LAUREA

Henkilön sähköinen vahva tunnistus

Mikkola, Teija

Leppävaara 2009

Laurea-ammattikorkeakoulu
Laurea Leppävaara

HENKILÖN SÄHKÖINEN VAHVA TUNNISTUS

Teija Mikkola
Tietojärjestelmäosaamisen koulutusohjelma, ylempi AMK
Opinnäytetyö
Maaliskuu 2009

Laurea-ammattikorkeakoulu Tiivistelmä
Laurea Leppävaara
Tietojärjestelmäosaamisen koulutusohjelma, ylempi AMK

Teija Mikkola

Henkilön vahva sähköinen tunnistaminen

Vuosi 2009 Sivumäärä 65

Tämän suunnittelutieteellisen toimintatutkimuksen tavoite on selvittää, mikä on henkilön vahva sähköinen tunnistaminen ja milloin sen käyttö on tarpeen verkkopalvelussa. Tutkimuksessa selvitetään keskeiset henkilön vahvojen sähköisten tunnistustapojen vaihtoehdot Suomessa. Tutkimuksen tavoitteena on myös soveltaa kerättyä tietoa Tapiola-ryhmän yritysasiakkaille tarjottaviin verkkopalveluihin. Tutkimuksen teoria-osuudessa perehdytään verkkopalvelujen luokittelutyyppeihin, tunnistautumisen luotettavuuteen sekä käyttäjäidentiteetin luotettavuuteen.

Käytössä olevia henkilön vahvoja sähköisiä tunnistustapoja ovat mm. pankkien tarjoama Tupas-palvelu, Verohallinnon ja Kelan Katso-tunniste, Väestörekisterikeskuksen ylläpitämä sähköinen henkilökortti sekä mobiilivarmenne. Yleisin ja tunnetuin henkilön vahva sähköinen tunnistustapa Suomessa on pankkien tarjoama Tupas-palvelu. Sen etuna on, että palveluntarjoajan ei tarvitse erikseen ylläpitää ja jakaa käyttäjätunnuksia ja salasanoja, koska lähes kaikilla kansalaisilla on jo käytössä jonkin pankin verkkopankkitunnukset.

Valtionvarainministeriö Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI on luokitellut verkkopalvelut sisältönsä ja luonteensa mukaan seitsemään päätyyppiin, joiden tarkoituksena on auttaa palveluntarjoajaa käytännön verkkopalvelujen tunnistamiselle asetettavan vaatimustason määrittämisessä. Sähköinen henkilökorttihanke ei ole lähtenyt liikkeelle toivotusti mutta tällä hetkellä vahvan sähköisen tunnistamisen yhtenäistämiselle on selkeä tarve ja tahtotila. Suomen kansalliset linjaukset sekä lakiesitykset edistävät tätä hanketta. Toistaiseksi käyttökelpoisin vahva sähköinen tunnistus on edellä mainittu pankkien tarjoama Tupas-palvelu, koska se on laajassa käytössä ja käyttäjät tuntevat ja luottavat Tupas-palveluun.

Asiasanat
Vahva sähköinen tunnistaminen, Tupas, mobiilitunnistaminen, verkkopalveluiden luokittelu

Laurea University of Applied Sciences Abstract
Laurea Leppävaara
Master Degree in information Systems

Teija Mikkola

Person's strong electronic identification

Year 2009 Pages 65

The aim of this study is to clarify what is the person's strong identification in web-services and when its use is necessary in web hosting. Most relavant strong identification methods used in Finland are described. One of the goals is also to apply gathered knowledge in Tapiola-group's online/web services. In theory part of the study, classification of web services, authenticity of identification and authenticity of the user identity are discussed.

There are many identification methods such as Tupas certification service offered by banks, Katso ID offered by Finnish tax administration and Kela, Identity card and mobile identification maintained by Population Register Centre. In Finland, the most widely used and known identification method is Tupas certification service. The benefit of it is that most of citizens have already username and passwords. Thus, there is no need for service provider to maintain and deliver usernames and passwords.

The Ministry of Finance, The Government Information Security Management Board (VAHTI) has classified web services in their contents and characters in seven main classes. These classes will help service provider to demand correct standard. Identity card -project has not started as planned but nowadays there is strong need and wish to integrate person's strong identification methods in Finland. Finland's national policy and government bill promotes this project. So far the Tupas certification service is useful method, since it is widely used and known to be reliable.

Key words
Strong identification, Tupas certification service, mobile identification, Identity card

SISÄLLYS

1 TAUSTAA

Internetin käyttäjät alkavat vähitellen tottua sähköisiin palveluihin ja sähköiseen asiointiin Internetissä. Sähköinen asiointi on miellyttävää, koska asioita voi hoitaa paikasta ja ajasta riippumatta ilman jonottamista. Sähköinen asiointi Internetissä onkin yleistynyt nopeasti ja merkittävästi viime vuosina. Kalakota ja Robinson (2001) ovat tunnistaneet kolme kronologista vaihetta Internetin kehityksessä palvelukanavana. Ensimmäisessä vaiheessa vuosina 1994 – 1997 tärkeää oli, että yrityksillä oli omat kotisivut Internetissä. Toisessa vaiheessa vuosina 1997 – 2000 voimakkaana trendinä oli kauppapaikan toteuttaminen Internetiin. Internetissä oli mahdollisuus myydä ja ostaa tuotteita sekä palveluja. Kolmannessa vaiheessa palvelun tarjoajat alkoivat enemmän ajatella asiakkaita ja heidän tarpeitaan sekä strategioita, joiden avulla Internetistä saataisiin yhä enemmän liiketoiminnallista hyötyä. Kolmas vaihe on määritelty e-liiketoimintavaiheeksi vuodesta 2000 eteenpäin. Liiketoimintaihmiset alkoivat nähdä Internetin mahdollisuudet palvelukanavana. E-liiketoiminta muuttuukin yhä enemmän e-palveluiksi. (Ahonen 2007, 264.)

Yhä useammat yritykset tuottavat Internetiin erilaisia lomakkeita ja toimintoja, joiden avulla asiakkaat voivat itse yllä pitää asiakkuuteensa liittyviä tietoja. Internet on nopea ja vaivaton kanava hoitaa rutiiniasiat. Kuluttajat käyttävät mielellään yritysten tarjoamia verkkopalveluita, koska he voivat tehdä tarvittavat muutokset silloin kun se heille parhaiten sopii.

Internet on nykyisin merkittävä palvelukanava. Muun muassa suomalaiset pankit ovat edelläkävijöitä sähköisten palvelujen kehittämisessä ja käyttöönottamisessa. Kuluttajat haluavatkin valita omiin tilannesidonnaisiin tarpeisiinsa erilaisia asiointitapoja – sama palvelu voidaan hankkia sekä sähköisesti että henkilökohtaisesti. Suuntaus on siis kohti monikanavamalleja ja -ratkaisuja. (Kuusela & Rintamäki 2002, 9, 85.) Myös vakuutusasiointi Internetissä on yleistymässä. Verkossa näkyminen on osa nykyaikaista liiketoimintaa. Vakuutusyhtiöt kasvattavat ja kehittävät voimakkaasti verkkoliiketoimintaansa. Yhä useammat vakuutusyhtiöt tarjoavat Internetissä enemmän tietoa vakuutuksista, mahdollisuuden ostaa vakuutuksia sekä hoitaa erilaisia vakuutusasioita. (Järvinen, Eriksson, Saastamoinen & Lystimäki 2001, 1.) Näin ollen myös tunnistusta vaativien verkkopalvelujen määrä on lisääntynyt. Vakuutusyhtiöt tarjoavat palveluita ekstranettien eli suljettujen verkkopalvelujen välityksellä, joita voivat käyttää vain palveluntarjoajien sallimat käyttäjät.

Luotettavan asiointitapahtuman lähtökohta on, että asiakas tunnistetaan. Sähköisessä asioinnissa henkilön tunnistaminen luotettavasti ei tapahdu samalla tavalla kuin esimerkiksi kasvotusten tai puhelimitse tarjottavassa asiakaspalvelussa. Verkkopalvelun käytön luottamustaso eli varmuus käyttäjän todellisesta identiteetistä on suoraan verrannollinen siihen, miten suuria riskejä palvelun väärinkäyttöön liittyy tai miten luottamuksellisia tietoja palvelussa käsitellään. Internetissä tietoturvavaatimukset korostuvat varsinkin silloin, kun asiointi käsittää henkilökohtaisia tai muuten arkoja tietoja.

Yleisemmin käytetty tunnistusmenetelmä Suomessa on käyttäjän itsensä luoma käyttäjätunnus ja salasanayhdistelmä. Tätä pidetään heikkona tunnistusmenetelmänä. Menetelmä ei ole kovin käyttäjäystävällinen, koska lukuisten käyttäjätunnusten ja salasanojen hallinta on käyttäjän kannalta hankalaa. Menetelmään liittyy myös huomattavia tietosuoja- ja tietoturvaongelmia. Menetelmän etu on se, että siitä ei yleensä aiheudu kustannuksia käyttäjälle. (Valtiovarainministeriö VAHTI 2006.)

2 TAVOITE, TUTKIMUSMENETELMÄT JA KÄSITTEET

2.1 Tutkimuksen tavoite

Tutkimuksen tarkoituksena on selvittää, mikä on henkilön vahva sähköinen tunnistaminen ja milloin se on tarpeen verkkopalveluissa. Lisäksi tutkimuksessa selvitetään keskeisten vahvojen sähköisten tunnistustapojen vaihtoehdot ja käyttömahdollisuudet Suomessa. Tarkoituksena on siis luoda kokonaiskuva henkilön vahvan sähköisen tunnistamisen menetelmistä Suomessa. Tutkimuksen lopussa teorian toimivuutta tutkitaan Tapiola-ryhmän yritysasiakkaiden verkkopalvelujen kautta (ks. luku 11). Tämän tutkimuksen tavoitteena on luoda vahva sähköinen tunnistamisratkaisumalli, joka voidaan ottaa tuotantokäyttöön yritysasiakkaan verkkopalvelussa.

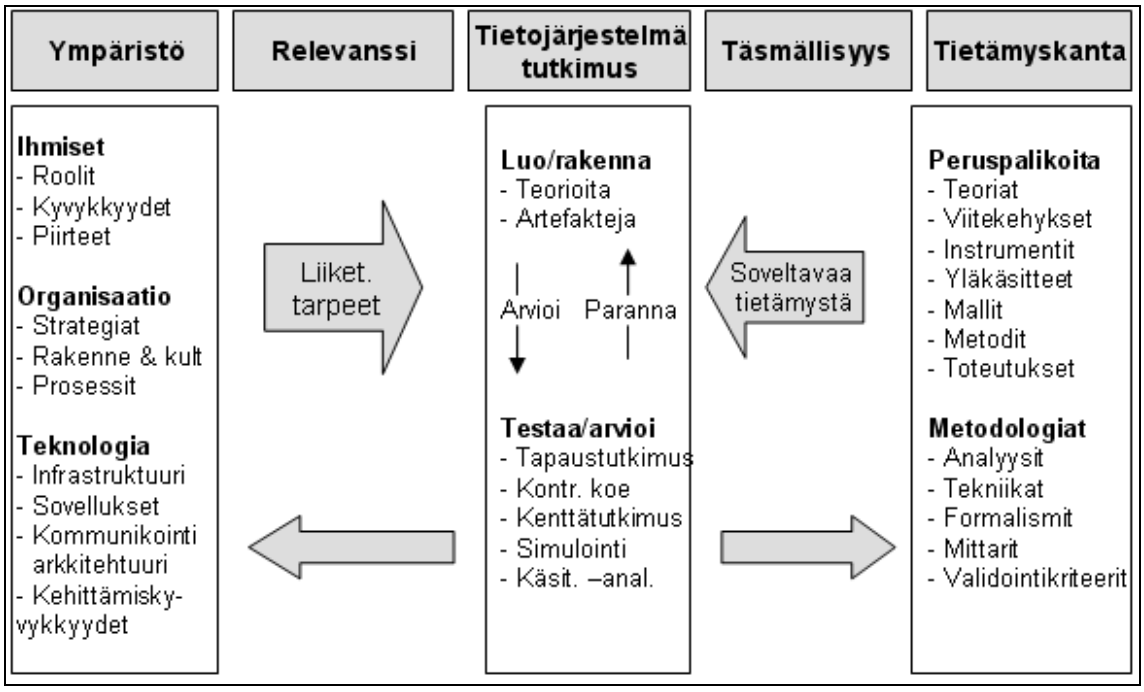
2.2 Tutkimuksen aineisto

Teoreettisen tutkimusaineiston lähteenä on käytetty sähköiseen tunnistamiseen liittyvää kirjallisuutta ja tieteellisiä artikkeleja.

