




TIEKE TIETOYHTEISKUNNAN KEHITTÄMISKESKUS RY:N JULKAISUSARJA



Luottamus tietoverkkojen käytössä

- *Varmenteet ja pankkitunnisteet*

JUHANI KOIVUNEN



Julkaisija:
TIEKE Tietoyhteiskunnan kehittämiskeskus ry
Salomonkatu 17 A, 00100 Helsinki
Puh. (09) 4763 0400
www.tieke.fi

Copyright: TIEKE Tietoyhteiskunnan kehittämiskeskus ry

TIEKE Tietoyhteiskunnan kehittämiskeskus ry:n julkaisusarja, ISSN 1459-6490
Julkaisusarjan osa 26: Luottamus tietoverkkojen käytössä - Varmenteet ja
pankkitunnisteet
ISBN 952-9714-48-3

Helsinki 2007-01

TIEKE 26

Luottamus tietoverkkojen käytössä

- Varmenteet ja pankkitunnisteet

JUHANI KOIVUNEN

Sisältö

	Esipuhe	5
1.	Johdon yhteenveto	6
2.	Projektin laajuus, tausta ja tavoitteet	7
	2.1. Tausta	7
	2.2. Tavoitteet	7
	2.3. Laajuus	7
3.	Läpiviennin kuvaus	9
4.	Projektin tulokset	10
	4.1. Tilanne EU:ssa ja eräissä vertailumaissa	10
	4.1.1. Viro	11
	4.1.2. Ruotsi	11
	4.1.3. Tanska	12
	4.1.4. Belgia	12
	4.1.5. Itävalta	12
	4.2. Tilanne Suomessa käyttöalueittain	12
	4.2.1. Tunnistaminen	12
	4.2.2. Oikeuksien esittäminen ja hallinta	14
	4.2.3. Luotettava tunnistamattomuus	14
	4.2.4. Vahva (kehittynyt) sähköinen allekirjoitus merkittävien sopimusten, suostumusten tms. yhteydessä	14
	4.2.5. Tiedon salaus ja tiedon suojaaminen muutoksilta	15
	4.2.6. Aikaleima	15
	4.3. Erityiskysymyksiä Suomessa	15
	4.3.1. Pankkitunnisteiden (TUPAS) käyttö	15
	4.3.2. Henkilövarmenteet	17
	4.3.3. Sähköisen asiointitunnuksen (SATU) tarve	18
	4.3.4. Valtion rooli turvallisuudessa ja varmenteissa	19
	4.3.5. Varmenneteknologian käytön yleisiä haasteita	20
	4.3.6. Kansainväliset tarpeet varmenteiden käytön edistämisessä	20
	4.3.7. Kansallisen yhteistyön tarve	22
	4.4. Tulevaisuuden tarpeet	22
	4.5. Johtopäätökset ja ehdotukset	23
	4.5.1. Johtopäätökset	23
	4.5.2. Ehdotus	24

Esipuhe

Turvallisuus ja luottamus sähköisiin toimintatapoihin ovat ensiarvoisen tärkeitä sähköisten palveluiden käytön lisäämiseksi. Yksi keskeinen asia luottamuksen rakentamisessa on verkossa toimivien osapuolien luotettava tunnistaminen tarvittaessa ja mahdollisuus anonyymiin toimintaan tilanteen niin vaatiessa. PKI-teknologiaan pohjautuvat henkilövarmenteet on kansainvälisesti nähty jo vuosia ratkaisuna näihin ongelmiin. Todellisuudessa yhteentoimivat kansainväliset ratkaisut kuitenkin puuttuvat edelleen. Sen sijaan pankkien tarjoamat TUPAS -tunnisteet ovat levinneet Suomessa laajaan käyttöön ilman merkittäviä ongelmia. Niiden puutteina nähdään lähinnä toiminnallisesti ja alueellisesti rajoittuneempi käyttö kuin mikä varmenteissa on ollut tavoitteena.

Tässä selvityksessä on haastateltu 18 merkittävää toimijaa sähköisessä liiketoiminnassa, niin yrityksiä kuin julkishallinnon yksiköiden edustajia. Näkemykset ovat selvityksen mukaan jakaantuneet käytännönläheisiin TUPAS-palveluiden kannattajiin, visionääriempiin PKI-varmenteiden kannattajiin sekä neutraalisti asiaan suhtautuviin. Tulevaisuudesta ei kukaan voi olla täysin varma.

Haastatteluissa nähtiin tarvetta yksittäiset näkemykset ylittävälle avoimelle yhteistyölle etsittäessä yhteistä tahtotilaa ja yhteisiä periaatteita tuleville ratkaisuille.

TIEKE toivoo selvityksen antavan pohjaa lisääntyvälle yhteistyölle alueella ja kiittää selvitykseen panoksensa antaneita henkilöitä.

Helsingissä joulukuussa 2006

Aatto J. Repo

Toiminnanjohtaja

TIEKE Tietoyhteiskunnan kehittämiskeskus ry

1 Johdon yhteenveto

TIEKEN hallitus päätti 23.5.2006 selvityksen tekemisestä varmenteiden käytön edistämiseksi. Selvityksen aikana haasteltiin 12 yrityksen ja 5 julkishallinnon yksikön edustajat. Sen lisäksi selvityksen johtoryhmään on kuulunut kahden yrityksen edustajat.

Tehtyjen haastattelujen pohjalta selvityksen kohdealue laajeni yleisemmäksi luottamuksen lisäämiseksi tietoverkkojen¹ käyttämisessä. Kohdealue käsitti tietoverkkojen käytössä tarpeellisen:

- tunnistuksen ja luotettavan tunnistamattomuuden
- sopimuksen tai suostumuksen vahvistamisen sähköisellä allekirjoituksella
- oikeuksien esittämisen
- tiedon salauksen ja suojauksen muutoksilta
- aikaleiman.

Kohdealueen keskeisin tarve tällä hetkellä on osapuolten luotettava tunnistaminen tarpeen niin edellyttäessä. Muut aktiviteetit, esimerkiksi sähköinen allekirjoitus, ovat huomattavasti harvemmin tarpeellisia tai sen katsotaan tapahtuvan tunnistamisen perusteella. Nykyiset ratkaisut, erityisesti pankkien tarjoama TUPAS-tunnistaminen, vastaavat tämän hetkisiin tarpeisiin varsin hyvin. PKI-tekniikan mukaisten varmenteiden käyttö on Suomessa, kuten yleensäkin maailmalla, edelleen vähäistä.

Tulevaisuudessa on odotettavissa luottamuksen merkityksen tietoverkkoja käytettäessä edelleen kasvavan ja monenlaisia ratkaisuja olevan käytössä. Kansainvälisten ratkaisujen uskotaan pohjautuvan PKI-pohjaisiin varmenteisiin, mutta niiden harmonisointi kestää vielä vuosia. Uudet käytännöt tulisi mahdollisuuksien mukaan luoda olemassa olevien ratkaisujen pohjal-

ta ja harkita uusien elementtien tarpeellisuus tarkkaan.

Suomessa nähdään tarvetta avoimelle yhteistyöryhmälle, joka luo yhteistä tahtotilaa ja yhteisiä periaatteita tämän alueen ratkaisuille. Lähiajan kehittämis-kohteina haastatteluissa tuli esiin:

- TUPAS –tunnuksiin pohjautuvien palveluiden edelleen kehittäminen
- suomalaisten varmenneratkaisujen edistäminen
- kansalaisten yksilöintikäytäntöjen kehittäminen sähköisissä palveluissa
- alueen lainsäädännön tarkistaminen
- huomioida kansainvälinen kehitys kotimaisissa ratkaisuisissa.

Tähän kehittämistyöhön esitetään perustettavaksi eri osapuolille avoin Luottamusfoorumi.

¹ Selvityksen ensisijaisena kohteena oli työasemapohjaiset internetpalvelut, mutta tulokset on pääosin sovellettavissa myös muihin tietoverkkoihin, esimerkiksi mobiiliverkkoihin.

2. Projektin laajuus, tausta ja tavoitteet

2.1. Tausta

Turvallisuus ja luottamus sähköisiin toimintatapoihin ovat ensiarvoisen tärkeitä sähköisten palveluiden käytön lisäämiseksi. Tämä edellyttää sähköisten identiteettien käyttöä. Tilanteissa, joissa tunnistettavalla henkilöllä ja palveluntarjoajalle ei ole keskinäistä aikaisempaa suhdetta, ainoa laajasti kansainvälisesti sovellettava teknologia tunnistamiseen tällä hetkellä on varmenne-teknologia (PKI-teknologia)². Yhteentoimivat kansainväliset ratkaisut kuitenkin puuttuvat edelleen.

Henkilövarmenteet vastaavat tietoverkoissa henkilöiden identiteettiä. Varmenteita käytetään erityisesti edistämään tietoturvaa. Keskeiset käyttökohteet ovat henkilöiden tunnistaminen ja henkilöiden oikeuksien tarkistaminen, sähköiset allekirjoitukset sitoumuksien teossa, tietojen suojaaminen asiattomilta henkilöiltä ja tietojen muuttamattomuuden varmistaminen. Varmenteiden luontia ja käyttöä säädetään sähköisen allekirjoituksen lailla (14/2003), joka pohjautuu sähköisen allekirjoituksen direktiiviin (1999/93/EY). Lainsäädäntö kohdistuu erityisesti nk. laatuvarmenteisiin ja niiden luonnissa tarvittaviin osapuoliin ja järjestelmiin. Säädöksillä halutaan varmistaa laatuvarmenteiden korkea luotettavuus edellyttämällä niiltä erityisesti luotettavia toimintatapoja.

