laissa määritellään ne vaatimukset, joita yleisesti tarjottavalle vahvalle sähköiselle tunnistamiselle Suomessa asetetaan. Lain tarkoituksena on sääntelyn avulla pyrkiä helpottamaan sähköisen tunnistamisen markkinaehtoista kehittymistä ja takamaan vapaan kilpailun pohjalta tapahtuva sähköisen tunnistamisen kustannustason alentuminen. Väestörekisterikeskuksen tuottamia tunnistuspalveluita säädellään edellä mainitun lain lisäksi laissa väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (661/2009).

Nykytilassa vahvan sähköisen tunnistamisen lainsäädäntövastuu jakaantuu liikenne- ja viestintäministeriön, valtiovarainministeriön ja sisäasiainministeriön vastuulle. Vahvan tunnistamisen toimijoiden toimintaa valvoo Viestintävirasto, joka vastaa myös yleisesti vahvaa sähköistä tunnistamista tarjoavien toimijoiden rekisteröinnistä.

Sähköisen tunnistamisen markkina on tällä hetkellä pääsääntöisesti pankkiasioinnissa ja verkkomaksamisessa, joissa tehdään valtaosa tunnistamisista. Muun kuin verkkopankkitoimintaan liittyvän tunnistamisen määrän arvioidaan kasvavan noin 30 prosenttia vuodessa. Julkinen hallinto on voimakkaasti lisäämässä sähköistä asiointia ja suurimpia toimijoita ovat muun muassa Kela, Verohallinto, sosiaali- ja terveyssektori sekä työ- ja elinkeinoministeriö.

Nykyisen lainsäädännön tavoitteena oli mahdollistaa eri tunnistustoimijoiden yhteistyö, jolla varmistetaan markkinoiden kehittyminen. Lainsäädännöstä huolimatta eri toimijat eivät ole pystyneet sopimaan keskenään laajamittaisesta sähköisten tunnisteiden vastavuoroisesta hyväksymisestä. Tämä on johtanut siihen, että sähköisten palvelutarjoajien on tehtävä sopimukset tunnistuspalveluiden käytöstä ja tekniset liittynät jokaisen pankin kanssa erikseen. Kansalaisille tämä näkyy esimerkiksi pankkikohtaisina salasanoina ja tunnuslukulistoina.

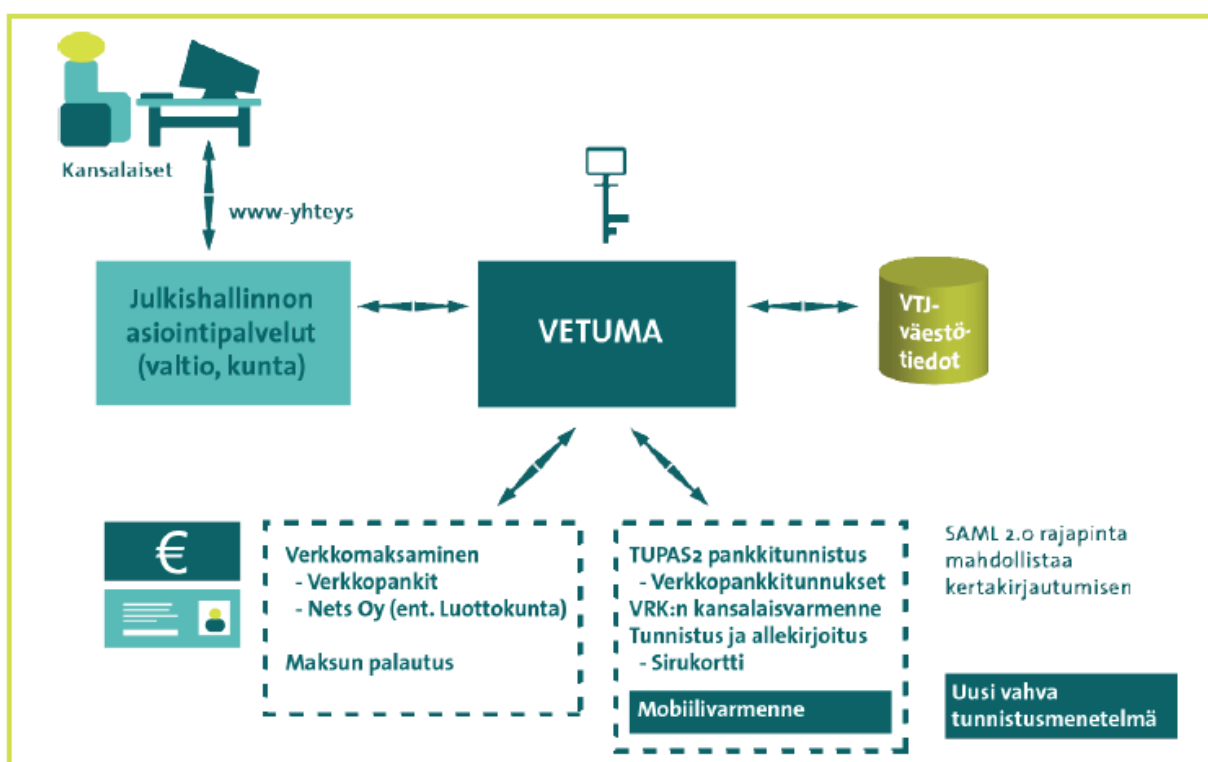
Valtiovarainministeriön johdolla toteutettavassa sähköisen asioinnin ja demokratian edistämishjelmassa (SADe) tuotetaan useita sähköisen asioin-