2.3 Toimintatutkimus ja tietojärjestelmätutkimus

Tämän tutkimuksen tutkimusmenetelmänä on suunnittelutieteellinen toimintatutkimus.

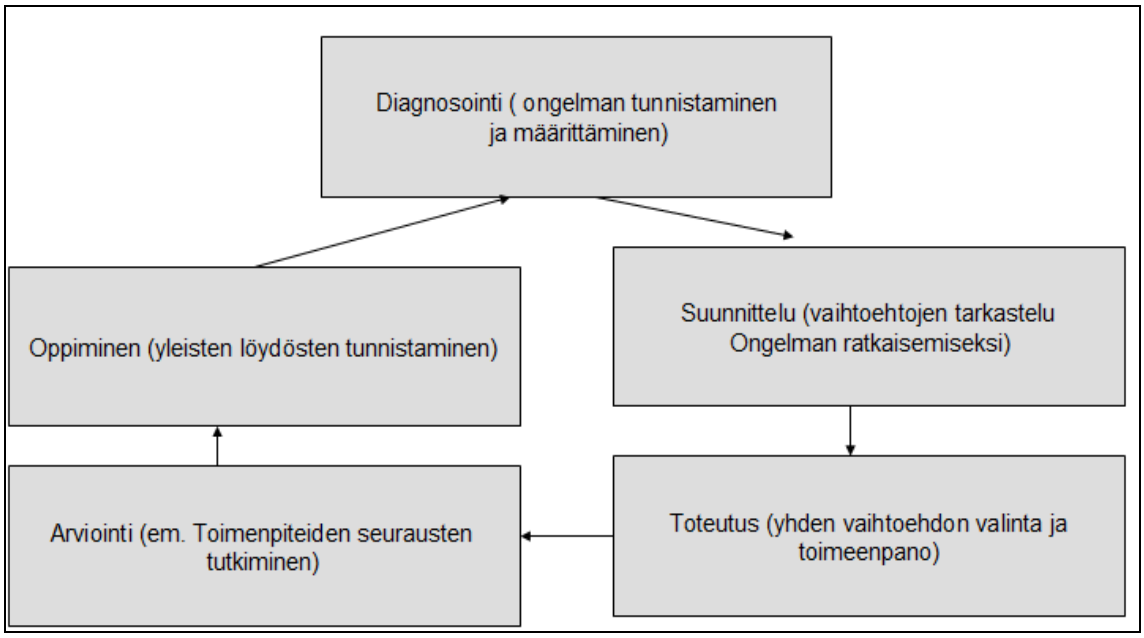
Suunnittelutieteen tarkoituksena on tuottaa sellaista uutta tietämystä, jota ammattilaiset voivat käyttää suunnittelu- ja konstruointiongelmien ratkaisemisessa (Aken 2005). Jokin tietty tutkimus kuuluu todennäköisesti suunnittelutieteen piiriin, jos sen tutkimuskysymyksessä esiintyy verbi rakentaa, muuttaa, vahvistaa tai laajentaa (Järvinen & Järvinen 2004). Suunnittelutiedettä voidaan edistää toimintatutkimuksella. Termin toimintatutkimus on todennäköisesti ensimmäisenä ottanut käyttöön sosiaalipsykologi Kurt Lewin vuonna 1946 tutkiessaan ryhmien dynamiikkaa. Toimintatutkimus on tutkijan toimimista yhtäältä käytännön ongelman ratkaisemiseksi ja samalla toisaalta sellaisen tiedon hankkimiseksi, jolla on tieteellistä mielenkiintoa. Toimintatutkimuksen kaksi tärkeää lähtökohtaa ovat käytännön ymmärtäminen sekä tilanteen parantaminen ja osallistuminen. Toimintatutkimuksen kolme minimivaatimusta on, että tutkimuksen aihe nousee liiketoiminnasta, tutkimus etenee syklisesti suunnittelun, toiminnan, tarkkailun ja pohdinnan kautta sekä projektissa on mukana vastuullisia henkilöitä, jotka kontrolloivat käytännön toimintaa ja osallistumista (Carr & Kemmis 1986).



Kuvio 1. Tietojärjestelmätutkimuksen viitekehys (Hevner 2004)

Kuviossa 1 on esitetty Hevnerin (2004) tietojärjestelmätutkimuksen viitekehys ymmärtämiselle, toteutukselle ja arvioinnille. Viitekehyksen ympäristö koostuu ihmisistä, liiketoimintaorganisaatiosta ja niiden olemassa olevista tai suunnitelluista teknologioista. Ihmisten kyvykkyydet, roolit ja piirteet muotoilevat heidän näkemyksiään liiketoimintatarpeista. Liiketoimintatarpeita punnitaan suhteessa strategioihin ja nykyisiin liiketoimintaprosesseihin sekä nykyiseen teknologiseen infrastruktuuriin (Hevner 2004). Tietojärjestelmätutkimus voi olla käyttäytymistieteellinen teoriaa luova tai teoriaa selittävä tai ennustava tutkimus liiketoiminnan tarpeisiin liittyen. Toinen vaihtoehto on, että se suunnittelutieteellinen tutkimus, jossa rakennetaan ja arvioidaan artefakti liiketoiminnan tunnistettuihin tarpeisiin. Käyttäytymistieteellinen tutkimus tavoittelee totuutta, kun taas suunnittelutieteellinen tutkimus hyötyjä (Järvinen&Järvinen 2005). Tietämyskanta puolestaan koostuu peruspalikoista ja metodologioista. Peruspalikoilla käsitetään teorioita, viitekehyksiä, instrumentteja, yläkäsitteitä, malleja, metodeja ja toteutuksia, joita käytetään teorian luontivaiheessa.

Toimintatutkimus on yleensä tulevaisuuteen suuntautuvaa, tiivistä yhteistyötä tutkijan ja tutkijayhteistyön tai projektinjäsenten kanssa. Toimintatutkimus aiheuttaa järjestelmän kehittymistä ja luo tiiviin yhteyden teorian ja käytännön välille. Toimintatutkimuksessa ratkaistaan käytännön ongelma yhdessä ns. asiakkaan kanssa. Davisin (1998) mukaan konstruktiivinen ajattelu ja tutkimus keskittyvät aina jonkin rakenteen kanssa toimimiseen. Kuviossa 2 on esitetty toimintatutkimuksen syklinen kehitysprosessi. Tavallisesti toimintatutkimus sisältää seuraavat viisi vaihetta: diagnosointi, suunnittelu, toteutus, arviointi ja oppinen (Susman & Evered 1978). Vaiheiden määrä vaihtelee toimintatutkimuksesta riippuen. Suunnitteluvaiheessa voi olla useampi sykli.



Kuvio 2. Toimintatutkimuksen syklinen kehitysprosessi (Susman & Evered 1978)

Fräntti ja Pirinen (2005, 64) määrittelevät teoksessaan Tutkiva oppiminen integratiivisessa oppimisympäristössä – BarLaurea ja REDlabs, että toimintatutkimuksen keskeiset vaiheet ovat:

- Tilanteen kartoitus ja lähtökohtien selvittäminen.
- Toiminnan tai vaikuttamisohjelman ideointi.
- Toiminnan käynnistäminen ja toteuttaminen.
- Evoluution havainnointi, vaikutusten seuranta ja havaintojen teko.
- Jälkihoito, eli uusmuotoisen toiminnan mahdollinen juurruttaminen tai korjaaminen.

2.4 Tutkimuksen rajaus ja sisältö

Tutkimus on rajattu keskittymään henkilön vahvaan sähköiseen tunnistamiseen. Käyttöoikeushallintaa ei käsitellä tässä tutkimuksessa.

Luku 3 käsittelee verkkopalvelujen luokittelua. Luvussa 4 kuvataan tunnistamista ja sen luotettavuutta. Luku 5 käsittelee PKI julkisen avaimen infrastruktuuria. Luvussa 6 kuvataan kansalaisvarmenne, kun taas luvussa 7 kuvataan Tupas-palvelu. Luku 8 käsittelee Katso-organisaatiotunnistetta. Luvussa 9 kuvataan Mobiilivarmennetta. Luku 10 esittelee vahvan sähköisen tunnistamisen linjaukset Suomessa. Luvussa 11 sovelletaan teoriaa Tapiolan verkkopalveluihin ja annetaan vastaukset tutkimuksen

tavoitteisiin. Luvussa 12 esitetään tutkimuksen kulku toimintatutkimusmenetelmän mukaisesti. Luvussa 13 esitetään työn johtopäätökset.

2.5 Käsitteet

Seuraavassa on määritelty tutkimuksessa käytettäviä käsitteitä.

Aikaleima:
Tapahtumatietoon tai viestiin on liitetty tieto lähetys-, saapumis- tai käsittelyajankohdasta sekä mahdollisesti tapahtuman osapuolista. Varmennetulla aikaleimalla saadaan aikaan viestin lähettämisen tai vastaanottamisen kiistämättömyys.

Biotunnistus tai biotunnistaminen:
Ihmisen fyysiseen ominaisuuteen, kuten kasvojen muotoon, sormenjälkiin, kämmenen verisuonistoon, ääneen tai silmän iirikseen perustuva tunnistus.

Epäsymmetrinen salaus:
Tiedon salausta, jossa salauksen ja sen purkamiseen käytetään eri avainta (ks. PKI).

Eväste tai cookie:
Web-palvelimesta verkkoaseman web-selaimeen palvelimen lähettämä tietue, jonka avulla palvelun ja selain voivat pysyä yhteydessä toisiinsa vaikka fyysinen yhteys välillä katkeaisikin.

Identification tai tunnistaminen:
Menettely, jossa tunnistetaan (yksilöidään) tietojärjestelmän käyttäjä. Käyttäjä voi olla henkilö, organisaatio tai toinen laite.

Julkinen avain:
Julkisen avaimen menetelmä toimii seuraavalla tavalla: Molemmilla osapuolilla on kaksi avainta, salainen ja julkinen. Viesti salataan vastaanottajan julkisella avaimella ja viestin purkaminen tapahtuu vastaanottajan salaisella avaimella. Julkinen avain voidaan jakaa kaikille, joiden kanssa on tarpeen vaihtaa tietoa julkisesti. Julkisen avaimen huonona puolena on sen hitaus verrattaessa salaiseen avaimeen. Tämän takia molempia menetelmiä käytetäänkin usein yhdessä siten, että julkista avainta käytetään tiedon todennukseen, kiistämättömyyteen ja viestin eheyden varmistamiseen ja salaista avainta puolestaan käytetään tiedon kryptaamiseen tiedonsiirtoa varten.

Kansalaisvarmenne:
Kansalaisvarmenteilla tarkoitetaan esimerkiksi poliisin myöntämällä henkilökortilla tai vastaavan turvatason tarjoamalla kortilla olevia Väestörekisterikeskuksen myöntämiä varmenteita.

Katso -organisaatiotunniste:
Katso-organisaatiotunniste ja valtuutushallinta on verohallinnon sekä Kelan yhteinen maksuton palvelu organisaatioiden tunnistamiselle viranomaisasioinnissa.