Varmenteisiin ja niiden käyttöön asetettiin suuret odotukset, kun ne tulivat markkinoille viime vuosikymmenen lopulla. Käytännön kehitys on ollut hidasta. Syiksi hitaaseen edistymiseen on esitetty varmenteita edellyttävien palveluiden vähyys, teknisen ja toiminnallisen infrastruktuurin heikkoudet, käyttöönottoon liittyvät

hankaluudet, hinta suhteessa hyötyihin, yksinkertaisemmat kilpailevat ratkaisut, eri ratkaisujen yhteentoimivuuden ongelmat ja eri toimialojen ja maiden kulttuuri- ja lainsäädäntöerot.

2.2. Tavoitteet

Projektin ensisijaisena tavoitteena oli laatia ehdotus varmenteiden käytön edistämisestä Suomessa. Ensi vaiheessa tuli kirkastaa näkemyksiä markkinasegmenteistä ja varmennekäytön tilanteesta, sen kehittymisen esteistä ja suhteesta kansainväliseen kehitykseen. Varsinaisena tavoitteena oli luoda yhteinen tahtotila huomioiden erityisesti kaupallisen sektorin näkemykset. Tavoitteena oli myös selvittää tarpeet luoda laaja yhteinen kansallinen foorumi, jossa eri osapuolet ovat edustettuina sekä mahdollisuudet edistää julkisen ja yksityisen sektorin yhteistyötä alueella. Pidemmän aikavälin tavoitteina oli synnyttää varmennepalveluille kriittinen massa, jolloin varmenteiden hinta voidaan kohtuullistaa suhteessa käyttömahdollisuuksiin, kouluttaa suomalaiset varmenteiden käyttämisen kulttuuriin ja aikaansaada kansainvälisiä ratkaisuja.

2.3. Laajuus

Selvitys pohjautuu keskeisiltä osiltaan varmennepalveluita käyttävien ja niitä tarjoavien organisaatioiden haastatteluihin ja kohteena olivat ne varmenteiden käytön alueet, jotka ovat keskeisiä kansalaisille suunnatuissa palveluissa. Haastatteluihin sisällytettiin myös pankkien TUPAS-palvelut johtuen niiden keskeisestä asemasta kansalaisten tunnistamisessa.

² Varmenneteknologialla tarkoitetaan tässä dokumentissa epäsymmetrisellä salausmenetelmällä (PKI-teknologialla) toteutettua henkilön identiteetin tai ominaisuuden sähköisen vastineen luonti- ja käyttömenetelmää.

SSL-suojausta³, järjestelmien yms. tunnistamista ei sisällytetty selvitykseen. Selvityksen yhteydessä kartoitettiin Euroopan Unionin tämän hetkistä tilannetta alueella sekä seuraavien maiden tilannetta vertailun takia:

- Belgia
- Itävalta
- Ruotsi
- Tanska
- Viro.

³ SSL (Secure Sockets Layer) mahdollistaa suojatun yhteyden käyttäjän selaimen ja käytettävän palvelimen välille.

3. Läpiviennin kuvaus

Projektin kokoonpano on ollut:

- Pekka Rauhala TeliaSonera, ohjausryhmän puheenjohtaja
- Matti Korkeala Osuuspankkikeskus, ohjausryhmän jäsen
- Aatto J. Repo TIEKE, ohjausryhmän jäsen
- Juhani Koivunen, selvityksen tekijä sekä ohjausryhmän sihteeri.

Selvitys on pohjautunut kirjallisuustutkimuksiin⁴ sekä seuraavien 17 organisaation haastatteluun:

- Elisa Oyj
- Finnair Oyj
- Fujitsu Services Oy
- KELA
- MTV Oy
- Nordea Pankki Suomi Oyj
- Sampo Oyj
- SOK-yhtymä
- Stakes
- Suomen Suoramarkkinointiliitto
- Tapiola-ryhmä
- TeliaSoneraFinland Oyj
- TietoEnator Oyj
- Vantaan kaupunki
- Verohallitus
- Väestörekisterikeskus
- WM-data Oy

Lisäksi haastattelujen havainnoista on käyty keskusteluja TIEKEN hallituksessa ja ohjausryhmässä.

⁴ EU:n ModinisIDM hankkeen tulokset, Porvoo-ryhmän maakatsaukset, IDABC's Quartely Newsletter Synergy 07 / September 2006, viitattujen palveluiden web-sivustot

4. Projektin tulokset

Turvallisuusasiat on monitahoinen kysymys, ja aihe on ikivanha. Tietoverkoissa eri kanavien avulla tapahtuva etämyynti ja – palvelut ovat korostaneet sen merkitystä nykyaikana. Esiintyvät tilanteet ja tarpeet ovat kuitenkin hyvin erilaisia, voidaan ostaa tuotteita, osallistua arvontaan, kysyä vähän lisätietoja, päivittää omia arkaluontoisiakin tietoja jne. Tarpeet näissä eri tilanteissa voivat olla hyvin erilaisia.

Haastateltavat toivatkin usein esiin tärkeänä lähteä todellisista asiakkaan tai kansalaisen tarpeista (tai palveluntarjoajan omista kustannuksista). Jos halutaan edistää esimerkiksi vahvaa tunnistamista⁵, siitä ei pidä tehdä pakkoa asioihin, joissa sitä ei tarvita. Riski on, että toiminta vähenee tai jopa loppuu kokonaan.

Verkkomaailmasta puuttuvat vakiintuneet käytännöt, mitkä fyysisessä maailmassa ovat syntyneet pitkän ajan kuluessa. Haastatteluissa tuli toistuvasti esiin epäonnistumisen riski, jos yritetään liian nopeasti suuria muutoksia. Uudet käytännöt tulisi ensisijaisesti luoda vanhojen ratkaisujen pohjalta ja harkita uusien elementtien tarpeellisuus tarkkaan.

Haastatteluissa todettiin myös, että julkisuudessa ruokitaan tarkoitushakuisesti epävarmuutta henkilöiden toimiessa verkon kautta. Väärinkäyttötapauksia on asian saamaan julkisuuteen nähden Suomessa toistaiseksi kohtuullisen vähän.

4.1. Tilanne EU:ssa ja eräissä vertailumaissa

Euroopassa on säädetty sähköisistä allekirjoituksista direktiivi (1999/93/EY), jolla on pyritty saamaan aikaan yhteiset periaatteet ja eri maissa toteutettavien ratkaisu-

jen yhteentoimivuus. Tämä ei kuitenkaan ole toiminut. Modinis^{IDM}-hankkeessa on listattu tämänhetkisiä vaikeuksia:

- tekniset
 - standardeja on runsaasti ja niiden keskinäinen yhteensovittaminen on vaikeaa
 - tekniikka kehitty nopeasti ja jatkuvasti tehdään erilaisia tilapäisiä ratkaisuja
 - eri maissa käytetään erilaisia alustoja (tokens) varmenteille
- lainsäädäntö
 - erilaisuudet lainsäädännössä
 - yksityisyyden suojan erot
 - valtuutuskäytäntöjen erilaisuudet
- toiminnalliset
 - kulttuurierot
 - tehdyt investoinnit estävät uusia yhdenmukaisia ratkaisuja
 - erilaiset käsitteistöt
 - sähköisten identiteettien moninaisuus.

EU:n ministeritason sähköisen hallinnon konferenssi totesi marraskuussa 2005, että vuoteen 2010 mennessä EU-alueella tulee olla käytössä yhteen toimiva sähköisen identiteetin hallintajärjestelmä julkisille palveluille. Käyttökohteina olisivat sähköinen hallinto ja sähköiset hankinnat. Tavoitteena on aikaansaada yhteiset määrittelyt sähköisen identiteetin hallintaan vuoden 2007 aikana sekä tarkistaa sähköisen allekirjoituksen lainsäädäntö vuonna 2009. Näkemykset julkisen sektorin ratkaisujen käyttökelpoisuudesta kaupallisille sektoreille vaihtelevat kuitenkin maittain. Tilanne kokonaisuudessaan on hyvin hajanainen.

⁵ Vahvalla tunnistamisella tarkoitetaan tässä lähinnä TUPAS-palveluihin tai laatuvarmentettiin pohjautuvaa tunnistamista. Objektivista vertailua eri menettelyjen kokonaisluotettavuudesta tämän selvityksen tekijällä ei ole käytettävissä.

Seuraavassa on esitetty eri maiden varmenteiden käytön tilannetta.

4.1.1. Viro

Viroa pidetään Euroopan edistyksellisimpänä maana varmenteiden käytössä. Sähköinen varmenne sijaitsee virallisella henkilökortilla, joka on pakollinen maan yli 15 vuotiaille kansalaisille sekä yli vuoden mittaisella luvalla maassa oleskeleville ulkomaalaisille.

Kortteja on maassa jaettu lähes miljoonalle henkilölle (asukasluku on 1,4 miljoonaa). Kortin hinta on 10 euroa. Varmentajana toimii yksityinen yritys (AS Sertifitseerimiskeskus), jolla on sopimus asiasta valtion kanssa. Kortin jakelu hoidetaan sen omistavien pankkien konttoreissa.

Kortilla olevissa varmenteissa, allekirjoitus- ja tunnistamisvarmenne, on haltijan nimi sekä kansallinen, yksikäsitteinen tunnistekoodi. Lisäksi tunnistamisvarmenne sisältää haltijan yksikäsitteisen sähköpostiosoitteen (joka on valtion antama elinikäinen osoite ja toimii vain linkkinä todellisiin sähköposteihin, jotka haltijan on erillisessä tietokannassa pidettävä yllä). Korteilla ei ole mitään rooli- tai valtuutus-tietoa, vaan ne on haettava erillisistä rekistereistä tunnistekoodin avulla. Tunnistekoodi on julkinen. Ainoastaan allekirjoitusvarmenne on laatuvarmenne. Varmenteilla ei ole käyttörajotteita.