nin palvelukokonaisuuksia eri hallinnonaloille. Useassa SADe-ohjelmassa tuotettavassa palvelussa on tarpeen käyttäjän vahva sähköinen tunnistaminen.

Sosiaali- ja terveydenhuoltoon on tulossa lähivuosina runsaasti uusia sähköisiä asiointipalveluita, joissa tarvitaan vahvaa tunnistamista. Sosiaali- ja terveyssektorilla käsitellään usein myös salassa pidettäväksi luokiteltavia henkilöiden terveyteen tai toimeentuloon liittyviä tietoja, mikä edellyttää käyttäjien ja tietoja käsittelevien henkilöiden riittävän vahvaa tunnistamista.

Sähköistä tunnistamista tehdään runsaasti myös muussa sähköisessä asiointissa kuten verkkokaupoissa, erilaisilla keskustelupalstoilla yms., joissa käytetään paljon yrityskohtaisia ratkaisuja. Näissä käytetään yleisesti heikkoa sähköistä tunnistamista, jossa käyttäjän tietoja ei varmisteta viranomaisrekistereistä.

Julkisen sektorin tuottamiin sähköisiin asiointipalveluihin on mahdollista tunnistautua kaikilla Viestintävirastoon rekisteröityjen vahvan sähköisen tunnistuspalveluiden tuottajien tunnisteilla. Julkisella sektorilla on käytössä tällä hetkellä kaksi tunnistuksen ohjauspalvelua (Vetuma ja tunnistus.fi), jotka tarjoavat yhden teknisen rajapinnan kautta kaikki Viestintäviraston hyväksymät tunnistuspalvelut julkisten palveluiden käytettäväksi. Tunnistus.fi:n käyttäjät ovat vaiheittain siirtymässä Vetuman käyttäjäksi.



Kuva 1b Vetuma-palvelun toimintaperiaate

Yhteisöjen (organisaatiot, joilla on y-tunnus ja muut yhteenliittymät) tunnistamiseksi julkishallinnon ja julkista tehtävää hoitavien organisaatioiden sähköisiin palveluihin on tällä hetkellä käytössä Verohallinnon väliaikainen KATSO-tunnistusratkaisu. Myös siinä käytetään ensitunnistamisessa pank-

kitunnisteita, joiden perusteella myönnetään yrityksen puolesta toimintaan oikeuttavat KATSO-tunnisteet. Tämä on tarkoitus uudistaa erillisessä hankkeessa.

3 Kansallinen sähköinen tunnistusmalli

3.1 Lähtökohdat ja tavoitteet

Kansallisen vahvan sähköisen tunnistusmallin lähtökohtana varmistaa jokaiselle kansalaiselle mahdollisuus sähköisesti todennettuun henkilöllisyyteen ja sen käyttöön, vahvaan sähköiseen tunnistamiseen perustuvan palvelutuotannon kehittyminen ja sähköisen tunnistamisen markkinaehtoinen kehittyminen. Käytännössä mallin tavoitteena on varmistaa, että kansalaisen hallussa olevalla vahvalla sähköisellä tunnisteella pääsee kaikkiin yksityisen ja julkisen sektorin tuottamiin palveluihin, eikä palvelun tuottajaorganisaatio voi erikseen estää tällaisen tunnisteiden hyväksyntää. Sähköisen tunnistamisen ja sähköisten palveluiden tuottamisen markkinaehtoinen kehittyminen edellyttää riittävän vapaata liiketoimintamallia, jossa eri sektoreilla toimivat yritykset voivat kehittää liiketoimintaansa sähköiseen tunnistamiseen tai sen mahdollistamiin palveluihin liittyen. Mallin avulla tavoitellaan sellaista toimintaympäristöä, joka mahdollistaa myös Suomessa kehitettyjen sähköisten tunnistuspalveluiden markkinoinnin myös ulkomaille.