Laatuvarmenne:
Laatuvarmenne täyttää sähköisen allekirjoituksista annetuissa laissa säädetyt vaatimukset ja sen on myöntänyt säädetyt vaatimukset täyttävä varmentaja. Viestintävirasto valvoo Suomessa laatuvarmenteita myöntäviä varmenneviranomaisia, laatuvarmentajia.

Mobiilitunnistaminen:
Matkapuhelimen SIM-kortin avulla tapahtuva tunnistaminen. Tunnistaminen voi tapahtua seuraavia tekniikoita käyttäen:

- tunnistetaan matkapuhelinliittymä puhelinsoiton tai lähetetyn tekstiviestin perusteella tai
- tunnistetaan SIM-kortilla oleva tai siihen liitetty varmenne.

PKI:
Public Key Infrastructure eli julkisen avaimen järjestelmä. Luottamuksen jakamiseen ja julkisen ja yksityisen avaimen käyttöön pohjautuva epäsymmetrinen salausjärjestelmä, jossa kolmas luotettu osapuoli hallinnoi julkisia avaimia. Yksityisen avaimet ovat vain omistajansa hallinnassa. Salaus voidaan tehdä joko julkisella tai yksityisellä avaimella, ja purkaa avainparin toisella puoliskolla.

Salainen avain:
Käytettäessä salaisen avaimen menetelmää viestin salaaminen tapahtuu siten, että viesti salataan ja avataan samalla avaimella. Salaisen avaimen menetelmässä on ongelmana se, miten saada avain molemmille käyttäjille ilman vaaraa, että se joutuu ulkopuolisten käsiin. Salaisen avaimen menetelmä on nopea, mikä tarkoittaa sitä, että sillä voidaan suojata suuriakin lähetyksiä tiedonsiirtonopeuden kärsimättä. (Internetopas.fi.)

SSL:
SSL on salausprotokolla, jolla voidaan salata tunnistus käyttäjän ja palvelimen välillä, tunnistaa palvelin ja neuvotella liikenteessä käytettävästä salauksesta. SSL on nykyisin yleisin pankkipääteyhteyksien suojausmenetelmä.

Symmetrinen salaus:
Symmetrisessä salauksessa viestin salauksen purkamiseen tarvittava avain on suoraan johdettavissa salausavaimesta. Käytännössä symmetrisissä salausalgoritmeissa viesti salataan ja salaus puretaan samalla avaimella. Symmetriset salausalgoritmit jaetaan yleisesti jono- ja lohkosalausmenetelmiin.

Tapiola-ryhmä:
Tapiola on suomalainen vakuutus- ja finanssiyhtiöryhmä, johon kuuluu neljä keskinäistä vakuutusyhtiötä – Keskinäinen Vakuutusyhtiö Tapiola, Keskinäinen Eläkevakuutusyhtiö Tapiola, Keskinäinen Henkivakuutusyhtiö Tapiola ja Yritysten Henkivakuutus Oy Tapiola – sekä Tapiola Omaisuudenhoito Oy, Tapiola Rahastoyhtiö Oy ja Tapiola Pankki Oy. Yhtiöryhmän omistavat sen asiakkaat eli vakuutuksenottajat.

Tupas tai Tupas-palvelu:
Tupas on suomalaisten pankkien yhteinen tunnistamispalvelu. Tupas-palvelu on Finanssialan Keskusliiton määrittelemä tapa tunnistaa verkkopalvelujen käyttäjiä pankkien verkkopalvelutunnuksilla.

VAHTI:
Valtiovarainministeriö on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimeksi.
VAHTI käsittelee valtionhallinnon tietoturvallisuutta koskevat säädökset, ohjeet, suositukset ja tavoitteet sekä muut tietoturvallisuuden linjaukset sekä ohjaa valtionhallinnon tietoturvatoimenpiteitä. VAHTI toimii hallinnon tietoturvallisuuden ja tietosuojan kehittämisestä ja ohjauksesta vastaavien hallinnon organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä sekä edistää verkostomaisen toimintatavan kehittämistä julkishallinnon tietoturvatyössä. VAHTI:n tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta. VAHTI:n toimialaan kuuluvat kaikki valtionhallinnon tietoturvallisuuden osa-alueet: hallinnollinen

tietoturvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus ja käyttöturvallisuus.

Vahva tunnistaminen:
Käyttäjän tunnistaminen käyttämällä vähintään kahta eri todennustapaa. Vahvaa tunnistamista on esimerkiksi se, kun pankkikortilla maksettaessa maksajalta vaaditaan sekä pankkikorttia että siihen liittyvän tunnusluvun tietämistä.

Verkkopalvelu:
Tässä työssä verkkopalvelulla tarkoitetaan kaikkia Internetin välityksellä tarjottavia informaatio-, asiointi- ja myyntipalveluja.

Yritysasiakkaan verkkopalvelu:
Tapiola-ryhmän tarjoama vahvan tunnistautumisen vaativa verkkopalvelu yritysvakuutusasiakkaalle.

Älykortti tai sirukortti:
Älykortti on muovinen kortti, johon on upotettu pieni tietokone käyttöjärjestelmineen ja sovelluksineen. Suurin osa sirukorteista on ISO-7816 -standardin mukaisia luottokortin kokoisia muovikortteja, joiden toisessa päässä keskellä on 9 kullanväristä kontaktipintaa. Yleisin ISO-7816 -kortti nykyisin on tavallinen kännykästä löytyvä SIM-kortti.

3 VERKKOPALVELUJEN LUOKITTELUA

Henkilö- ja yritysasiakkaille tarjotaan Internetissä erilaisia verkkopalveluja. Yritysten Internet-sivut on useimmiten informatiivisia. Ne esittelevät yrityksen tarjoamia tuotteita ja palveluita sekä esimerkiksi yrityksen yhteystiedot. Internet-sivuilta löytyy myös erilaisia lomakkeita ja sovelluksia, kuten osoitteenmuutos-, palaute-, tilauslomakkeita ja vahinkoilmoituksia, joiden käyttö ei vaadi erillistä tunnistautumista, vaan lomakkeet ovat kaikkien sivuilla kävijöiden käytössä. Lomakkeet ovat yleensä SSL-suojattuja, koska niiden välityksellä lähetetään muun muassa henkilötietoja. Yritykset tarjoavat asiakkailleen myös tunnistuksen vaativia palveluja eli ns. ekstranet-palveluja, kuten esimerkiksi pankkien verkkopankit. Yritysten Intranet-palvelut puolestaan on suunnattu

vain oman organisaation omille työntekijöille ja siten ne on tarkoitettu vain yrityksen sisäiseen käyttöön.

Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI on luokitellut verkkopalvelut sisältönsä ja luonteensa mukaan seitsemään tyyppiin, joiden tarkoituksena on auttaa palveluntarjoajaa käytännön verkkopalvelujen tunnistamiselle asetettavan vaatimustason määrittämisessä (Valtiovarainministeriö VAHTI 2006).

Verkkopalveluiden päätyypit ovat seuraavat:

A. Tietopalvelut ja tiedottaminen, jossa asiakkaalle tarjotaan tietoa hallinnosta ja hallinnon palveluista

B. Asiakaspalaute ja kansalaisten osallistuminen, jossa kansalaiset voivat antaa palautetta esimerkiksi viranomaiselle palveluista tai osallistua keskusteluun, jolla pyritään kehittämään yhteiskunnan toimintaa

C. Ei-luottamuksellinen vuorovaikutteinen asiointi, joka koskee muuta kuin asiakkaan luottamuksellisia henkilökohtaisia tietoja

D. Vireillepano, jossa asiakkaalle tarjotaan mahdollisuus täyttää hakemuslomake sähköisesti ja lähettää se sähköisesti palveluntarjoajalle

E. Luottamuksellinen vuorovaikutteinen asiointi, jossa käsitellään asiakkaan luottamuksellisia henkilökohtaisia tietoja

F. Tietojärjestelmien välinen tietojenvaihto, jossa tietojärjestelmäsovellukset keskustelevat automaattisesti keskenään. Esimerkiksi tietojen haku toisen viranomaisen rekisteristä, verkkomaksutapahtumat, viran omaisten keskinäiset tai asiakkaiden ja viranomaisten väliset tietojen siirrot

G. Viranomaispalvelut, jolla tarkoitetaan kaikenlaisia yksinomaan viranomaisten sisäiseen käyttöön tarkoitettuja verkkopalveluja sekä eri viranomaisten välisen virkamieskäytön, kuten virkamies virastosta A käyttää viraston B palvelua.

Julkishallinnon tekemää palveluiden jaottelua voidaan soveltaa myös yksityissektorille, koska palveluiden sisältö ja luonne ovat hyvin samanlaiset. Verkkopalveluiden kehitystyössä edellä esitetty päätyypitys auttaa valitsemaan oikean tasoisen tunnistusratkaisun. Henkilön vahva sähköinen tunnistaminen ei ole itsetarkoitus, vaan sitä käytetään vain silloin, kun se on tarpeen verkkopalvelun sisällön vuoksi.

4 TUNNISTAMINEN JA SEN LUOTETTAVUUS

Verkkopalvelujen käytön edellytyksenä on, että käyttäjä tunnistetaan. Verkkopalvelujen turvallisuus ja luotettavuus on puhuttanut niin kauan kuin verkkopalveluja on ollut olemassa. Verkkopalveluiden turvallisuus ja luotettavuus on noussut jälleen lehdistön puheenaiheeksi kevään 2008 aikana, kun erään pankkikonsernin verkkopalvelussa oli paljon tietoturvaongelmia pankkiohjelman vaihdon yhteydessä (Taloussanomat 2008). Toisaalta Ahvenanmaalaisen peliyhtiön järjestelmästä paljastui alkeellinen virhe, jonka seurauksena asiakkaan onnistui kerätä pelitililleen miljoona euroa. Tapaus paljastui, kun asiakas yritti nostaa rahoja liian suurissa erissä. Kelan verkkopalvelussa taas asiakas näki väärän henkilön sairastiedot. (Järvinen 2008.) Verkkopalveluiden luotettavuus voidaan menettää nopeasti ja siksi onkin tärkeää panostaa luotettavuuteen riittävästi.

4.1 Tunnistaminen ja todentaminen

Tunnistaminen (Identification) on menettely, jossa tunnistetaan tietojärjestelmän käyttäjä. Käyttäjä voi olla paitsi henkilö, myös organisaatio tai toinen laite. Tunnistamisen tarkoitus on erottaa käyttäjät toisistaan käyttäen jotain tunnistetta (identifier). Tunniste voi olla esimerkiksi tietojärjestelmistä tuttu käyttäjätunnus. (Linden 2003.)

Todentaminen (authentication) tarkoittaa järjestelmän käyttäjän tunnistuksen varmistamista. Todentamista kutsutaan vahvaksi (strong authentication), kun se hyödyntää kryptografista laskentaa, kuten esimerkiksi julkisen avaimen menetelmää. Vahva todentaminen on esimerkiksi salasanaan perustavaa henkilön todentamista luotettavampaa, koska todentamistietoihin ei ulkopuoliset voi päästä käsiksi. Todentamista hyödynnetään sähköisessä asioinnissa valtuuden tarkistamisen

yhteydessä, kuten tietojärjestelmiin kirjautumisessa tai muussa sähköisen asioinnin osapuolten aitouden todentamisessa. (Linden 2003.)

Todentamista sanotaan kevyeksi tunnistamiseksi, jos se nojautuu vain yhteen todentamistapaan. Tällaisia todentamistapoja ovat:

- käyttäjätunnus ja salasana
- pelkkä varmenteellisen sirukortin esittäminen tai pelkkä puhelinsoitto matkapuhelimesta tai matkapuhelimeen tai
- pelkkä biotunnistaminen.