Varmenteita ei anneta pelkästään henkilöille vaan myös organisaatioille. Organisaatioille annetut varmenteet ovat teknisesti täysin samanlaisia kuin henkilövarmenteet, mutta ne eivät ole laatuvarmenteita.

Toiminnallisuuden edistämiseksi tarjotaan vapaasti käyttöön DigiDoc-arkkitehtuuria ja siihen pohjautuvia välineitä, joista osa on ilmaisia.

Huolimatta kortin laajasta käyttäjäkunnasta sen käyttö tietoverkkopalveluissa on kuitenkin ollut vähäistä. Noin 2,5 % kortin omistavista henkilöistä käyttää sitä sähköisten palveluiden yhteydessä. Vuonna 2005 sähköisten veroilmoitusten allekirjoittamiseen sitä käytti noin 1600 henkilöä, kun samanaikaisesti pankkitunnisteita käytti noin 400 000 ihmistä.

Varmenne on yhteentoimiva Suomen kansalaisvarmenteen kanssa, Belgian kanssa tehdään yhteistyötä yhteentoimivuuden saavuttamiseksi.

4.1.2. Ruotsi

Ruotsissa ei ole laatuvarmentajia. Menestynein sähköinen toteutus on pankkien kehittämä BankId (www.bankid.com). Pankki vastaa yksittäisen asiakkaansa tunnistamisesta, kun sähköinen henkilöllisyys luovutetaan. Varmenne sijoitetaan asiakkaan koneeseen tai asiakkaan valitsemaan liikuteltavaan muistivälineeseen ns. sw-varmenteena. Pankit vastaavat varmentajatoiminnosta yhdessä Bankgirocentralen 'n kanssa ja antavat asiakkailleen varmenteen ilmaiseksi. Myös TeliaSonera toimii varmentajana. Ruotsissa varmenteita on myönnetty noin 1 200 000 kappaletta.

Ruotsissa on viranomaistoimenpiteenä luotu yhteinen PKI-varmenteiden standardi (www.e-legitimation.se), mitä eri toimijoiden (mm. bank-id, Nordea, Telia) PKI-pohjaisten ratkaisujen tulee noudattaa.

Aiemmin Ruotsissa oli toimikorttipohjaisia varmenteita käytössä esimerkiksi Nordbankenilla, mutta niiden käytöstä on luovuttu johtuen asiakkaiden haluttomuudesta käyttöön ja tarvittavien investointien suuruudesta. Nordea on markkinoinut voimakkaasti kertakäyttösalasanaratkaisua verkkopankkiin ja on saanut lyhyessä ajassa noin 1,5 miljoonaa käyttäjää.

4.1.3. Tanska

Hallitus on vuodesta 2003 asti tarjonnut kansalaisille ja yrityksille ilmaisia sähköisiä sw-varmenteita, joilla voidaan tunnistautua. Hallitus tekee yhteistyötä TDC:n (Tele-Danmark Communications'n) kanssa, mutta lähtökohtaisesti kuka tahansa yritys voi toimia varmentajana. Näitä varmenteita käyttää sekä julkinen sektori että jotkut pankit. Pankkisektorilla on yleisimmin käytössä kertakäyttöiset salasana- ja salasanat. Hallitus ei ole esittänyt suunnitelmia toimikortti-pohjaisista varmenteista.

4.1.4. Belgia

Belgia esitetään Viron ohella toisena edistyksellisenä maana toimikorttipohjaisen varmenteiden käytössä. Hallitus on jakanut vuoden 2003 loppupuolelta alkaen kansalaisille sähköiset varmenteet (allekirjoitukseen ja tunnistamiseen) sisältäviä henkilökortteja ja kortteja on jo jaettu yli miljoona. Kortin jakelijana (Registration Authority) toimivat kunnat. Tavoitteena on saada jaettua kortit kaikille yli 12-vuotiaille vuoden 2008 alkupuolella. Toistaiseksi kortteja on jaettu vain Belgian kansalaisille. Varmentajana toimii Belgacom, jonka suurin omistaja Belgian valtio on. Kansalaiset yksilöivänä tunnisteena on henkilörekisterinumero. Belgia tutkii mahdollisuuksia yhteentoimivuuteen muiden maiden mm. Viron kanssa. On esitetty epäilyjä, että Belgian ratkaisu on hyvin toimikorttipohjainen ja muiden alustojen mukaan ottaminen tulee olemaan hyvin vaikeaa.

4.1.5. Itävalta

Itävallassa kehitteillä on kansalaiskortti ("Bürgerkarte"), joka mahdollistaa sähköiset allekirjoitukset ja autentikoinnin erilaisten online-periaatteella luotavien "sähköisten henkilöllisyyksien" ja eri välineiden, kuten älykortin ja matkapuhelimen, avulla. Järjestelmää voidaan soveltaa myös luotto- ja pankkikortteihin.

Käytännössä jokainen kansalainen voi itse päättää, ottaako käyttöön kansalaiskortin vai ei, ja mitä välinettä käyttäen.

Koska kansalaiskortin voi saada erilaisilta julkisen ja yksityisen sektorin toimijoilta, sen hinta vaihtelee ilmaisesta 15 euroon. Se on voimassa kolme vuotta, mutta ei ole virallinen henkilökortti sanan tavanomaisessa merkityksessä. Tähän mennessä noin 70.000 henkilölle on myönnetty noin 100.000 korttia. Sähköinen allekirjoitus on käytössä. Maassa on useita sekä yksityisiä että julkisia vastuullisia varmentajaorganisaatioita, joiden toiminta perustuu lakiin (sähköistä hallintoa koskeva laki ja asetus sähköisestä allekirjoituksesta, molemmat vuodelta 2004).

Itävallalaisessa järjestelmässä kansalaisen tunnistamistietoja ei siirretä sähköisen palvelun sovelluksiin. Sen sijaan käytetään ns. sektorikohtaisia tunnusnumeroita, jotka luodaan erikseen jokaista palvelua varten ja joiden avulla ei voida selvittää kansalaisen omaa tunnistetta. Tämä on erittäin varma tapa estää henkilötietojen aiheeton levittäminen.

4.2. Tilanne Suomessa käyttö-alueittain

4.2.1. Tunnistaminen

Osapuolien tunnistaminen on ehdottomasti laajimmin käytössä oleva yksittäinen turvallisuutta lisäävä toimenpide. Henkilöiden tunnistamisessa käytetään tällä hetkellä seuraavia ratkaisuja:

- Tunnistautumista vaativissa verkkopalveluissa (jos ei ole olemassa olevaa asiakassuhdetta) käytetään lähes yksinomaan pankkien TUPAS-palveluita. Pankit rinnastavat TUPAS-tunnisteet PKI-pohjaisiin varmenteisiin ja tehdyn toimenpiteen vahvistamisen TUPAS-tunnisteilla sähköiseen allekirjoitukseen. Myös valtionvarainministeriö suosittelee (VM 6/01/2003,

29.9.2003) laatuvarmenteen ohella TUPAS-menettelyä. Pankkiasioinnissa kysymyksessä voivat olla isot rahasummat, joten asiakkaan luotettava tunnistaminen on keskeinen vaatimus. Pankkien tietoturvan täytyykin olla erittäin korkealla tasolla, luottamuksen pettäminen pelkästään verkkokanavassakin olisi iso juttu.

■ Kansalaisvarmenteet: Tapauksissa, missä kansalaisvarmenteiden käyttö olisi mahdollista, niitä poikkeuksetta käytetään erittäin vähän. Esimerkkejä tästä ovat Kela, Vantaan kaupunki ja Verohallitus. Vastaavia esimerkkejä löytyy ulkomailta, mm. Virossa.

■ Asiakastunnukset ja salasana: Useat palveluntarjoajat antavat asiakkailleen tunnuksen ja salasanan. Tunnistautuminen on kuitenkin mahdollista vain kyseisen palveluntarjoajan palveluihin (poikkeuksena on pankkien TUPAS-ratkaisu). Jos henkilöt voivat hakea asiakkuutta verkossa, he voivat tunnistautua käyttäen joko TUPAS-tunnisteita tai kansalaisvarmennetta.

■ Erilliset tunnistautumiskäytännöt, jotka pohjautuvat TUPAS-tunnisteisiin ja kansalaisvarmenteisiin. Koko julkishallintoa varten on kehitetty VETUMA-ratkaisu, joka tunnistamisen lisäksi mahdollistaa myös maksamisen. Ratkaisu ei ole vielä laajasti käyttöön otettu ja käyttöönotot riippuvat julkishallinnon yksiköiden päätöksistä. Verohallituksen, Kelan ja työministeriön palveluissa kansalaisen on mahdollista tunnistautua tunnistus.fi:ssä. Yrityspuolelle kyseiset organisaatiot ovat kehittäneet vastaavan palvelun, KATSO-organisaatio-tunnistajärjestelmän. Siinä yrityksen vastuuhenkilö voi luoda yrityksen työntekijöille tunnukset ja tarpeelliset valtuudet. Tietoyhteiskuntaohjelman ministeriryhmä on ottanut kannan, että KATSO-järjestelmästä kehitetään koko yhteiskunnan organisaatiotunnistajärjestelmä.