Kansallisessa kyberturvallisuusstrategian toimeenpanosuunnitelmasta:

”Toimeenpano-ohjelmaan tuotu kehittämis ehdotus sähköisen identiteetin hallintaratkaisusta liittyy palveluväyläkokonaisuuteen. Luotettava tunnistaminen edellyttää hyvää sähköisen identiteetin hallintaratkaisua, joka toimenpideohjelman esityksen mukaan kattaisi myös valtuutusten tunnistamisen sekä henkilön eri roolien tunnistamisen. Hallintaratkaisua tarvitaan kansallisen palveluarkkitehtuurin ja palveluväylän tehokkaaseen hyödyntämiseen. Tarkoituksena on taata kansalaisille turvallinen sähköinen tunnistaminen ja kehittää markkinoiden toimintaa. Tietoturvallisuuteen tulee kiinnittää erityistä huomiota. Kansalaisten tietosuojan varmistamiseksi kehitetään palvelu, jossa kansalainen voi nähdä ja hallinnoida itseään koskevien tietojen välittymistä eri organisaatioiden välillä.”

Julkisen hallinnon palvelutuotanto tapahtuu tulevaisuudessa merkittävästi sähköisten palveluiden kautta. Sähköisiin palveluihin kohdistuu suuri toiminnan tehostamispotentiaali suurivolyymisten asiointipalveluiden osalta, joissa on myös suurimmat kasvunäkymät. Julkisessa hallinnossa on käynnissä kansallisia sähköisen palvelutoiminnan kehittämishankkeita.

Julkisen hallinnon palvelutuotannon osalta sähköisen tunnistamisen kustannustehokkuus on avainasemassa. Julkisen hallinnon tuottamien asiointipalveluiden käytön pitää olla kansalaisille hyvin edullista. Perinteisessä asiointinnissa kansalaisen itsensä kustannettavaksi on jäänyt matka- tai postikulut. Julkisen hallinnon palvelujen käyttö ei saa tuottaa merkittäviä lisämaksuja kuluttajille eikä vaatia esimerkiksi kalliiden laitteiden hankkimista vain tähän tarkoitukseen.

Tehostamispotentiaalia on myös nykyisessä sähköisen tunnistamisen järjestämiseen käytetyssä hallinnointiresursseissa. Kansallisen tunnistusmallin yksi tavoite on pyrkiä merkittävästi yksinkertaistamaan vahvan sähköisen tunnistamispalvelun käyttöönottoon liittyviä sopimuksia.

Työn lähtökohtana on, että tunnistamisesta aiheutuvan kokonaiskustannustaso ei saa nousta sähköisen palvelun tarjoajille suhteellisesti nykyistä tasoa korkeammalle. Kustannusten osalta on otettava huomioon jatkuvasti lisääntyvän viranomaissääntelyn aiheuttamat muutokset sekä voimakkaasti lisääntyvän verkkorikollisuuden aiheuttamat sähköisen tunnistamisen yleiseen turvallisuuteen tehdyt panostukset.

Sähköisen todennetun henkilöllisyyden käytön aiheuttamat kustannukset kansalaiselle ja sähköisten palveluiden tuottajille pitää olla hallittavissa ja ennakoitavissa riittävässä määrin. Kansallisen sähköisen tunnistusmallin tulee mahdollistaa ja edesauttaa uusien sähköisten tunnistus- ja asiointipalveluiden kehittymistä.

3.2 Periaatteet

Jokaisella kansalaisella tulee olla tasa-arvoinen oikeus sähköisesti todennettuun henkilöllisyyteen, sen käytön mahdollistamaan tunnistusvälineeseen ja käyttöön sähköisissä palveluissa. Tunnistusmallin tulee mahdollistaa erilaisiin käyttäjätarpeisiin tuotettavat riittävän turvalliset tunnistuspalvelut. Kansallisella tunnistusmallilla vastataan myös tuleviin rajat ylittävää sähköistä tunnistamista koskeviin EU-säädöksiin.

Virallinen sähköisesti todennettu henkilöllisyys pohjautuu aina viranomaisen myöntämään virallista henkilöllisyystodistusta vasten tehtyyn fyysiseen ensitunnistamiseen tai olemassa olevan sähköisesti todennetun henkilöllisyyden avulla tehtyyn tunnistamiseen. Sähköisesti todennettuun henkilöllisyyteen liittyvät tiedot varmistetaan aina valtion ylläpitämästä väestötietojärjestelmästä. Ensitunnistuksen perusteella voidaan myöntää tunniste, johon sähköisesti todennettu henkilöllisyys liitetään. Näin myönnettyä sähköisesti todennettua henkilöllisyyttä ei voida pitää rajatun asiakasjoukon sähköisenä tunnisteena ja se voidaan ketjuttaa uusien sähköisten tunnisteiden luomiseksi.