Vahva todentaminen perustuu kahden tekijän sääntöön. Vahva todentaminen edellyttää, että vähintään kaksi ehdoista täyttyy samanaikaisesti tunnistamistapahtumassa. Tällaisia tunnisteita ja tunnistamismenetelmiä ovat:

- verkkopankkitunnuksiin ja vaihtuviin salasanalistoihin perustuva Tupas-tunnistus
- käyttäjätunnus, salasana ja puhelinsoitto matkapuhelimesta tai matkapuhelimeen
- varmenteellinen sirukortti ja salasana (PIN-koodi)
- varmenteellinen sirukortti ja biotunnistus
- laatuvarmenteellinen sirukortti ja salasana (PIN-koodi) tai
- laatuvarmenteellinen sirukortti ja biotunnistus.

Tardon ja Alagappan mukaan (1991, 232 – 244) vahvaa todentamista ovat tekniikat, joiden avulla henkilö voi todistaa tietävänsä tietyn salaisuuden, paljastamatta sitä. Määritelmän mukaisia tunnistustapoja on käytännössä vain julkisen avaimen menetelmään pohjautuvat tunnistamis- ja todentamisratkaisut.

4.2 Luotettavuus VAHTI:n mukaan

Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI:n mukaan verkkopalveluissa saavutettavissa olevaa käyttäjien tunnistamisen luotettavuutta voidaan tarkastella kahdesta näkökulmasta:

1. käytetyn käyttäjäidentiteetin luotettavuus
2. käytetyn käyttäjäidentiteetin todentamisen luotettavuus.

Käyttäjäidentiteetillä tarkoitetaan palveluntarjoajan tiedossa olevia käyttäjän henkilöllisyyttä yksilöiviä ja kuvaavia tietoja. Käyttäjäidentiteetti luodaan palvelujärjestelmään silloin, kun käyttäjä rekisteröidään järjestelmän käyttäjäksi. Lähtökohtana luotettavuutta mitattaessa voidaan pitää sitä, että näiden kahden luotettavuustekijöiden näkökulman tulee olla suunnilleen samantasoisia. Käytännössä näin ei kuitenkaan aina ole. Esimerkiksi lääketieteellistä testauspalvelua voidaan käyttää nimimerkillä (ts. alhaisen luotettavuustason käyttäjäidentiteetillä), mutta jonka tulosten tulee pysyä luottamuksellisina, eli käyttäjältä tulee vaatia vahvaa sähköistä tunnistamista. Vastaavasti voi olla järkevää mahdollistaa ei-luottamuksellisten palvelujen käyttö myös korkean luotettavuustason käyttäjäidentiteetillä kuten kansalaisvarmenteella, jos käyttäjällä sellainen jo on, vaikka palvelun käyttö ei käyttäjiltään sellaista muuten edellytäkään. (Valtiovarainministeriö VAHTI 2006.)

4.2.1 Käyttäjäidentiteetin luotettavuus

Käyttäjäidentiteetin luotettavuus riippuu rekisteröintiprosessista. Jos käyttäjä antaa rekisteröinnin yhteydessä itse tietonsa, joita ei mitenkään tarkisteta, käyttäjäidentiteetin luotettavuus on alhainen. Vastaavasti jos käyttäjän henkilöllisyys selvitetään luotettavasti esimerkiksi kasvotusten, rekisteröinnin tuloksena syntyy käyttäjäidentiteetti, jonka luotettavuus on maksimaalinen. (Valtiovarainministeriö VAHTI 2006.)

Joissain tapauksissa henkilön identiteetti ei ole tärkeää, vaan se kuuluuko henkilö johonkin ryhmään (esim. kuntalaisuus) ja onko hän näin oikeutettu esimerkiksi jonkin palvelun käyttöön. Käyttäjän ilmoittamat tiedot, kuten nimi ja osoite, riittävät monissa palveluissa sellaisenaan tunnistukseksi. Tarvittaessa voidaan tietojen luotettavuus varmistaa vertailemalla ilmoitettuja tietoja palvelun tarjoajan omissa tietojärjestelmissä oleviin tietoihin. (Valtiovarainministeriö VAHTI 2006.) Aina todentamista ei tarvita, vaan joskus esimerkiksi riittää että palvelun käyttäjä suorittaa palvelusta aiheutuvan maksun ilman, että maksajan henkilöllisyys olisi tiedossa.

Käyttäjä identiteetin luotettavuuden kuvaamiseen voidaan käyttää seuraavaa nelitasoista luokittelua.

Taso 0: Anonyymikäyttäjät

Käyttäjiä ei rekisteröidä, eivätkä he ole palvelujen eri käyttökerroilla erotettavissa toisistaan.

Taso 1: Yksilöitävissä olevat käyttäjät

Käyttäjillä on rekisteröity käyttäjäidentiteetti, jonka perusteella he ovat yksilöitävissä. Käyttäjäidentiteetti ei kuitenkaan välttämättä paljasta käyttäjän todellista henkilöllisyyttä, asuinpaikkaa tai muuta sellaista, koska rekisteröinnin yhteydessä annettujen käyttäjätietojen paikkansapitävyyttä ei ole tarkistettu. Käyttäjä voi olla yksilöitävissä myös teknisesti ilman rekisteröintiä, palvelun käyttäjän työasemalle tallettaman evästeen perusteella. Yksilöinti kohdistuu tällöin tarkkaan ottaen käyttäjän päätelaitteeseen eikä itse käyttäjään. Henkilötietolain mukaan kuitenkin nämäkin yksilöintitiedot voitaisiin katsoa henkilötiedoiksi. Yhteiskäyttöiseltä koneelta luettava eväste aiheuttaa identiteettien sekaantumisen eli evästeeseen luottava sovellus ymmärtää kaksi peräkkäistä konetta käyttävää samaksi henkilöksi. (Valtiovarainministeriö VAHTI 2006.)

Taso 2: Kevyesti todennetut käyttäjät

Käyttäjillä on käyttäjäidentiteetti, jonka rekisteröintiprosessin yhteydessä on varmistauduttu siitä, että ainakin jotkut annetuista käyttäjätiedoista, kuten puhelinnumero, osoite, luotto-kortin numero tms. pitävät paikkansa, jolloin käyttäjä identiteettiä voidaan pitää moniin tarkoituksiin riittävän luotettavana (Valtiovarainministeriö VAHTI 2006).

Taso 3: Vahvasti todennetut käyttäjät

Käyttäjien henkilöllisyys on selvitetty luotettavasti, esimerkiksi henkilökohtaisella tapaamisella rekisteröintitilanteessa. Henkilön identiteetin varmistaa valtuutetun organisaation edustaja. Henkilön on todistettava henkilöllisyytensä virallisella henkilökortilla, ajokortilla tai passilla. (Valtiovarainministeriö VAHTI 2006.)

4.2.2 Käyttäjäidentiteetin todentamisen luotettavuus

Todentamisen luotettavuus riippuu tunnistamisessa käytettävästä todentamismenetelmästä. Käyttäjäidentiteetin todentaminen perustuu johonkin seuraavista kolmesta vaihtoehdosta:

A) johonkin mitä käyttäjä tietää
B) johonkin mitä käyttäjällä on hallussaan tai
C) johonkin mitä käyttäjä on.

A-vaihtoehto on sähköisessä asioinnissa perinteisesti eniten käytetty todentamistapa ja tarkoittaa salasanaa tai salalausetta, jonka käyttäjä antaa tunnistetietonsa eli käyttäjätunnuksensa yhteydessä. Käyttäjän tulee olla aiemmin sitoutunut olemaan luovuttamatta tietoa kenellekään muulle. Kyse on salaisuudesta, jonka käyttäjä ja järjestelmä jakavat keskenään. Käyttäjätunnuksen tai nimen perusteella käyttäjä tunnistetaan (identification) ja salasanan avulla käyttäjä todennetaan oikeaksi (authentication). Salasanojen heikkous on siinä, että niitä voi monistaa ja jakaa eteenpäin. Salasana voi myös paljastua vahingossa tai sen voi unohtaa. Järjestelmät pyytävät käyttäjiä vaihtamaan salasanoja säännöllisin väliajoin. (Järvinen 2003.)

B-vaihtoehto tarkoittaa, että henkilön todentaminen perustuu esimerkiksi avaimeen tai henkilökorttiin. Tämä on hyvin yleinen menetelmä. Menetelmä ei kuitenkaan yksinään takaa mitään, koska pääsyn avaavaa esinettä ei ole tarpeeksi sidottu henkilöön. Avaimesta voi tehdä helposti kopion tai henkilökortin voi luovuttaa toiselle henkilölle. Todennuksen parantamiseksi esineen pitäisi olla sellainen, ettei sitä voi helposti väärentää eikä monistaa. Lisäksi se pitää saada sidottua jotenkin käyttäjään. (Järvinen 2003.)

C-vaihtoehto tarkoittaa käytännössä jotain käyttäjän biometristä ominaisuutta, kuten esimerkiksi sormenjälkeä, kasvojen muotoa, silmän iiristä tms. Biometrisillä tekniikoilla on mahdollista koodata ihmisten ominaisuuksia tietokoneen ymmärtämään muotoon. Ääni tai kasvonpiirteet voidaan digitoida ja verrata mitattuihin arvoihin. Tietokoneiden etuna on mahdollisuus hyödyntää käyttäjälle paljaalle silmälle näkymättömiä ominaisuuksia, kuten sormenjälkiä tai verkkokalvoa. Biometrinen tunnistaminen ei yksinään takaa vahvaa tunnistamista. Tekniikat ovat kehitysvaiheessa, tunnisteet ja

niihin liittyvät haavoittuvuudet muuttuvat tekniikan kehittyessä. (Valtiovarainministeriö VAHTI 2006.)

5 PKI JULKISEN AVAIMEN INFRASTRUKTUURI

Julkisen avaimen infrastruktuuri (PKI, Public Key Infrastructure) on eräänlainen toimintamalli julkisten avainten ja varmenteiden hallintaan. PKI:ssä hyödynnetään avainpareihin perustuvia epäsymmetrisiä salausmenetelmiä siten, että voidaan toteuttaa turvallisen sähköisen asioinnin perusteet: digitaalinen allekirjoitus allekirjoittajan yksityisellä avaimella ja viestin salaus vastaanottajan julkisella avaimella (Levi, Caglayan & Koc 2004). Olennainen osa PKI-toimintamallissa on luottamus. Jotta ennestään tuntemattomat osapuolet voivat viestiä keskenään luottamuksellisesti, tarvitaan kolmas osapuoli varmistamaan näiden osapuolten henkilöllisyys. PKI-toimintamallissa luottamus perustuu kolmantena osapuolena toimivaan varmentajaan, johon molemman viestinnän osapuolet luottavat. Varmentaja yhdistää myöntämässään varmenteessa julkisen avaimen ja sen haltijan toisiinsa. Näin luottamuksellinen viestintä ja digitaaliset allekirjoitukset onnistuvat, vaikka osapuolet eivät tuntisi toisiaan entuudestaan (Wilson 2008).

PKI-järjestelmä (Public Key Infrastructure) koostuu varmenteiden myöntämisestä, jakelusta, hallinnoinnista ja ylläpidosta. Tukijärjestelmä tekee varmenteiden käytöstä kattavaa, helppoa ja turvallista. PKI-järjestelmän ytimenä toimii varmenteiden myöntäjä Certification Authority, CA (Rawles&Baker 2003).

PKI arkkitehtuuri koostuu neljästä seuraavasta ydinpalvelusta:

1. Vahva tunnistaminen: Todennetaan varmasti asioiva osapuoli esimerkiksi henkilö, laite tai ohjelmisto. Voidaan olla varmoja, että tunnistettu osapuoli on se, jona esittäytyy
2. Tiedon eheys: Osoitetaan, että osapuolten välisessä viestissä mitään ei ole muutettu
3. Luottamuksellisuus: Taataan, että kukaan muu kuin vastaanottaja ei voi saada selville viestin sisältöä.
4. Kiistämättömyys ja digitaalinen allekirjoitus: Varmennetaan, että lähetetty viesti on lähettäjän lähettämä ja muuttumaton.