Terveyspuolella henkilöiden vahva tunnistaminen korostuu. Hyvä esimerkki on potilastietorekisterissä olevien tietojen suojaaminen ja käyttö. Terveysviranomaiset lähtevät siitä, että kun tietoa luovutetaan tai käytetään, lokiin pitää aina jäädä tieto, kuka on käyttänyt, mitä, koska ja mihin tarkoitukseen. Uuden lain mukaan kansalaisilla on rajoittamaton tiedonsaanti-oikeus tähän rekisteriin omien tietojensa osalta. Tämän pitää olla myös sähköisesti mahdollista sen jälkeen, kun asiakas on tunnistettu. Tämä on osa luottamuksen rakentamista, mutta myös pelote väärinkäyttäjille.

Terveyssektorilla on jo käytössä pilottivarmennejärjestelmä 11 sairaanhoitopiirissä (20:stä). Lääkäreillä on terveydenhuollon ammattilaiskortit ja ne ovat käytännössä terveydenhuollon toimintayksiköiden antamia kortteja, varmennetietokanta on yhteinen. Tulevaisuudessa varmentajana tulee olemaan TEO (terveydenhuollon oikeusturvakeskus), rekisteröintiyksikkö (Registration Authority) tulee olemaan paikallinen toimintayksikkö ja kortilla voi myös olla paikallisia varmenteita. Se, että henkilö on lääkäri ja hänen oikeutensa tarkistetaan keskitetystä tietokannasta. Palveluntarjoajat tullaan kilpailuttamaan.

Terveyssektorilla nähdään tärkeäksi pitää yksityishenkilö ja ammattirooli (sekä vastaavat kortit tms.) erossa toisistaan. Erillään oloa puolustaa myös se seikka, että ammattihenkilön suorittama salaus pitää voida purkaa, jos potilaan terveydenhoito sitä edellyttää.

Useat haastatellut näkivät, että tarve henkilöiden tunnistamiseen verkossa on lisääntymässä. Järjestys näyttää olevan: yrityksissä, ammattilaiset, tavalliset kansalaiset. Haastatteluissa tuotiin myös esiin palveluntarjoajien ja palvelunkäyttäjien mahdollisuus keskinäiseen sopimiseen

mahdollisesta tunnistetusta tai tunnistamattomasta asiakkuudesta.

Tunnistaminen tarkoittaa yleensä henkilön tunnistamista. Myös sähköisen allekirjoituksen lainsäädännön katsotaan koskevan vain henkilöiden tunnistamista. Kuitenkin esimerkiksi terveydenhuollossa on tilanteita, joissa tunnistamisen kohteena on organisaatio. On tärkeää, että kansalaiset voivat myös verkossa luottaa jonkin organisaation olevan se, mikä se ilmoittaa olevansa. Tähän kaivattiin haastatteluissa jopa erillistä lainsäädäntöä.

4.2.2. Oikeuksien esittäminen ja hallinta

Yleinen näkemys haastatteluissa oli, että henkilön oikeudet erotetaan tunnistamisesta. Tunnistamisen jälkeen henkilön oikeudet katsotaan tietokannasta. Yritysten henkilöiden oikeuksien hallintaan Patentti- ja rekisterihallitus on kehittänyt palvelun. Terveydenhuollossa rooleilla ja oikeuksilla on suuri merkitys, on sekä pysyviä että dynaamisia rooleja.

4.2.3. Luotettava tunnistamattomuus

Edelliseen liittyen tavoitteeksi on esitetty myös kansalaisen mahdollisuus asioida nimettömänä silloin, kun henkilön tunnistaminen ei ole välttämätöntä. Haastateltujen enemmistö tulkitsi tämän toteutuvan silloin, kun henkilöä ei kappaleessa 4.2.1 esitetyllä tavalla tunnisteta. Kysymys ei kuitenkaan ole luotettavasta tunnistamattomuudesta, koska järjestelmiin jää merkintöjä yhteyden ottajan verkkosoitteesta.

Luotettavalle tunnistamattomuudelle ei yleensä koettu olevan tällä hetkellä merkittävää tarvetta. Se tuli kuitenkin vahvasti esiin terveystietojen yhteydessä (vertailuna tuotiin esiin ihmisen mahdollisuus saada nimettömänä hoitoa sukupuoliklinikalla). Siellä asiaan liitettiin myös terveystietojen säilyttäminen,

säilytysaikojen pituus ja periaatteet tietojen hävittämiselle.

Useat haastatellut, varsinkin yritysten edustajat, toivat sen sijaan esille tarpeen saada heidän verkkopalveluissaan nimettömän käyneiden henkilöiden profiilitietoa, esimerkiksi tietoa ikä-, asuinpaikka-, koulutus- ja sukupuoli-jakaumasta. Lisäksi todettiin palveluntarjoajien tarve tietää henkilöistä jotain tietoa (esimerkiksi ikä) ilman että häntä varsinaisesti yksilöidään.

4.2.4. Vahva (kehittynyt⁶) sähköinen allekirjoitus merkittävien sopimusten, suostumusten tms. yhteydessä

Eräät haastatelluista esittivät vahvan sähköisen allekirjoituksen erottamista teknisistä sähköisistä allekirjoituksista, joilla tarkoitettiin esimerkiksi henkilön tekemän verkkotapahtuman rutiininomaisesta vahvistamisesta. Vahvan sähköisen allekirjoituksen tarve tuli esiin seuraavissa tilanteissa:

- testamentti
- kiinteistökauppa
- suostumus omien terveystietojen

luovuttamiseen ja terveydenhoitoon liittyviä muitakin suostumuksia. Terveydenhuollossa pidetään erityisen merkittävänä kysymyksenä sitä, että asiakas on riittävän informoitu antaessaan suostumuksensa. Asiakkaan käyttäessä tietoverkkoja tätä kysymystä pidetään ongelmallisena. Tämän seurauksena tällä hetkellä suostumukset pyydetään vain paperilla.

Haastatteluissa kritisoitiin vahvan sähköisen allekirjoituksen rutiininomaista vaatimista kaikissa sähköisissä allekirjoitustilanteissa. Vaatimus rinnastettiin siihen, että perinteinen allekirjoitus tulisi aina käydä kolmannella osapuolella vahvista-

⁶ Laki sähköisistä allekirjoituksista 24.1.2003

massa. Esitettiin, että tulisi käydä nykyistä byrokraatiaa ja sen tarvetta kriittisesti läpi. Lisäksi esitettiin näkemyksiä, että vaatimalla turhaan allekirjoituksia vähennetään merkittävästi kansalaisten halua käyttää tarjolla olevia palveluita.

Kritiikkiä esitettiin myös kansalaisvarmenteen markkinoinnista puhuttaessa kiistämättömästi sähköisestä allekirjoituksesta. Sellaista ei juridisesti voi olla. Sähköisen allekirjoituksen direktiivi päinvastoin toteaa, että allekirjoitusta ei pidä jättää huomioimatta vain sen takia, että se on sähköinen, ettei se ole tehty laatuvarmenteella jne. Kiistämätöntä sen sijaan voi olla, että teknisesti allekirjoitus on tehty käyttäen tiettyyn varmenteeseen liittyvää salaista avainta ja sopimus pohjaisesti vain yhdellä henkilöllä on ollut tähän tarvittava tieto ja oikeus.

Suomessa oikeustoimille ei ole yleensä asetettu erityisiä muotovaatimuksia. Laissa tai muussa normissa voidaan kuitenkin erikseen säätää erilaisista muotovaatimuksista. Yksityisoikeudellisten sopimusten osalta lainsäädännössä yleisimmin käytetyt muotovaatimuksia ovat lähinnä sopimuksen tekeminen kirjallisesti ja sopimuksen allekirjoittaminen. Ilmauksia ”kirjallisesti” tai ”allekirjoittaa” ei ole määritelty tarkemmin lainsäädännössä.

Lailta sähköisistä allekirjoituksista on varmistettu, että ainakin laatuvarmenteeseen perustuva ja turvallisen allekirjoituksen luomisvälineen avulla luotu kehittynyt sähköinen allekirjoitus samaistetaan perinteiseen, käsintehtyyn allekirjoitukseen. Säännös ei vaikuta muiden sähköisten allekirjoitusten pätevyyteen. Millaisella sähköisellä allekirjoituksella tahansa tehty toimenpide voidaan myös riitauttaa vastaavasti kuin perinteisellä käsintehdylläkin allekirjoituksella tehty.

4.2.5. Tiedon salaus ja tiedon suojaaminen muutoksilta

Haastateltavat näkivät, että tieto on suojattuna silloin, kun se on organisaatioiden omissa järjestelmissä, jotka on suljettu ulkopuoliselta käytöltä. Näissä käyttötilanteissa noudatetaan organisaatioiden omia suojaus- ja käyttöoikeustapoja. Sitä, miten organisaatiot ovat suojanneet tiedot oman henkilökunnan mahdollisesti tekemiltä luvattomilta muutoksilta, haastatteluissa ei käsitelty.

Tiedon liikkua organisaatioiden ulkopuolella erityinen suojaus on tarpeellista. Suojaus tehdään tällä hetkellä yleensä käyttäen suojattuja yhteyksiä (VPN, SSL-suojaus) ja ne eivät silloin vaadi henkilövarmenteita. Sähköpostiviestinnässäkään ei tunnistettu merkittävää tarvetta varmenteiden käytölle tiedon salaamiseen tai suojaamiseen muutoksilta⁷.

4.2.6. Aikaleima

Aikaleimojen tarve koettiin pankkitoiminnoissa ja terveyssektorilla tärkeäksi, lisäksi suurissa julkisissa hankinnoissa ja niihin liittyvissä huutokaupoissa. Muualla tarvetta niille ei tunnistettu.