Kansallisen mallin avulla Suomeen luodaan edellytykset vahvan sähköisen tunnistamisen markkinoiden syntymiselle ja ylläpidetään markkinoiden toimivuuden edellytyksiä. Lisäksi tavoitteena on luoda sellainen markkinaympäristö, joka mahdollistaa myös Suomen ulkopuolelle sopivien tunnistuspalveluiden kehittämisen.

Uudessa mallissa on tarkoitus luoda puitteet muun muassa yksityisille tunnistuspalveluiden ja varmennepalveluiden tarjoajille. Tunnistamismarkkinoilla liiketaloudellisten palvelujen luonne on siinä määrin etäännytynyt julkiseen hallintotehtävään liitettävistä ominaispiirteistä, että toimintaa ei ole pidettävä julkisena hallintotehtävänä, vaikka vahvan sähköisen tunnistamisen

välineillä ja varmennetoiminnalla sinänsä onkin merkitystä erilaisissa oikeustoimissa¹.

Suomessa vahva sähköinen tunnistaminen tarkoittaa sellaisia tunnistuspalveluita, joista ollaan säätämässä Euroopan Unionin asetuksessa sähköisestä tunnistamisesta ja luottamuspalveluista sisämarkkinoilla. Asetuksessa turvatasot määritellään seuraavasti: low, substantial ja high.

”Matala” (low) vastannee EU-pilotti Storkin turvatasoja 1-2, ”suuri” (substantial) vastannee Storkin turvatasoa 3 ja ”korkea” (high) vastannee Storkin turvatasoa 4. Turvatasojen teknisistä määrittelyistä ja niiden käytännön toteutuksesta tullaan päättämään täytäntöönpanosäännöksillä, joiden käsittely aloitettiin komission työryhmässä huhtikuussa 2014. Asetus tulee kokonaisuudessaan voimaan vuonna 2018.

Suomessa vahva sähköinen tunnistaminen tulee uudessa mallissa tarkoittamaan asetuksen turvatasoja ”suuri” tai ”korkea” asetuksen tultua näiltä osin voimaan. Siihen saakka kestävän siirtymäkauden aikana kaikkeen tunnistamiseen riittää laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista tarkoitettu vahva sähköinen tunnistaminen sellaisena kuin se on ko. laissa tällä hetkellä määritelty. Kaikilla tämän vaatimuksen täyttävillä välineillä ja tunnistusratkaisuilla pääsee kaikkiin julkisiin ja yksityisiin palveluihin, joissa vaaditaan vahvaa sähköistä tunnistamista. Lain mukaisia vahvan sähköisen tunnistamisen välineitä ovat tällä hetkellä pankkitunnistukset, mobiilivarmenteet ja HST-kortti.

Siirtymäkauden jälkeen vahvan sähköisen tunnistamisen perustaso Suomessa on ”suuri”. Myös nykyisten tunnistusvälineiden ja tunnistusratkaisujen käyttöä voidaan jatkaa, jos ne täyttävät edellä mainitun vaatimuksen.

Tason High (korkea) täyttäviä tunnistusvälineitä voidaan vaatia esimerkiksi tietyissä sensitiivissä tietoa sisältävissä palveluissa tai tapahtumissa, joissa tehdään merkittäviä henkilön omaisuuteen tai oikeuksiin liittyviä tapahtumia julkisen tai yksityisen sektorin tuottamissa palveluissa. Vahvaa sähköistä tunnistamista käyttävä sähköisen palvelun tarjoaja voi palvelukohtaisesti edellyttää ”korkean” turvatason käyttöä. Tunnistustason päättäminen on siten aina tunnistuspalveluja käyttävän palveluntarjoajan itsensä harkittava asia.

Julkisissa palveluissa tarvitaan edelleen edellä kuvatun kaltaista tunnistusten välityspalvelua Vetumaa. Välityspalvelu tullaan liittämään palveluväylään ja on näin ollen yksi tulevan palveluarkkitehtuurin komponenteista. Mallin valmistelun yhteydessä voidaan tarkastella olisiko sen käyttö laajennettavissa muille yhteiskunnan toimijoille.

¹ PeVL 16/2009 vp – HE 36/2009 vp