Järvisen (2003) mukaan jokaisen PKI – järjestelmän on tarjottava ainakin seuraavat peruspalvelut:

1. Rekisteröinti: Varmennetta hakevan henkilöllisyyden tarkastaminen.

2. Varmenteen luonti: Tietojen kirjoittaminen varmenteeksi ja tietojen allekirjoitus; mahdollisesti myös julkisen tai yksityisen avaimen luonti ellei niitä ole luotu edellisessä kohdassa.

3. Varmenteen jakelu: Luodun varmenteen ja siihen mahdollisesti liittyvän yksityisen avaimen turvallinen jakelu varmenteen haltijalle.

4. Varmennehakemiston ylläpito: Ajan tasalla olevan hakemiston ylläpito kaikista myönnetyistä varmenteista. PKI -järjestelmän käyttäjät voivat etsiä hakemistosta muiden varmenteita ja noutaa niitä omaan käyttöönsä. Varmennekyselyiden tekoon käytetään usein LDAP-protokollaa (Lightweight Directory Access Protocol).

5. Sulkulistapalvelut: Sulkulistalle (Certificate Revocation List, CRL) lisätään niiden varmenteiden sarjanumerot, jotka on jouduttu mitätöimään ennen normaalia vanhenemista. Reaaliaikaisia sulkulistakyselyitä varten on kehitetty OCSP-protokolla (Online Certificate Status Protocol). Jokaisella PKI -järjestelmällä on URL-osoite, josta uusimman sulkulistan saa ladattua.

6. Tukipalvelut: Ylläpito- ja tukipalveluihin kuuluvat mm. myönnettyjen varmenteiden tieto-kantaa on yllä pidettävä ja tiedot turvattava varmuuskopioilla.

7. Toimintakuvaus: PKI-järjestelmän yläpidon on laadittava toiminnastaan kuvaus eli varmennekäytöntölausuma tai varmennepolitiikka (Certification Practise Statement, CPS). Kuvauksessa kuvataan varmenteiden tekninen sisältö sekä niiden myöntämiseen, jakeluun, hallinnointiin, mitätöintiin ja muuhun vastaavaan toimintaan liittyvät ohjeet. Toimintakuvauksen perusteella voidaan arvioida toiminnan luotettavuutta. (Järvinen 2003.)

6 KESKEISIMMÄT VAHVAT TUNNISTAMISVAIHTOEHDOT

Seuraavaksi esitellään keskeisimmät vahvat tunnistamismenetelmät, jotka ovat käytössä Suomessa.

6.1 KANSALAISVARMENNE

Suomessa otettiin käyttöön ensimmäisenä koko maailmassa kansallinen sähköinen henkilökortti (HST-kortti). Väestörekisterikeskus on vuodesta 1999 tarjonnut luonnollisille henkilöille, jotka ovat suomalaisia tai asuvat pysyvästi Suomessa, mahdollisuutta hankkia sähköinen henkilökortti eli kansalaisvarmenne. Kansalaisvarmenteen lisäksi sähköinen henkilökortti toimii tavallisena henkilöllisyystodistuksena, Kela-korttina ja matkustusasiakirjana EU-maissa. (Väestörekisterikeskus Opas palveluntarjoajille 2005.)

Kansalaisvarmenne on standardimuodossa kerrottu henkilötieto, sähköinen henkilöllisyys, joka perustuu julkisen avaimen menetelmään. Se sisältää mm. etu- ja sukunimen sekä sähköisen asiointitunnuksen. Kansalaisvarmenteen varmennetiedoissa eri varmenteen haltijat erotetaan luotettavasti toisistaan yksilöllisen sähköisen asiointitunnuksen eli SATU:n avulla. SATU on juokseva sarjanumero, jonka ainoa tarkoitus on eri varmenteiden ja niiden haltijoiden erottaminen toisistaan. Käyttötarkoituksen perusteella SATU vastaa siis perinteisen tunnistamisen henkilötunnusta. SATU ei kuitenkaan kerro haltijastaan mitään tietoja, toisin kuin henkilötunnus. SATU:n avulla sähköisen tunnistautumispalvelun tarjoaja voi käyttää varmenteeseen liitettyjä henkilötietoja väestörekisterikeskuksen kautta. Väestörekisterikeskuksen varmenneratkaisut perustuvat edellä luvussa 5 esitettyihin PKI-pohjaisiin toteutuksiin.

Kansalaisvarmenne on yleiskäyttöinen ja teknisestä alustasta riippumaton. Kansalaisvarmenne voidaan tallentaa erilaisille korttialustoille tai muuhun tekniseen välineeseen, kuten sähköiselle henkilökortille (älykortille), pankkikortille tai matkapuhelimen SIM-kortille. Kaikki eri alustoilla olevat kansalaisvarmenteet täyttävät sähköisiä allekirjoituksia koskevan EU-direktiivin (1999/93/EY) sekä sähköisistä allekirjoituksista annetun lain (14/2003) vaatimukset ja ovat näin ollen myös laatuvarmenteita. Kansalaisvarmenteiden tuottaminen on Väestörekisterikeskuksen lakisääteinen tehtävä. Kansalaisvarmenne on voimassa viisi vuotta. Digitoday lehden

mukaan kansalaisvarmenteita oli myönnetty noin 180 000 kappaletta keväällä 2008, kun tavoite on ollut 1,7 miljoonaa (Lehtinen 2008). Kansalaisvarmenteen käyttöä on rajoittanut mm. lukijalaitteiden vähyys (Arjen tietoyhteiskunta Sähköisen tunnistamisen nykytila Suomessa 2008).

Älykortin haltija on kortin turvallisuuden kannalta keskeisessä asemassa. Kun kortti on turvallisesti luovutettu sen oikealle omistajalle, vastuu kortin käytöstä siirtyy kortinhaltijalle. Sähköiseen tunnistamiseen tarkoitetulla kortilla voi kuitenkin helposti aiheuttaa vakavaa vahinkoa kortin omistajalle, jos joku muu saa kortin haltuunsa. Väärä kortinkäyttäjä voi mahdollisesti allekirjoittaa digitaalisesti laillisesti sitovia sopimuksia, allekirjoituksen kiistäminen voi olla jälkeenpäin melko työlästä. Tunnistuskortin väärinkäyttö esimerkiksi verkkoon kirjautumisessa voi myös aiheuttaa erittäin vakavia vahinkoja. Mikäli ulkopuolinen tunkeutuja pääsee väärän henkilöllisyyden turvin yrityksen verkkoon, hän voi pahimmassa tapauksessa tuhota kriittisiä tietoja tai käyttää luottamuksellisia tietoja hyväkseen kortin omistajan vahingoksi. Kortin PIN-luvun salassa pitäminen onkin kortin käytön turvallisuuden kulmakiviä. PIN-lukua ei saa kirjoittaa paperille tai ainakaan PIN-lukua ei saa säilyttää kortin yhteydessä. (Rinne 2002, 67.)

6.1.1 Kansalaisvarmenteen nykytila ja tulevaisuus

Suomi oli aikaansa edellä vuonna 1999, kun markkinoille tuotiin kansalaisvarmenne. Älykorttien käyttö sähköisessä tunnistamisessa ja digitaalisten allekirjoitusten välineenä ei ole kuitenkaan yleistynyt toivotulla tavalla. Tämän sovellusalueen hankkeet ovat olleet yleensä julkisen hallinnon vetämiä. Niitä ovat hidastaneet paitsi digitaalisia allekirjoituksia säätelevien lakien viiveet myös yritysmaailman sitoutumattomuus hallitusvetoisten hankkeiden kehittämiseen. Esimerkiksi Suomessa HST-hanke (Henkilön Sähköinen Tunnistaminen) on kärsinyt älykorttien käyttöön perustuvien palvelujen niukkuudesta. Vain muutama yritys on rakentanut Internet-palveluja, joissa tunnistus- tai allekirjoitusvälineenä voi käyttää sähköistä henkilökorttia eli HST-korttia. (Rinne 2002, 16.) Ratkaiseva sysäys sähköisien henkilökorttien ja samalla kansaisvarmenteiden yleistymiselle saattaa olla jo näköpiirissä. Jos sähköisestä henkilökortista tulee passiin verrattava matkustusasiakirja, saattaa moni valita henkilökortin kätevämmän kokonsa takia. (Nikulainen 2008.)

Sähköisen henkilökortin hienous on sen konkreettisuudessa. Käyttäjän sähköinen identiteetti on kirjaimellisesti omissa käsissä ja siksi helposti säädeltävissä. Toisin kuin salasanoja, identiteettiä ei voi varastaa haittaohjelmilla. Lisäksi käyttäjä saa itse valita, milloin haluaa tulla todennetuksi. Sähköinen henkilökortti toimii kuin perinteinen avain. Siksi sen käyttö on maallikollekin riittävän yksinkertaista. Petteri Järvinen ehdottaa, että kortti sekä usb- porttiin liitettävä lukija jaetaan kaikille ilmaiseksi. Kustannukset olisivat noin 30 euroa henkilöltä. Toisena ehdotuksena Järvinen esittää, että sähköisen henkilökortin siru upotetaan usb-muistitikkuun, jolloin erillistä kortin lukijaa, ei tarvita ja tikkua voidaan käyttää missä tahansa tietokoneessa, jossa on usb-portti. Kansallinen usb-muistitikku olisi rohkea ratkaisu mutta toisaalta sellaista Suomi tarvitsee, jos se haluaa olla kehityksen kärjessä. Verkkotoiminta perustuu luottamukseen. Juuri sitä kilpailuetua Suomen kannattaa hyödyntää. (Järvinen 2008, 21.)

6.1.2 Sähköinen varmenne Virossa

Viroa pidetään Euroopan edistyksellisimpänä maana sähköisten varmenteiden käytössä. Henkilökortin sähköinen varmenne on pakollinen maan yli 15-vuotiaille kansalaisille sekä yli vuoden mittaisella luvalla maassa oleskeleville ulkomaalaisille.

Viron asukasluku on noin 1,4 miljoonaa ja kortteja on jaettu lähes miljoonalle henkilölle. Varmentajana toimii yritys AS Sertifiseerimiskeskus, jolla on sopimus asiasta valtion kanssa. Kortin jakelu hoidetaan sen omistavien pankkien konttoreissa.

Kortilla olevissa varmenteissa, allekirjoitus- ja tunnistamisvarmenteissa, on henkilön nimi sekä kansallinen, yksikäsitteinen tunnistekoodi. Lisäksi tunnistamisvarmenne sisältää henkilön yksikäsitteisen sähköpostiosoitteen, joka on valtion antama elinikäinen osoite ja toimii vain linkkinä todellisiin sähköposteihin, jotka haltijan on erillisessä tietokannassa ylläpidettävä. Tunnistekoodi on julkinen. Ainostaan allekirjoitusvarmenne on laatuvarmenne. Varmenteilla ei ole käyttörajoitteita.

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

Huolimatta kortin laajasta käyttäjäkunnasta sen käyttö tietoverkkopalveluissa on kuitenkin vähäistä. Noin 2,5 % kortin omistavista henkilöistä käyttää sitä sähköisten

palveluiden yhteydessä. Varmenne on yhteensopiva Suomen kansalaisvarmenteen kanssa.

6.2 TUPAS-PALVELU

Pankkien Tupas-varmennepalvelun (jatkossa Tupas-palvelu) avulla sähköisiä asiointi-palveluita tarjoava yritys tai yhteisö voi tunnistaa asiakkaansa Tupas-varmenteita hyväksikäyttäen. Tupas-palvelussa pankki tunnistaa asiakkaan vahvalla tunnistuksella omien rekisteriensä perusteella. Tupas-palvelua käytetään ensisijaisesti sähköiseen tunnistamiseen ja sähköiseen allekirjoittamiseen palveluntarjoajan asiointipalvelussa. (Finanssialan keskusliitto 2008.)