4.3. Erityiskysymyksiä Suomessa

4.3.1. Pankkitunnisteiden (TUPAS) käyttö

Pankkien TUPAS-palvelu mahdollistaa palvelun käyttöönottan, sähköisiä asiointipalveluja internetissä tarjoavan yrityksen tai yhteisön tunnistaa asiakkaansa Tupas-palvelun myöntämien ns. TUPAS-varmenteiden avulla. TUPAS-palvelussa pankki tunnistaa asiakkaansa kertakäyttösalasanoihin perustuvilla pankkitunnisteilla.

⁷ Salauksen käyttö sopivilla sähköpostiohjelmistoilla olisi sinällään helppoa. Organisaatioilla ei kuitenkaan yleensä ole valmiuksia tähän.

Tunnistamistapaa pidetään teknisesti PKI-tunnistamista heikompana, mutta käytännössä riittävän luotettavana. Menettelyn suurimmat tekniset heikkoudet periaatteessa ovat salasanojen lyhyys ja se, että kertakäyttösalasanat luodaan pankin ympäristössä ennen niiden toimittamista asiakkaalle. Käytännön kritiikkiä esitettiin TUPAS-palveluiden käytön kalleudesta sekä pankkien erilaisista hinnoittelutavoista.

Pankkitunnisteet ovat levinneet Suomessa (ja myös mm. Virossa) laajaan käyttöön ja ne koetaan yleisesti riittävän turvalliseksi henkilöiden tunnistamiseen. Pankit tarjoavat kolmantena luotettavana osapuolena tunnistamispalveluita myös muiden käyttöön. Haastattelussa tuli tähän johtaneina tekijöinä esiin:

- Suomen pankkimaailman kehittyneisyys ja pankkien panostukset TUPAS -järjestelmään
- Evoluutiomainen kehitys
- Järjestelmän tekninen yksinkertaisuus ja yksinkertaisuus käytössä (siitä huolimatta, että erillisen salanalistan käyttämistä pidetään hankalana)
- Luottamus pankkien toimintaan (pankkeihin luotetaan kriittisissä rahasioissakin).

Jossain määrin eräät haastatelluista vierasivat pankkien toimimista luotettavan tunnistajan roolissa tilanteessa, mikä ei muuten pankkia kosketa. Yleensä näissä tapauksissa haastatellut kuitenkin perusteluiden kysymisen jälkeen totesivat, ettei heillä ole mitään erityistä syytä epäillä pankkien luotettavuutta. Perusteltu kriittinen suhtautuminen pankkitunnisteisiin lähti phishing -ilmiöstä, joka on tullut Suomeenkin, mutta on huomattavasti suurempi ongelma esimerkiksi Englannissa ja Japanissa. Toisena pankkitunnisteiden luotettavuutta vähentävänä tekijänä nähtiin, että edelleen on kovin yleistä

käyttää avio- tai avopuolison tunnisteita⁸. Yleensä tällöin kyseiset henkilöt ovat keskenään sopineet menetellä näin. Pankkitunnisteiden väärinkäyttötilanteita haastateltavat eivät tuoneet esiin.

Pankkitunnisteiden käyttöä rajoittavana tulevaisuuden tekijänä tuotiin esiin mahdolliset ongelmat, jos pankeilta lähdetään vaatimaan korvauksia virheellisistä tunnistustapahtumista. Tähän mennessä pankit eivät ole sopineet korvauksista, mikäli virheitä tapahtuu niiden toimiessa tunnistajana kolmantena osapuolena. Pankkejahan TUPAS-tunnistamisessa ei sido laki sähköisestä allekirjoituksesta, jossa (16 §) laatuvarmentajiin kohdistuu ankaraksikin luonnehdittu vahingonkorvausvastuu. Siinä varmentajan on itse osoitettava, ettei ole aiheuttanut vahinkoa omasta huolimattomuudestaan vapautuakseen vastuusta.

Pankeilta odotetaan myös avoimempaa tiedottamista TUPAS-palvelun kehityssuunnitelmista, koska niillä voi olla vaikutusta muiden toimijoiden sitä hyödyntäviin palveluihin.

Näkemykset pankkitunnisteiden leviämisen mahdollisuudesta laajasti muihin maihin vaihtelivat. Enemmistö piti niitä kuitenkin lähinnä suomalaisena käytäntönä ja uskoi PKI-pohjaisten varmenteiden kehittyvän kansainväliseksi ratkaisuksi.

Enemmistö haastatelluista oli sitä mieltä, että TUPAS-palvelu ei kilpaile PKI-varmenteratkaisujen kanssa muilla alueilla kuin tunnistamisessa. Periaatteessa pankeilla on mahdollisuus verkottua nykyistä laajemminkin yhteiskuntaan ja tarjota verkostossa laajasti luotettavan kolmannen osapuolen rooliin sopivia palveluita. Esimerkkinä voi

⁸ Tämä on pankkitunnusten luovutus sopimuksessa kielletty.

todeta kahden osapuolen välisen sopimuksen, jossa pankki tallettaa sopimuksen omiin järjestelmiinsä ja vahvistaa molempien osapuolten hyväksyneen sen. Haastattelut kuitenkin osoittivat, että edes pankkien keskuudessa ei Suomessa ole yhteistä tahtotilaa tällaiseen palvelutarjonnan laajentamiseen.

4.3.2. Henkilövarmenteet

Haastateltavat kyseenalaistivat laajasti henkilövarmenteiden tämän hetkisen tarpeen. Keskeinen syy on, että tunnistaminen on keskeinen käyttötarve tällä hetkellä ja pankkitunnisteet toimivat siinä riittävän hyvin.

Käytännössä haastateltavat olivat yksimielisiä, että ei ole järkevää tarjota erillistä varmennekorttia. Varmenne tulee sijoittaa kansalaisilla jo muutenkin oleville korteille tai alustoille. Suuntauskin on menossa tähän, koska kansalaisvarmenteen saa jo pankkikortille ja SIM-kortille perinteisemmän poliisin myöntämän henkilökortin sijaan. Kuitenkin kansalaisvarmenteita hankitaan edelleen eniten henkilökortille.

Henkilökorttiakin kehitetään parhaillaan siten, että tulevaisuudessa kortin sirulle voidaan liittää myös muita palveluita. Tämän selvityksen tarkoituksena ei kuitenkaan ollut tarkemmin ottaa kantaa yhteiskunnan korttilinjauksiin.

“Isolla toimikortilla” sijaitsevan varmenteen käytössä nähtiin vaikeuksia. Ne liittyivät seuraaviin asioihin:

- Toimikortin käyttöä estää toimikortin lukijoiden vähäisyys. Päinvastaisista uskomuksista huolimatta uudetkin työasemat ja kannettavat tietokoneet on vain poikkeustapauksissa varustettu kortinlukijoilla. Haastatteluissa tuli esiin myös näkemys, että ne ovat liian kalliita varusteita tullakseen mukaan kovassa hintakil-

pailupaineessa olevien tietokoneiden peruskokoonpanoihin lähitulevaisuudessa.

- Toimikortit, niiden lukijat ja tarvittavat ohjelmat muodostavat kokonaisuuden, jonka käyttäminen ei aina ole yksinkertaista, mutta vielä hankalampaa on asentaa kaikki tarvittavat osat järjestelmään. Eri osien yhteentoimivuudessa on ongelmia, jotka käytännössä rajoittavat tavallisen kansalaisen mahdollisuuksia saada toimivaa kokonaisuutta tietokoneelle. Erään selvityksen mukaan jo pienikin monimutkaistuminen palvelun käytössä pudottaa käyttävien kansalaisten lukumäärän kymmenenteen osaan.

- Markkinoilla on liian vähäinen määrä palveluita, joissa henkilövarmenteilla on käyttöä ja lähes aina on jokin tapa korvata henkilövarmenteen käyttö.

- Kansalaisvarmenteen hakemista poliisilaitokselta pidettiin asiana, joka vähentää kiinnostusta siihen. Tämä ongelma on kuitenkin poistumassa, koska jo nyt kansalaisvarmenteen saa pankkikortille käymällä vain pankkikonttorissa. Operaattorit ja Väestörekisterikeskus uskoivat myös siihen, että mobiilivarmenteen saa ensi vuoden aikana operaattorien palvelupisteistä.

- Varmenteen hankkiminen toimikortille on kallista suhteessa siitä saataviin hyötyihin.

Haastateltujen henkilöiden enemmistön näkemys oli, että yhden asian korjaaminen (esimerkiksi varmenteen ilmainen jakelu) ei riitä saamaan henkilövarmenteiden käyttöä “lentämään”. Valtion varmenteen mahdollisen ilmaisen jakelun uskottiin myös saavan ratkaisun kilpailijoilta kovan vastustuksen ja olevan kilpailulainsäädännön vastaista. Ilmaiset palvelut johtavat kehityksen harhaan.

Vaihtoehtona isolla toimikortilla sijaitse-

valle varmenteelle on kännykän SIM-kortille sijoitettu ns. mobiilivarmenne. Ainakaan haastatellut palveluntarjoajat eivät ole toistaiseksi tehneet päätöksiä sen käyttöön otosta. Asiaan ei joko toistaiseksi ollut paneuduttu tai toteutustavan operaattorikeskeisyys koettiin heikkoudeksi. Tapahtumien kiertämisen operaattoriverkon kautta pelättiin olevan hidasta (puhuttiin kymmenien sekuntien viiveistä) tai pelättiin operaattorien rahastusta kyseisellä palvelulla. Hyväksyttävänä toimintamallina esitettiin mobiilivarmenteen käyttäminen paikallisyhteydellä (bluetooth-tekniologia tuotiin esille, soveltuvampi tekniologia ilmeisesti olisi kuitenkin uusi NFC, Near Field Communication -tekniologia). Haastatellut operaattorien edustajat kuitenkin totesivat, että paikallisyhteyksiin pohjautuva toimintamalli merkitsi vastaavia yhteentoimivuushaasteita, kuin on esiintynyt isojen toimikorttien ja kortinlukijoiden tapauksessa. Lisäperusteluna mobiilivarmenteiden paremmuudesta tulevaisuuden ratkaisuna todettiin niiden parempi soveltuvuus uusiin telepalveluihin. Esimerkkinä tuotiin esiin monikanavapalvelut, joissa henkilö voi yhtä aikaa asioida useammalla kanavalla ja tunnistautua samalla yksinkertaisesti mobiilivarmenteella.

Pankkien suhtautumista PKI-varmenteeseen ja sen sisällyttämistä omiin kortteihin pidettiin merkittävänä asiana varmenteiden leviämiseksi⁹. Esitettiin myös näkemys, että paras tapa asian eteenpäin viemiseen on pankkien ja julkisen hallinnon keskinäinen yhteistyö. Näin voitaisiin synnyttää sellaisia tapahtumavolyymeja, että ne imisivät muutkin tahot mukaan. Toisena realistisena vaihtoehtona on mobiilivarmenteiden leviäminen. Realistista on nähdä, että tulevaisuudessakin on rinnakkaisia ratkaisuja. Samoin realismia on, että koska kysymyksessä on miljoonien varmenteiden jakaminen, se tulee vie-

mään pitkäaikaisen ajan ratkaisusta riippumatta.

Haastatteluissa tuotiin esiin periaatteellisenä erona varmenteiden ja tunnistamispalveluiden (TUPAS) välillä se, että varmenteita tarjotaan palveluna yksityishenkilöille ja tunnistamispalveluita palveluntarjoajille. Todellisuudessa tämänhetkinen ero johtuu kuitenkin jo siitä, että pankkitunnisteet ovat jo lähes kaikilla yksityishenkilöillä, jolloin niitä ei enää tarvitse heille markkinoida. Varmenteiden osalta markkinointi on tarpeen. Totta on kuitenkin, että varmenteet tarjoavat tulevaisuuden kansalaisille pankkitunnisteita enemmän palvelumahdollisuuksia.

4.3.3. Sähköisen asiointitunnuksen (SATU) tarve

Haastatteluissa kritisoitiin sähköisen asiointitunnuksen käyttöä. Sen nähtiin johtavan yrityksissä ja virastoissa turhaan välivaiheeseen, kun sähköisen asiointitunnuksen pohjalta pitää selvittää henkilön henkilötunnus. Tällä hetkellä se toimii vain Väestörekisterikeskukselle keinona yksilöidä varmenteen haltija sähköisessä maailmassa. Jotkut kokivat sen turhaksi kustannusrasitteeksi. Yrityksillä on oikeus tallentaa asiakkaidensa SATU niiltä osin, kun asiakkailla sellaiset on.

Sähköisen asiointitunnuksen käyttöön liittyy toisaalta sen avoimuudella ja laajakäyttöisyydellä saatavat hyödyt ja toisaalta sen väärinkäyttöön liittyvät riskit, jotka kasvavat käytön laajentuessa. Toisaalta asiaan liittyy hyvin erilaiset tietosuojakäytännöt eri maissa, myös Euroopan Unionissa. Tietosuojavaltuutettu

⁹ Positiivinenkaan suhtautuminen ei tietenkään poista suurimpia korttipohjaisiin varmenteisiin liittyviä ongelmia (kortinlukija ohjelmistoinen, asennusongelmat ja kanavariippuvuus)

esitettiin keskeisenä tahona, jonka kanssa tulisi pohtia tarpeita ja mahdollisuuksia tehdä asialle jotain. Usea haastateltava esitti näkemyksen, että jos SATU avataan laajempaan käyttöön, sille on tarve. Mahdollisena pidettiin myös, että mikäli SATU päästettäisiin leviämään laajemmin, se voisi johtaa nykyistä turvallisempiin ratkaisuihin.

4.3.4. Valtion rooli turvallisuudessa ja varmenteissa

Terveyssektorilla nähtiin, että varmentajan tulee ehdottomasti olla julkishallinnosta. Haastatteluissa esitettiin myös kysymys, miksi joku kaupallinen taho lähtisi rahallisesti panostamaan yhteiskunnan infrastruktuuriin tavalla, mitä Suomeen tulevat kansainväliset kilpailijat eivät kuitenkaan tekisi. Panostamiseen pitää löytyä liiketoiminnallinen hyöty. Kaupallistenkin tahojen tulee kuitenkin olla joustavasti mukana yhteistoimintaa rakennettaessa.

Enemmistö haastatelluista otti positiivisen kannan valtion aktiiviseen rooliin laatuvarmenteiden tarjoajana. Tämä siitä huolimatta, että EU:n sähköisen allekirjoituksen direktiivi (1999/93/EY) ja sähköisen allekirjoituksen laki /14/2003) toteavat varmennepalvelut markkinaehtoisesti tarjottaviksi palveluiksi (laatuvarmentajalle asetetaan tiettyjä luotettavuusvaatimuksia). Valtion yksikön mukanaolo palvelujen tarjoajana herättää silloin luonnollisesti myös kritiikkiä. Valtion aktiivisella roolilla on vältetty erilaisten ratkaisujen moninaisuus. Silti kilpailun ja markkinaehtoisuuden olemassaoloa pidettiin hyvänä asiana. Esitettiin kuitenkin myös kysymys, tuhlaako viranomaisen verorahoja. Samoin esitettiin kritiikkiä, jos valtio tukee yhteä teknologiaa muiden kustannuksella. Tulisi vain luoda peruspelissäännöt ja universaalisti käytettävät perusprosessit. Kilpailu hoitaa yleensä loput. Valtion asemaa palvelujen tuottajan pidettiin problemaattisena myös

siksi, että se omalla toiminnallaan tappoi orastavan liiketoiminnan vuosituhanen vaihteessa.

Useat haastattelijat näkivät tunnistamisen olevan osa tietoyhteiskunnan infrastruktuuria. Joillakin oli pelkoa, että mikäli jollakin tai joillakin kaupallisilla toimijoilla on merkittävä rooli tunnistamisessa, se voi vaikuttaa heidän kilpailuasemaansa epäterveellä tavalla. He voisivat myös yrittää rajoittaa kilpailijoidensa mahdollisuuksia käyttää tunnistamisratkaisuja. Tämä mahdollisuus on olemassa riippumatta siitä, mikä tekniikka on kysymyksessä. Esimerkki: Kansalainen haluaisi käyttää yrityksen A (jonka asiakas hän on) tunnistusmenetelmää tehdäkseen verkossa sopimuksen siirtyä käyttämään yrityksen B (joka on A:n kilpailija) palveluita. Yritys A ei suostu tekemään sopimusta tällaisesta käytöstä yrityksen B kanssa, jolloin yrityksen A asiakkaat eivät voi tehdä verkossa sopimuksia, joilla siirtyisivät yrityksen B asiakkaaksi.

Vaikka valtion yksiköiden eduksi nähtiin kilpailuneutraliteetti, heikkoutena tuotiin esiin huono kyky edistää asioita aktiivisesti.

Vaihtoehtona on osapuolista riippumaton tunnistuspalveluiden tarjoaja. Yhtenä lainsäädännön epäkohtana yksityisille palveluntarjoajille tuotiin esiin laatuvarmentajiin kohdistuvat sanktiot ja niiden ankaruus. Lainsäädäntö ei ole myöskään teknologianeutraali tässä suhteessa, koska esimerkiksi pankkitunnisteisiin ei liity vastaavia rasitteita.

Haastatteluissa tuotiin esiin huonoja kokemuksia yritysten pitämistä yritysrekistereistä. Ajan mittaan sinne kertyi olemattomia yrityksiä.

4.3.5. Varmenneteknologian käytön yleisiä haasteita

Varmenteen käyttöään lyhyttä kritisoitiin. Toinen keskeinen henkilövarmenteiden käyttöön liittyvä haaste on joko varmenteen ja sen alustan käyttöön liittyminen toisiinsa. Yksi laatuvarmenteeseen liittyvä keskeinen vaatimus on, että sitä vastaavaa salaista avainta ei pidä voida paljastaa eikä siirtää toiseen alustaan. Vaatimus lähtee turvallisuudesta ja liittyy mm. identiteettivarkauksiin. Tästä vaatimuksesta seuraa kaksi haastetta:

- Jos henkilö haluaa vaihtaa palveluntarjoajaa, jolta hän on alustan saanut (esimerkiksi mobiilioperaattori tai pankki), hän ei voi enää käyttää vanhaa varmennetta. Näin henkilö hankkiessaan varmenteen lisää sitoutumistaan mahdollisesti pidemmäksi aikaa yhteen palveluntarjoajaan kuin hän haluaisikaan. Lisäksi suurin osa henkilöistä ymmärtäisi asian vasta halutessaan tehdä kyseisen vaihdon (eli käytännössä liian myöhään). Jos henkilöllä on tietoa, joka on salattu vanhalla varmenteella, pitäisi kyseinen tieto avata ennen varmenteen lakkauttamista ja salata tarvittaessa uudelleen uudella varmenteella.