Tupas-palvelu otettiin käyttöön 2002. Palvelua on kehitetty asiakaspalautteiden perusteella ja se on nykyään monipuolisempi kuin käyttöönottohetkellä. Tupas-palvelu määritettiin aluksi vain henkilöiden tunnistamista varten. Henkilöistä välitettiin nimi- ja henkilötunnustiedot. Yrityksistä välitettiin ainoastaan yrityksen nimi ja y-tunnus. Palveluun on kehitetty uusia piirteitä 2007. Uudet ominaisuudet otetaan käyttöön pankkikohtaisesti kehitysaikataulujen mukaisesti. Uusia ominaisuuksia on, että palveluntarjoaja voi jatkossa mm. määritellä tunnistuksen koskemaan henkilö- ja/tai y-tunnuksia. Yritystä tunnistettaessa on yrityksen nimen ja y-tunnuksen lisäksi mahdollisuus tunnistaa myös tunnistusta tekevä henkilö.

Tupas-palvelu on pankkien yhteisesti määrittelemä. Kukin pankki tunnistaa henkilön samoilla pankkikohtaisilla tunnisteilla, joita henkilö käyttää pankin omissa verkkopalveluissa esimerkiksi verkkopankissa. Tupas-palvelu täyttää vahvan tunnistuksen määritelmän, ja soveltuu käytettäväksi verkkopalveluihin, joissa on tarve tunnistaa käyttäjät luotettavasti. Vahvan tunnistamisen lisäksi tapahtuman täytyy perustua riittävän turvalliseen menettelyyn. Pankkien käyttämät vaihtuvat tunnusluvut täyttävät turvallisen tunnistustapahtuman kriteerit. (Finanssialan keskusliitto FK. 2008.)

Tupas-palvelussa pankki huolehtii ainoastaan käyttäjän tunnistamisesta palvelukuvauksessa mainitulla tavalla eikä vastaa asiakkaan ja palveluntuottajan välisen oikeustoimen sitovuudesta tai sisällöstä. Palveluntarjoaja ja käyttäjä voivat sopia Tupas-varmenteen käytöstä osana sähköistä allekirjoitusta käyttäjän ja palveluntarjoajan välisessä oikeustoimessa, mikä mahdollistaa erilaisten hakemusten vastaanottamisen sekä sopimusten tekemisen verkossa. Palveluntarjoajan on

huolehdittava muista sähköisen allekirjoituksen edellyttämistä seikoista, kuten tietojen kokonaisuuden hallinnasta, eheydestä, kiistämättömyydestä ja vastaussanoman tallentamisesta. Tupas-varmenteen käyttämistä sähköisenä allekirjoituksena tukevat vastaussanomien aikaleimat ja pankkien lokitiedot. (Finanssialan keskusliitto 2008.)

Palveluntarjoajan on tehtävä erillinen sopimus kaikkien niiden pankkien kanssa, joiden tuottamaa Tupas-palvelua palveluntarjoaja tahtoo käyttää. Palveluntarjoajan tiedot rekisteröidään kussakin pankissa ja palveluntarjoaja ilmoittaa kullekin pankille erikseen, kun hänen sopimustietoihinsa tulee muutoksia. (Finanssialan keskusliitto 2008.)

Pankki toimittaa sopimuksen teon jälkeen palveluntarjoajalle Tupas-palvelussa käytettävän pankkikohtaisen asiakastunnuksen ja tarkisteavaimen. Tiedot toimitetaan pankkikohtaisella menettelyllä joko sähköisessä muodossa tai paperitulosteena. Testausvaiheessa käytettävät pankkikohtaiset tiedot ovat saatavilla pankkien palvelukuvauksissa. Palveluntarjoaja voi testata Tupas-palvelua tuotanto-ympäristössä jo ennen kuin sopimus on tehty käyttämällä pankkikohtaisia testitunnuksia. (Finanssialan keskusliitto 2008.)

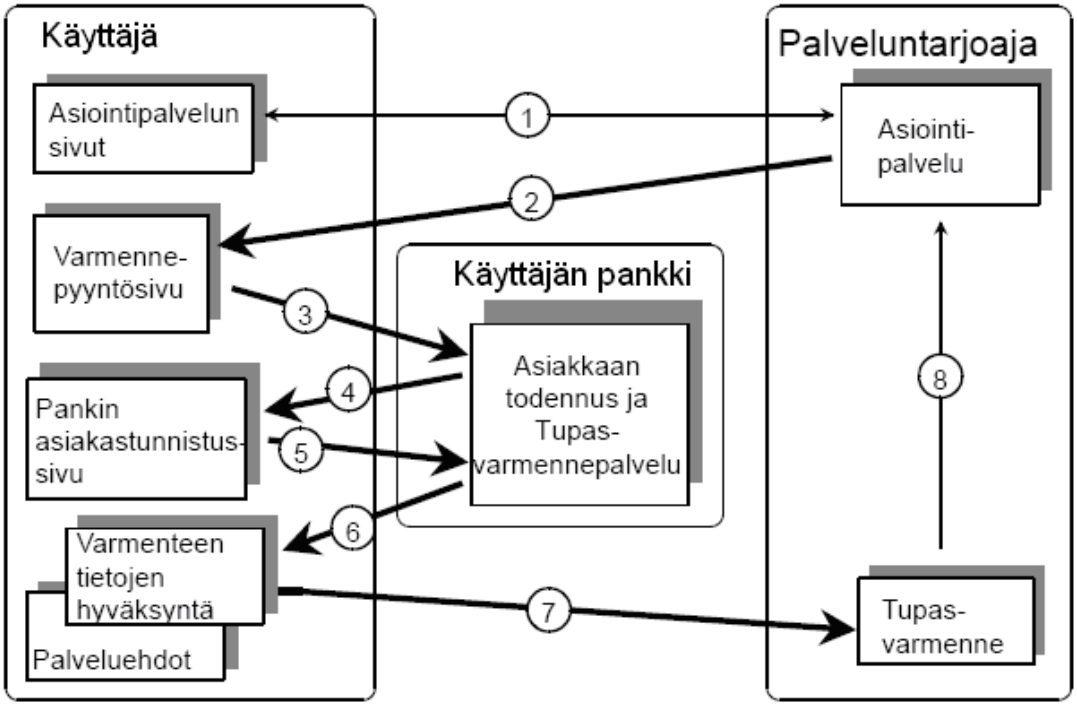
Tupas-palvelu on Finanssialan keskusliiton tavaramerkki, joka perustuu yhteiseen määritykseen. Pankit tarjoavat omaa yhteisen standardin mukaista Tupas-palveluaan. Palveluntarjoajan ja pankin välisten Tupas-tunnistussanomien tietosisältö on tunnistusvälineestä riippumaton. Pankin varmenteessa on aina käyttäjän (henkilön ja /tai yrityksen) nimi. Tämän lisäksi välitettävä käyttäjän yksilöintitieto voi olla joko selväkielinen tai salattu.

Yksilöintitiedon ollessa selväkielinen, pankki voi välittää käyttäjän henkilötunnuksen, henkilötunnuksen tarkisteosan, Y-tunnuksen tai muun sähköisen asiointitunnuksen sen mukaan, mistä on sovittu palvelusopimuksessa. Selväkielisen henkilötunnuksen pankki välittää vain palveluntarjoajille, joilla on oikeus rekisteröidä se.

Kun yksilöintitieto on salattu, pankki välittää palveluntarjoajalle tiedon, joka perustuu käyttäjän henkilötunnukseen, Y-tunnukseen tai muuhun sähköiseen asiointitunnukseen. Itse tunnus ei kuitenkaan välity vastaussanoman mukana. Siksi palveluntarjoajalla tulee olla käytössään käyttäjän henkilötunnus, Y-tunnus tai muu sähköinen asiointitunnus, jotta palveluntarjoaja voi varmistua pankin antaman vastaussanoman tietojen avulla käyttäjän henkilöllisyyden oikeasta todennuksesta. Jos

palveluntarjoajalla ei ole käyttäjän tunnusta, hänen tulee kysyä se ennen varmennepyynnön lähettämistä. Tämä toiminnallisuus soveltuu siten asiakkaan ilmoittamien tietojen oikeellisuuden tarkastamiseen pankista. (Finanssialan keskusliitto 2007.)

Seuraavassa kuviossa 3 on esitetty Tupas-palvelun tunnistamisprosessi.



KUVIO 3. Tupas-palvelun tunnistamisprosessi

Seuraavassa on selvitetty tunnistamisprosessin vaiheet:

Vaihe 1: Tunnistautuva käyttäjä on yhteydessä palveluntarjoajan palveluun. Käyttäjän ja palveluntarjoajan välisen tietoliikenteen tulee olla SSL-suojattu, kun käyttäjä siirtyy Varmennepalveluun liittyvien tietojen syöttöön. Vaiheiden 2–7 aikana tiedonsiirtoyhteys on aina SSL-suojattu.

Vaihe 2: Palveluntarjoaja lähettää käyttäjälle varmennepyynnön, joka sisältää tapahtumaan liittyvät yksilöintitiedot. Käyttäjä tarkastaa vastaanottamansa pyynnön tiedot, mutta hän ei voi muuttaa niitä. Käyttäjä voi halutessaan keskeyttää tunnistuksen ja palata takaisin asiointipalveluun. Käyttäjän selaimen varmennepyyntösivulla ovat varmennepalveluun johtavat toimintopainikkeet ja peruutuspainike.

Vaihe 3: Käyttäjä painaa toimintopainiketta, joka johtaa hänen pankkinsa varmennepalveluun. Pankkiin välittyvä varmennepyyntö sisältää varmennepalvelun tarvitsemat tiedot palveluntarjoajasta ja tapahtumasta. Pankki tarkastaa pyynnön eheyden ja tietojen oikeellisuuden.

Vaihe 4: Pankki lähettää käyttäjälle tunnistuspyynnön, jos palveluntarjoajan varmennepyyntö on virheetön. Pankki antaa käyttäjälle virheilmoituksen, jos pankki havaitsee varmennepyynnössä virheitä, jolloin käyttäjä palaa tapahtuman peruutuspainikkeella takaisin palveluntarjoajan palveluun.

Vaihe 5: Käyttäjä tunnistautuu pankkinsa varmennepalvelussa. Pankki palauttaa käyttäjälle virheilmoituksen, jos tunnistus epäonnistuu, jolloin käyttäjä palaa peruutuspainikkeella takaisin palveluntarjoajan palveluun.

Vaihe 6: Onnistuneen tunnistuksen jälkeen pankki muodostaa vastaussanoman, ”Varmenteen”. Pankin varmennepalvelu asettaa käyttäjälle hyväksymis- ja peruutuspainikkeet.

Vaihe 7: Käyttäjä tarkastaa varmenteen tiedot ja hyväksyy varmenteen välittämisen palveluntarjoajalle. Käyttäjä voi peruutuspainikkeella keskeyttää tunnistustapahtuman ja palata takaisin palveluntarjoajan palveluun.

Vaihe 8: Palveluntarjoaja varmistaa vastaanottamansa Varmenteen eheyden ja ainutkertaisuuden. Palveluntarjoaja liittää Varmenteen käyttäjän palvelutapahtumaan ja säilyttää sitä yhtä kauan kuin muita palvelutietoja säilytetään. Käyttäjän yksilöintitietoja ei saa rekisteröidä tai käyttää muuhun tarkoitukseen. (Finanssialan keskusliitto 2007.)

Finanssialan keskusliiton Tupas-palvelun käyttöönottoon liittyvässä palvelukuvauksessa on mm. pankkikohtaisten painikkeiden kuvien käytöstä, sulkupalvelusta ja palveluntarjoajan yhteystiedoista, joista kerrotaan seuraavaksi. Asiointipalvelussa käytettävien, pankkikohtaisten painikkeiden kuvatiedostot ovat noudettavissa ko. pankin www-sivuilta kunkin pankin erikseen ilmoittamasta osoitteesta. Painikkeiden kokoja tai värejä ei saa muuttaa. Tarkemmat ohjeet kuvien käytöstä ovat pankkikohtaisessa palveluntarjoajan ja pankin välisessä palvelusopimuksen ehdoissa. Painikkeen kuvaa ei saa käyttää muuhun tarkoitukseen kuin sopimuksessa on sovittu. (Finanssialan keskusliitto 2008). Pankit tarjoavat

pankkitunnusten käyttäjille ympärivuorokautista (24/7) pankkikohtaista sulkupalvelua, jonne käyttäjä voi ilmoittaa pankkitunnusten katoamisesta tai joutumisesta vääriin käsiin. Palveluntarjoajan on annettava verkkosivuillaan itsestään täsmällistä, selkeää ja helposti saatavilla olevaa tietoa, kuten esimerkiksi palveluntarjoajan yhteystiedot, yritys- ja yhteisötunnus, kenelle palvelu on suunnattu, palveluntarjoajaa valvova viranomainen. Käyttäjän on selvästi voitava havaita ja erottaa, milloin hän siirtyy Tupas-palvelun tuottajan sivulta muun palvelun tarjoajan sivulle. Tupas-palvelun palvelukuvaus palveluntarjoajalle löytyy Finanssialan keskusliiton Internet-sivuilta.