- Kun alustan käyttöikä päättyy (esimerkiksi 3 vuotta tai 5 vuotta), henkilö saa uuden varmenteen ja hänellä on samat ongelmat kuin edellisessäkin kohdassa. Varmenne ja uusi kortti on siis usein järkevää hankkia (tai palveluntarjoajan antaa) samanaikaisesti. Mitä enemmän kortilla on erilaisia käyttösovelluksia, sitä enemmän hankaluuksia koko kortin vaihtamisesta voi seurata.

Selvää ratkaisua edellä olevaan haasteeseen ei ole olemassa. Tosin on todettava, että ongelma ei koske tunnistamista, koska silloin ei ole olemassa mitään aiemmin salattua tietoa, mitä pitäisi voida uudella varmenteella avata.

PKI-pohjainen varmenneteknologia on edelleen varsin uusi teknologia ja sen tarpeen puolesta esitettävät argumentit ovat usein luonteeltaan teknisiä. Vähemmän on mietitty sen käyttöön ja vaihtoon liittyviä käytötapauksia ja miten niissä tulisi toimia. Esimerkkinä tästä on yksityishenkilön saama sähköisesti allekirjoitettu dokumentti. Henkilön mahdollisuuksia selvittää dokumentin allekirjoittaja ei ole kunnolla suunniteltu. Vastaanottaja näkee varmenteesta henkilön sähköisen asiointitunnuksen ja nimen, mutta samannimisiä henkilöitä voi olla paljonkin ja yksityishenkilö ei voi sähköisen asiointitunnuksen perusteella selvittää allekirjoittajan henkilötunnusta. Toisaalta henkilötunnuskaan ei välttämättä kertoisi vastaanottajalle, kuka henkilö on kysymyksessä (vastaanottaja voi tuntea lähettäjän tiettyyn asiaan liittyneenä, esimerkiksi naapuruus, tietämättä hänen henkilötunnustaan). Tulisi miettiä geneerinen toimintatapa, miten tällaisessa tilanteissa tulisi toimia. Yhtenä esimerkkinä voisi olla, että henkilöillä on sähköinen asiointitunnus käyntikorteillaan, jolloin tutuilta tulleet sähköiset allekirjoitukset voisi täten tarkistaa.

Tarpeena, joihin vielä ei ole vakiintuneita ratkaisuja, tuli esiin kaksinkertainen allekirjoitus, mitä joidenkin organisaatioiden säännöt vaativat. Myös sähköisten allekirjoitusten käyttö valtuutuksissa edellyttää yhteisten ratkaisutapojen kehittämistä.

4.3.6. Kansainväliset tarpeet varmenteiden käytön edistämiseksi

Haastatteluissa pyrittiin selvittämään kansainvälisyyden lisääntymisen luomia tarpeita käyttää varmenteita tai lisätä varmenteiden käyttöä tulevaisuudessa. Esillä olivat seuraavat tilanteet:

- Kansainvälinen kauppa ja siihen liittyvä maksaminen. Maksaminen hoituu tänä päivänä joko kansainvälisten brändi-

en (luottokorttiyhtiöt) avulla tai siten, että asiakas tunnistautuu pankkiinsa TUPAS-tunnisteilla ja pankki hoitaa kansainvälisen maksamisen. Esimerkkinä oli hotelli-toiminta, mikä on kansainvälistä. Henkilöt voivat tehdä varauksensa verkossa mistä päin maailmaa tahansa ja maksaminen tapahtuu hotellissa yöpymisen yhteydessä. Tässä ei ole ollut käytännössä väärinkäytöksiä tai muita ongelmia. Kuitenkin olisi hyvä, jos kuluttajalle olisi turvallisempi vaihtoehto kuin lähettää verkossa luottokortin tiedot.

■ Suomessa olevan tai Suomeen muuttavan ulkomaisen henkilön tarpeet. Haastattelussa tuli esiin vain yksi tilanne, jossa olisi etua henkilön mahdollisuudesta käyttää oman maansa varmenteita Suomessa. Tämä liittyi tapaukseen, jossa ulkomaisella Suomessa olevalla henkilöllä on velvoitteita verohallintoon ja hänen mahdollisuuteensa hoitaa ne verkossa. Kun henkilö asuu täällä pitempään, hän saa Suomen kansalaisvarmenteen halutesaan.

■ Viranomaisten tarpeet vaihtaa tietoja keskenään henkilöistä (esimerkiksi ulkomaisissa työskentelevät). Näissä tilanteissa on selviä ongelmia, mutta käytännössä ne liittyvät eri maiden järjestelmien matalaan automaatioasteeseen ja huonoon keskinäiseen yhteentoimivuuteen. Yksi perimmäisiä vaikeuksia on ihmisten erilainen yksilöintitapa (jossain maassa esimerkiksi nimi + postiosoite). Varmenteisiin ja niiden kansainväliseen yhtenäisyyteen liittyvät ongelmat tulevat käytännössä vasta myöhemmin merkittäviksi.

■ Terveyssektorilla on tarpeita ammattilaiskorttien käyttämiseen kansainvälisesti. Ammattilaiskortteja (Health Professional Cards) on jo monessa maassa, mm. Saksassa, Ranskassa ja Unkarissa. Tällä hetkellä kortit eivät ole keskenään ristiin toimivia, ehkä joskus tulevaisuudessa.

■ Kansainväliset fuusiot voivat synnyttää

tarpeita tai niillä voi olla vaikutusta palveluihin, mitä yritys haluaa tarjota. Esimerkiksi pankkipuolen fuusiot voivat vaikuttaa pankin tarjoamiin tunnistuspalveluihin Suomessa.

Kansainvälisyydestä aiheutuvia varmenteitarpeita ei tällä hetkellä pidetty merkittävänä ja ongelmista ensisijaisena. Joidenkin mielestä ongelma sen sijaan on esimerkiksi ihmisten erilainen yksilöintitieto eri maissa. Erityinen ongelma on erilaiset yksityisyydensuojaperiaatteet eri maissa. Joissain maissa ei esimerkiksi ymmärretä, että yritys voi antaa työntekijänsä tietoja (esimerkiksi verottajan tarvitsemia tietoja) suoraan viranomaiselle.

Näkemykset poikkesivat sen suhteen, tulisiko kansainväliset tarpeet huomioida heti vai myöhemmin. Perusteluna huomiomiselle oli, että tarve kuitenkin tulee ja on jo nyt olemassa, vaikkakin harvoissa tapauksissa. Erityisesti yritysmaailmassa se on jo nyt merkittävä. Perusteluna huomiomatta jättämiselle oli, että asia on vaikea, kansainväliset linjaukset ovat tekemättä ja kansainvälisyyden huomiointi vain monimutkaistaisi tilannetta.

Haastattelussa esitettiin myös, että kansainväliset ratkaisut syntyvät parhaiten kansainvälisen brändin kautta (kaupalliselta pohjalta). Vaihtoehto tälle on roamingtyyppinen malli kansallisten ratkaisujen verkottamiseksi. Mobiilioperaattorit vakuuttivat uskovansa siihen, että mobiilivarmenteet tulevat toimimaan kansainvälisesti. Tähän auttaa ETSIn roaming-malli ja operaattorien vuosikymmenten kokemukset roamingista muissa ratkaisuisa. Suomen kanssa samaan standardiin perustuvia ratkaisuja on jo joko käytössä ja käyttöönottovaiheessa mm. Norjassa, Latviassa, Belgiassa, Virossa, Sveitsissä, Espanjassa, Kuwaitissa ja Sloveniassa.

Haastatteluissa tuotiin myös esiin mahdollisuus levittää suomalainen TUPAS – käytäntö muihin, erityisesti EU-maihin. Tähän vaihtoehtoon ei kovin moni uskonut kuin korkeintaan väliaikaisena lähitulevaisuuden ratkaisuna joissakin EU-maissa.

Enemmistö uskoi, että PKI-pohjainen varmenne on tulevaisuuden kansainvälinen ratkaisu. Silti ei poissuljettu mahdollisuutta, että suomalainen TUPAS-ratkaisu leviäisi ainakin joihinkin EU-maihin.

4.3.7. Kansallisen yhteistyön tarve

HST-ryhmä on tehnyt yhteistyötä kansalaisvarmenteen edistämiseksi. Ryhmä on avoin, valtion kansalaisvarmenteen yleistymistä edistävien sirukorttien liikellelaskija-yhteisöjen muodostama yhteistyöelin. Ryhmän jäseneksi voi liittyä muitakin laatuvarmentajia, joiden kanssa kehitetään varmenteiden yleistä käytettävyyttä ja tunnettuutta.

HST-ryhmä on haastateltavien mielestä tehnyt hyvää työtä kansalaisvarmenteen ja siihen liittyvien käytäntöjen edistämisessä. Toisaalta esiin tuli kuitenkin tarve avoimemmalle ja laajemmalle keskustelulle varmenteisiin, tunnistamiseen ja yleensä tietoverkkojen turvallisuuteen kohdistuen. Enemmistö haastatelluista piti toivottavana yhteistyöryhmän (foorumin) perustamista, kolmannes haastatelluista suhtautui ajatukseen epäillen ja pari kielteisesti. Keskeisenä syynä epäilyyn oli, että osallistajat kuitenkin katsovat asioita lähtökohteisesti omien toimintojensa ja liiketoimintamahdollisuuksien näkökulmasta, jolloin todellisia tuloksia on vaikea saada aikaan.

Valtion tulisi olla vahvasti mukana kansallisessa yhteistyössä.

4.4. Tulevaisuuden tarpeet

Haastatteluissa korostuivat tämänhetkiset tilanteet ja lähitulevaisuudessa nähtävissä olevat tarpeet ja kehitys erityisesti tunnistamisessa ja palveluiden tarjoajien näkökulmasta. Tietoverkkojen turvallisuus on ollut erittäin runsaasti esillä viimeisten vuosien aikana ja jatkuvasti on korostettu tietoverkkoihin liittyviä uhkia. Tässä mielessä haastatteluissa esiin tuotu tyytyväisyys nykyratkaisuihin ja -tilanteeseen oli yllättävä. Yleisimpänä perusteluna oli toteamus, että verkkoasioinnissa suoritetaan kuitenkin paremmin henkilön (esimerkiksi allekirjoittajan todellinen henkilöllisyys) tunnistaminen kuin perinteisessä fyysisessä maailmassa.

Suurimmat tunnistamiseen liittyvät tulevaisuuden uhkakuvat esitetään muista maista. Esimerkiksi Yhdysvalloissa todetaan identiteettivarkaudet nopeimmin kasvavaksi rikollisuuden lajiksi. Englannissa arvioidaan, että ne vaikuttavat siellä 100 000 kansalaiseen joka vuosi. Aberdeen Group on arvioinut, että identiteettivarkauksien kustannukset maailmanlaajuisesti ovat vuoden 2005 loppuun mennessä ylittäneet 2000 miljardia \$. Ihmiset, joiden identiteetti on varastettu, voivat joutua kuukausia puhdistamaan nimeään erilaisista luottotieto- ym. rekistereistä.

Haastattelut toivat esiin yhden Suomessa koetun uhkan, phishingin, pankkien TUPAS-tunnisteisiin kohdistuvana. Julkisuuressakin olleiden tietojen mukaan siitä aiheutuneet menetykset ovat olleet noin 60 000 euroa. Toisena uhkana tuli esiin kansalaisten yleisen epäluottamuksen syntyminen verkkopalveluihin, jos esiintyy liikaa väärinkäytöksiä. Sen toteutuminen olisi jo merkittävä takaisku tietoyhteiskunnan kehittämisessä.

Enemmistön selvä kanta oli, että tulevaisuuden tunnistaminen tulee pohjautumaan

PKI-varmenteisiin. Ne mahdollistavat tunnistamisen ohella myös muita turvallisuutta parantavia käytäntöjä, edellä todetut sähköiset allekirjoitukset, oikeuksien esittämiset, tiedon muuttamattomuuden jne. Samoin uskottiin, että markkinoilla ei tule olemaan ainoastaan yhtä ratkaisua vaan useampi erilainen ratkaisu tulee elämään rinnakkain, näiden joukossa kertakäyttösalasanat. Ajasta, jolloin varmenteet tulevat Suomessa ja Euroopassa laajaan käyttöön, ei kukaan uskaltanut sanoa mitään varmaa. Kuitenkin todettiin, että liiketoiminnassa ei tänä päivänä voi lähteä siitä, että Euroopassa olisi viiden vuoden kuluessa yhtenäiset ratkaisut. Teknologia itsessään ei ole ainoa määräävä tekijä, vaan turvallisuuteen voidaan vaikuttaa merkittävästi myös käytettävillä työprosesseilla.

4.5. Johtopäätökset ja ehdotukset

4.5.1. Johtopäätöksiä

Näkemykset Suomessa ovat tällä hetkellä voimakkaasti jakaantuneet, toisaalta TUPAS-palveluiden kannattajiin ja toisaalta PKI-varmenteiden käytön edistäjiin. Edelliset perustavat puoltavan kantansa TUPAS-palveluiden valmiuteen ja levineisyyteen, jälkimmäiset PKI-tekniikan osapuoliriippumattomuuteen, sen saamaan suureen kansainväliseen huomioon ja teoreettiseen paremmuuteen. Kukaan ei täysin varmasti pysty sanomaan, miksi tilanne kehittyy tulevaisuudessa.

Vaikka erityisesti palveluntarjoajat ovat tyytyväisiä tilanteeseen Suomessa, tietoverkkojen turvallisuus edellyttää jatkuvaa kehittämistä. Tunnistaminen on tällä hetkellä keskeinen tarve ja TUPAS-palvelut riittävät siihen. Tarpeet tulevat kuitenkin monipuolistumaan ja myös tarve kansainvälisiin ratkaisuihin lisääntyy. On mahdollista, että TUPAS-tunnisteet tulevat lähitulevaisuudessa täyttämään osittain

kansainvälisiäkin tunnistamistarpeita. Kuitenkin pitkällä aikavälillä ratkaisut saattavat pohjautua PKI-pohjaisiin varmenteisiin. Tätä puoltaa aiemmin raportissa todetun tarpeiden monipuolistumisen lisäksi sähköisen liiketoimintojen volyymin kasvu tulevaisuudessa, mikä houkuttelee rikollista toimintaa. Kansainvälisten ratkaisujen harmonisoituminen EU-alueellakin tullee kestämaan vuosia. Markkinoilla tullee olemaan rinnakkaisia ratkaisuja. PKI-pohjaisten varmenteiden menestymisen keskeinen edellytys on, että yhtenäisten vakiintuneiden käytäntöjen kehittämiseen ja kansainväliseen harmonisointiin saadaan merkittävästi nykyistä enemmän vauhtia. Tämä ei koske pelkästään varmenteita, niihin liittyvää tekniikkaa ja käyttötapoja vaan myös muita tarpeellisia perusedellytyksiä, esimerkiksi henkilöiden riittävän yhtenäistä kansainvälistä yksilöintiä.

Varmenteissa menestynevät ratkaisut:

- joissa ratkaisu on paketoitu siten, että niiden käyttöönotto ja käyttö on yksinkertaista
- joissa roaming eri varmentajien ratkaisujen välillä toimii käyttäjille näkymättömästi, ja myös kansainvälisesti
- jotka houkuttelevat palveluntarjoajia liittämään ne palveluihinsa
- jotka ovat riittävän turvallisia ja
- joissa varmenteet on sijoitettu alustalle, jota sen haltija käyttää aktiivisesti (esimerkiksi pankkikortti tai kännykkä).

Tietoverkoissa yksilön tunnistamisen ja tietosuojan välinen tasapaino on tärkeää. Sähköisen asiointitunnuksen (SATU) käyttöperiaatteet kaipaavat uudelleen harkintaa, jotta sen mahdollistamat hyödyt pystyttäisiin saavuttamaan kuitenkin vähentämättä yksilöiden tietosuojaa.

Pankkien tarjoama TUPAS-tunnistuspalvelu

on tällä hetkellä todellisuudessa henkilön sähköisen tunnistamisen infrastruktuuri yhteiskunnassa. Pankitkin tuovat esiin tarpeen sen avaamiseen nykyistä paremmin kaikkeen käyttöön ja myös valmiuden keskustella sen toteuttamistavasta. Neutraaliin tunnistuspalveluun tulisi myös harkita osittaisen tunnistamisen (esimerkiksi tunnistettavan iän) mahdollisuutta.

Sähköisen allekirjoituksen lainsäädäntö ei tällä hetkellä ole tasapuolinen erilaisille teknologioille, mikä heijastuu myös näiden teknologioiden käyttöön tunnistamisessa. Yksimielisiä ei myöskään olla, voiko lakia soveltaa tunnistamiseen eikä vain pelkkään allekirjoitukseen. Näitä kohtia tulisi uudelleen harkita ja tarpeellisin osin selvittää.

Tietoverkkojen turvallisuuden ja varmenteiden käytön alueella on monia asioita, joita tulisi edistää ja luoda yhteistä tahtotilaa. Haastattelun pohjalta enemmistö kannatti yhteistyöryhmän (foorumin) perustamista luomaan yhteistä tahtotilaa ja parempia ratkaisuja alueelle.

4.5.2. Ehdotus

Perustetaan Luottamusfoorumi edistämään luottamuksen rakentamista tietoverkkojen käyttöön. TIEKE toimii foorumin kokoonkutsujana.

Foorumin keskeiset lähiajan tavoitteet ovat:

- sopia yhteistyön muodoista ja periaatteista (huomioiden vapaa kilpailu)
- muodostaa yhteinen näkemys TUPAS-tunnistuksen kehittämisestä osapuolineutraaliksi palveluksi ja tarjottavista lisäpalveluista (osittainen tunnistus, profiilitietopalvelu)
- sopia mobiilivarmenteen toteuttamisperiaatteista palveluntarjoajien kanssa
- sopia yhteisistä varmenteen käyttöta-

voista niiltä osin kuin se nähdään tarpeelliseksi

- kehittää sähköisen asiointitunnuksen käyttöä
 - kartoittaa alueen lainsäädännön kehittämistarpeita, mm selkeyden lisääminen ja teknologianeutraalisuus
 - seurata kansainvälistä kehitystä ja muodostaa yhteinen näkemys kansallisten kommenttien pohjaksi.
- Foorumin toimintaan voivat halukkaat osallistua, keskeisiä kutsuttavia tahoja ovat:
- toimintaa ohjaavat viranomaiset pankit
 - mobiilioperaattorit
 - luottamuspalveluja käyttävät yritykset (verkkopalveluiden tarjoajat)
 - luottamuspalveluja käyttävät viranomaiset
 - luottamuspalveluja tarjoavat viranomaiset
 - tietotekniikkaratkaisujen toimittajat
 - kansalaisten edustajat.

Foorumin toiminnan kuluja kattamiseksi osallistujamaksujen lisäksi haetaan julkista rahoitusta keskeisille kehittämishankkeille.



TIEKE TIETOYHTEISKUNNAN
KEHITTÄMISKESKUS RY
www.tieke.fi