6.2.1 Tupas-palvelun hyödyt käyttäjälle

Tupas-palvelu on käyttäjälle turvallinen ja luotettava, koska Tupas-palvelun pankin varmenne on ainutkertainen ja se on sidottu aikaleimalla sekä palvelutarjoajan palvelutapahtumaan että käyttäjään. Tupas-palvelu soveltuu pääasiassa kuluttajille suunnattuihin palveluihin. Tupas-palvelu on yleiskäyttöinen sillä pankkitunnuksilla allekirjoitetaan myös merkittävä osa pankkien lainasopimuksista sekä puhelin-, sähkö- ja muita sopimuksia. Pankkien asiakkailla on verkkopalvelutunnuksia 3,9 miljoonaa kappaletta. Verkkopalvelutunnuksilla tehdään noin 99 %:a vahvan tunnistamisen vaativista tapahtumista. Lisäksi verkkopalvelutunnuksia käytetään kolmansien osapuolten verkkopalveluissa sähköisten allekirjoitusten tekoon verkkomaksamisen yhteydessä. (Arjen tietoyhteiskunta 2008.)

Tupas-palvelun käyttäjä ei ole sidoksissa yhteen tiettyyn laitteeseen, koska menetelmä ei tarvitse päätteeseen sijoitettua lukijaa tai erillisohjelmistoa. Tunnistusmenettely on pankkikohtainen. Pankkitunnukset ovat aina henkilökohtaiset riippumatta siitä, onko ne annettu henkilö-, yritys- tai yhteisöasiakkaan käyttöön. Kukin pankki tunnistaa käyttäjän samoilla pankkikohtaisilla pankkitunnisteilla, joita käytetään pankin omissa palveluissa. Käyttäjä saa henkilökohtaiset pankkitunnukset käyttöönsä kirjallisen, henkilökohtaisesti tehdyn sopimuksen perusteella. Käyttäjän henkilöllisyys varmistetaan konttorissa esimerkiksi ajokortista, henkilökortista, passista tai kuvallisesta kela-kortista. Käyttäjä voi kirjautua usean eri palvelutarjoajan verkkopalveluihin samoilla käyttäjätunnuksilla. Verkkopalveluja joihin voi kirjautua Tupas-palvelun avulla on esimerkiksi Kela, Veikkaus oy, Verohallinto tai VR.

6.2.2 Palvelun turvallisuus

Tupas-palvelun osapuolten välisessä tietoliikenteessä käytetään SSL siirtokäytäntöä, joten ulkopuoliset eivät näe tietoja eivätkä voi muuttaa niitä. Palveluntarjoajan palvelinohjelmiston on tuettava 128 bitin avaimilla toteutettua SSL-salausta. Yhteydellä käytettävä avainpituus määräytyy kuitenkin asiakkaan käyttämän selaimen ominaisuuksien perusteella. Varmennepyynnön ja varmenteen tiedot on suojattu tiedon eheyden turvaavalla tarkisteella, joten varmenteen välitystä ohjaavalla asiakkaalla ei ole mahdollisuutta muuttaa tietoja palveluntarjoajan tai pankin sitä havaitsematta.

Kukin osapuoli vastaa omien palveluittensa suojauksesta, turvallisuudesta ja säilyttämiensä tietojen oikeellisuudesta. Tunnistautuva asiakas vastaa siitä, että pankin antamat pankkitunnukset eivät joudu ulkopuolisten haltuun. Palveluntarjoajan on huomautettava asiointipalvelussaan, että palvelussa käytetään varmennepalvelua, jossa käytetään henkilöasiakas tai yritysasiakaskäyttöön tarkoitettuja pankkitunnuksia. Palveluntarjoajan tulee muokata asiointipalvelussaan olevaa huomautustekstiä sen mukaisesti haluaako palveluntarjoaja tunnistaa henkilöasiakkaita vai yritysasiakkaita. (Finanssialan keskusliitto 2007.)

6.3 KATSO-ORGANISAATIOTUNNISTE

Katso-organisaatiotunniste on Verohallinnon ja Kelan perustama yhteinen maksuton organisaatioiden tunnistamiseen tarkoitettu palvelu, jota käytetään viranomaisten sähköisissä asiointipalveluissa. Sen peruskonseptin mukaan organisaatiolle nimetään pääkäyttäjä, joka voi jakaa organisaatiossa oleville henkilöille erilaisia rooliin sidottuja käyttöoikeuksia. Katso-tunnisteen avulla voi valtuuttaa esimerkiksi työntekijän tai tilitoimiston toimimaan yrityksen puolesta.

Katso-organisaatiotunniste korvaa ajan mittaan entiset Tyvi-tunnukset. Katso-organisaatiotunniste koostuu käyttäjätunnuksesta, salasanasta ja kertakäyttösalasanasta. Tunnisteella kirjauduttaessa saadaan luotettavasti selville tunnisteen omistaja ja hänen oikeutensa toimia muiden puolesta.

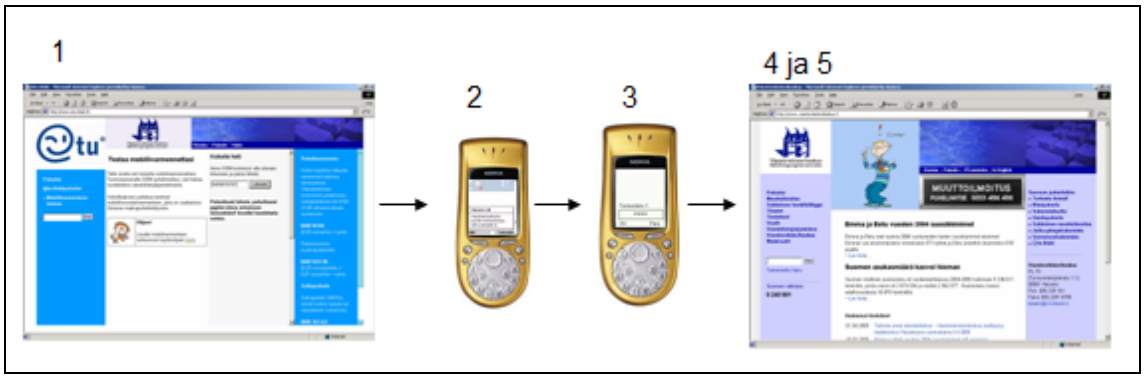
Verohallinnon palveluissa Katso-organisaatiotunnistetta voi käyttää esimerkiksi Tyvi-palveluissa (kuukausi-ilmoittamiseen, vuosi-ilmoittamiseen, tuloveroilmoittamiseen). Tunnistetta voi käyttää myös muiden viranomaisten, kuten Kelan tarjoamissa

palveluissa. Pääkäyttäjän Katso-organisaatiotunnisteen voi hakea verkkopankkitunnuksilla tai HST-kortilla.

6.4 MOBIILIVARMENNE

Edellä selvitettyjen tunnistuspalveluiden lisäksi myös teleyritykset tarjoavat varmennepalveluita. Matkaoperaattoreiden tarjoamat, yleiseen käyttöön kehitetyt tunnistamispalvelut perustuvat matkapuhelinliittymän SIM- korttiin liitettävään mobiilivarmenteeseen ja julkisen avaimen menetelmään. TeliaSoneralla ja Elisalla on noin 4,6 miljoonaa matkapuhelinliittymää Suomessa (2008). TeliaSoneran ja Elisan tunnistamispalveluissa varmentajana toimii Väestörekisterikeskus. Varmenteet ovat kansalais- ja laatuvarmenteita. Mobiilivarmenteita voidaan käyttää henkilön sähköiseen tunnistamiseen, lain sähköisestä allekirjoituksesta tarkoittamiin kehittyneisiin sähköisiin allekirjoituksiin sekä tiedon eheyden ja muuttumattomuuden suojaamiseen digitaalisella allekirjoituksella. Mobiilitunnistamisen on tarkoitus olla maksullista sekä palveluntarjoajalle että varmenteen haltijalle. Teleoperaattoreiden tarjoama mobiilivarmenne edellyttää PKI- ominaisuuksilla varustettua SIM-korttia, jonka liikkeellelaskijana operaattori toimii. Mobiilivarmenne toimii kaikissa matkapuhelimissa, eikä edellytä erillisiä lukijalaitteita tai ohjelmistoja. Mobiilivarmenteen etuna on myös se, että matkapuhelin on useimmilla lähes aina mukana, eli päätelaite on lähes aina käytettävissä. Käyttäjä yksilöidään henkilötunnuksella (SATU). Mobiilivarmenteita voidaan hyödyntää Internetselainpohjaisissa palveluissa, mobiilipalveluissa ja asiakaspuhelinpalveluissa. Tunnistamisprosessin turvallisuuden kannalta on merkittävää, että tunnistus tehdään eri kanavassa kuin asiointikanava. (Arjentietoyhteiskunnan neuvottelukunta 2008.)

Tunnistaminen mobiilivarmenteella tapahtuu kuvion 4 mukaisesti seuraavasti:



KUVIO 4. Tunnistaminen mobiilivarmenteella

1) Käyttäjä kytkeytyy tietokoneella asiointipalveluun ja valitsee tunnustaudu mobiilivarmenteella ja syöttää gsm-numeron
2) Tunnistuspyyntö lähetetään käyttäjän matkapuhelimeen
3) Käyttäjä syöttää henkilökohtaisen tunnistamis-PIN:in
4) Tunnistamispyyntö välitetään palvelulle
5) Tunnistaminen suoritettu (Vainio 2008).

Matkapuhelimen pieni koko on liikuteltavuuden kannalta etu, mutta toisaalta se rajoittaa huomattavasti matkapuhelimeen toteutettavia sovelluksia ja heikentää niiden käytettävyyttä. Matkapuhelimen katoaminen tai varastaminen, aiheuttaa häiriöitä palveluiden saatavuuden suhteen sekä voi aiheuttaa kalliitakin varajärjestelyjä. Mobiilivarmenteen ja operaattorin rajapintojen käytöstä koituu myös kustannuksia kuukausimaksujen ja teksti-viestien muodossa.

6.4.1 Mobiili Asiointivarmenne – konsepti

Suomalaiset teleoperaattorit suunnittelevat kehittävänsä ja tuovansa markkinoille uuden Mobiili Asiointivarmenteen vuoden 2009 aikana. Varmenteen suunnittelussa on huomioitu erityisesti suomalaisten liikepankkien tarpeet henkilöiden verkkotunnistamisen kehittämisessä. Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry on valmistellut Mobiili Asiointivarmenne-palvelukonseptia työryhmässä, jossa ovat olleet edustettuina DNA Finland oy, Elisa Oyj ja TeliaSonera Oy. Esitys on toimitettu Finanssialan keskusliiton jäsenille jatkokeskustelun pohjaksi heinäkuun 2008 aikana.
Mobiili Asiointivarmenne – konsepti on matkapuhelinverkon SIM-kortilla toteutettava henkilökohtainen asiointivarmenne. Varmennepalvelun tuottaa teleoperaattorit. Teleoperaattorit toimivat itsenäisinä varmentajina (CA, Certication Authority) yhteisen

varmennepolitiikan mukaisesti. Yhteinen varmennepolitiikka takaa palveluntarjoajalle yhdenmukaisen toimintamallin ja turvallisuustason eri varmentajien kesken. Palvelukonsepti on ensisijaisesti suomalaisille liikepankeille tarjottava tunnistus- ja allekirjoitusrajapinta. Konsepti on hyvin samankaltainen kuin operaattoreiden ja Väestörekisterikeskuksen toteuttama kansalaisvarmennepalvelu.

Asiointivarmenne ei ole laatuvarmenne, vaan markkinatarvetta vastaava riittävän turvallinen henkilön tunnistamisen ja allekirjoittamisen helppokäyttöinen väline. Mobiili Asiointivarmenne -konseptin arvioidaan täyttävän Rahoitustarkastuksen standardin, joka määrittää vaatimukset asiakkaan tunnistamisesta ja tuntemisesta rahanpesun, terrorismin rahoituksen sekä markkinoiden väärinkäytösten estämiseksi. Konseptia on arvioitu suhteessa EU:n IDABC:n (Interoperability for PEGS Authentication assurance levels) valmistelemaan ehdotukseen tunnistusratkaisujen turvatasoista.

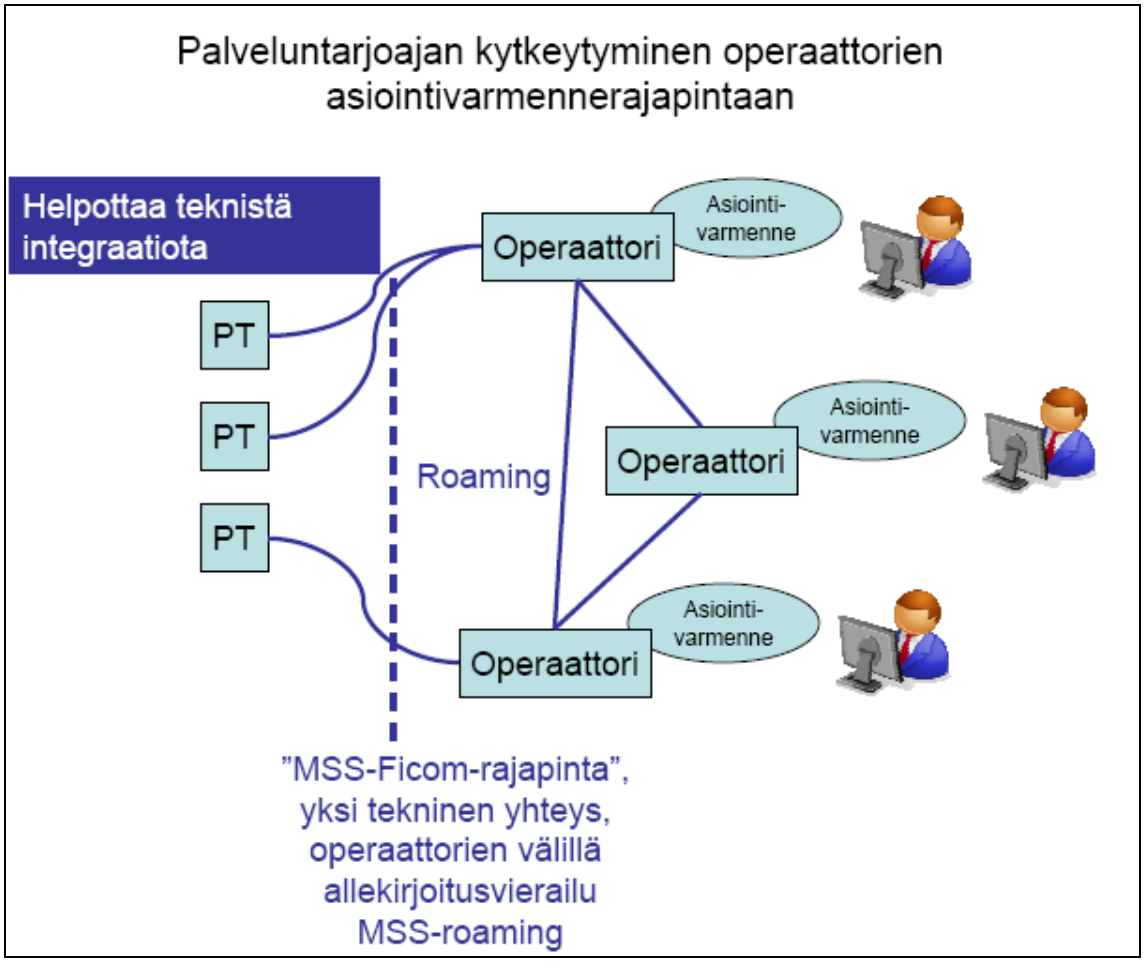
Asiointivarmenne on maksullinen matkapuhelinliittymän palvelu, joka voidaan hankkia yksityishenkilön tai yrityksen matkapuhelin liittymän haltijalle. Tunnistusvälineenä toimii SIM-kortti, jolla sijaitsevat henkilön yksityiset tunnistus- ja allekirjoitusavaimet. RSA-avainten pituus on aluksi 1024 bittiä. Avainpituutta kasvatetaan kokonaisratkaisun turvallisuustason säännöllisen arvioinnin perusteella. Avainten käyttö on suojattu henkilön asetettavissa olevilla 4-merkkisillä SPIN-tunnusluvuilla, joka lukkiutuu usean väärän yrityksen jälkeen. Lukkiutuneen kortin voi avata vain henkilön hallussa olevalla SPUK-koodilla.

Asiointivarmenne sisältää henkilön pysyvät identiteettitiedot, jotka ovat henkilön virallinen nimi, henkilötunnus salatussa muodossa (tiivisteenä), mahdollisesti myös sähköinen asiointitunnus (SATU), syntymäaika, sukupuoli ja kansalaisuus. Varmenteen tietosisältö mahdollistaa selväkielisten tietojen tarkastamisen suoraan, henkilötunnuksen tarkastamisen (henkilötunnuksen tarkastamisen), silloin kun henkilö on itse luovuttanut sen palveluntarjoajalle. Henkilötunnuksen tiivistettä voidaan käyttää tietojärjestelmissä henkilön yksilöimiseen.

Teleoperaattoreiden tarkoituksena on, että käyttäjiä ohjataan verkkopankissa hankkimaan Mobiili Asiointivarmenne. Varmenteen voisi rekisteröidä ensivaiheessa itsepalveluna operaattorien verkkoasiointipalvelussa verkkopankkitunnusten avulla. Asiointivarmenteen käyttöönotto edellyttää SIM-kortin vaihtoa. Varmenne voidaan rekisteröidä operaattorin verkkopalvelun kautta, kun uusi SIM-kortti on aktivoitu

matkapuhelinverkkoon. Myöhemmin on tarkoitus toteuttaa kasvokkain rekisteröinti operaattorin tai pankin toimipisteessä. Asiointivarmenteen voi uusia verkkoasiointipalvelun kautta ennen sen voimassaolon päättymistä.

Teleoperaattorit tarjoavat siis tulevaisuudessa yhtenäisen standardisoidun ratkaisun suomalaisille liikepankeille henkilöiden tunnistamista ja sitoumusten allekirjoittamista varten. Palveluntarjoajan liittymärajapinta perustuu ETSI:n standardiin TS 102.204 (Mobile Signature Service) ja Ficomin MSS- soveltamisohjeeseen (ks. kuvio 5). Toteutuksen etuna on operaattorien välinen allekirjoitusvierailu, joka mahdollistaa palveluntarjoajalle yhden operaattorin teknisen käyttöyhteyden kautta kaikkien operaattoreiden asiointivarmennekäyttäjien tavoittamisen. Yhteyden osapuolet tunnistetaan varmenteilla ja liikenne suojataan salaamalla. Palvelusopimukset ovat todennäköisesti operaattorikohtaiset nykyisen käytännön mukaisesti. (FiCom Tietoliikenteen ja tietotekniikan keskusliitto 2008.)



KUVIO 5. Palveluntarjoajan kytkeminen operaattorien asiointivarmennerajapintaan

7 VAHVAN SÄHKÖISEN TUNNISTAMISEN LINJAUKSET SUOMESSA

Kansalaisten sähköisten palveluiden ja asioinnin kehittymistä edistävälle Arjen tietoyhteiskunnan neuvottelukunnalle on esitetty 15.10.2008 pidetyssä kokouksessa kansalliset vahvan sähköisen tunnistamisen suuntaviivat. Suuntaviivoja on valmisteltu neuvottelukunnan sähköisen tunnistamisen kehittämisryhmän toimesta, joka koostuu sekä yksityisten että julkisen sektorin asiantuntijoista.

Tavoitteena on luoda Suomeen edellytykset toimivien vahvan sähköisen tunnistamisen markkinoiden syntymiselle. Tunnusomaista markkinoille on tunnistusvälineiden yleiskäyttöisyys ja vapaa kilpailu. Keskeisenä edellytyksenä markkinoiden syntymiselle ja toimimiselle on osapuolten välinen yhteistyö. Sähköisessä tunnistamisessa erotetaan heikko ja vahva tunnistaminen. Lainsäädännöllä säädellään vahvan tunnistamisen palveluiden tarjonnan puitteet.

Vahvan tunnistamisen luotettavuus perustuu käytettyyn menetelmään, palvelumallin turvallisuuteen ja auditoitaviin prosesseihin sekä toteutustapoihin. Luotettavuus perustuu myös lainsäädännössä vahvan sähköisen tunnistamisen palveluiden tarjoamiselle asetettaviin perusedellytyksiin, vahvan tunnistamisen palvelua tarjoavien ja sitä käyttävien palvelutarjoajien muodostamaan luottamusverkostoon sekä viranomaisvalvontaan. Vahva sähköinen tunnistaminen soveltuu lähtökohtaisesti kaikkeen luotettavaan sähköiseen tunnistamiseen yksityisellä ja julkisella sektorilla. Käyttäjien luottamus vahvan sähköisen tunnistamisen palveluihin edellyttää lisäksi, että palveluntarjoajat varmistavat, että kuluttaja- ja yksityisyyden suojaa koskevia säännöksiä noudatetaan sovitusti.

Käyttäjälähtöisyys on vahvan sähköisen tunnistamispalveluiden tarjonnan perusta. Jokainen käyttäjä voi valita itselleen sopivimman tunnistamismenetelmän markkinoilla tarjolla olevista vahvan sähköisen tunnistamisen vaihtoehdoista.

Huomioitavaa on, että vahva sähköinen tunnistaminen ei ole itse tarkoitus vaan luotettavan sähköisen asioinnin mahdollistaja. On olemassa myös palveluja, joissa tunnistaminen ei ole lainkaan tarpeen. Palveluntarjoajien on erotettava ne palvelut, joissa tunnistaminen on tarpeen.

Liikenne- ja viestintäministeriö on valmistellut säännökset vahvalle sähköiselle tunnistamiselle. Säännökset esitetään lisättäväksi lakiin sähköisistä allekirjoituksista. Uudella lainsäädännöllä halutaan luoda puitteet sille, että markkinoilla olisi useita vahvoja tunnistamismenetelmiä helposti kansalaisten saatavissa. Laki toisi sähköisten tunnistamispalveluiden tarjonnalle perussäännöt. Samalla varmistettaisiin palveluntarjoajien viranomaisvalvonta sekä palveluiden luotettavuus ja turvallisuus. (Liikenne- ja viestintäministeriö 2008.) Lakiluonnos on ollut lausuntokierroksella. Lain voimaantuloajaksi on ehdotettu syyskuuta 2009 (Tietosuoja 4/2008).

8 TAPIOLA

8.1 Vakuutusyhtiöiden verkkopalvelut

Vakuutusyhtiöt ovat jo usean vuoden ajan rakentaneet ja kehittäneet verkkopalveluita henkilö- ja yritysasiakkaiden käyttöön. Nykyään verkkopalvelut ovat laajoja ja kattavia kokonaisuuksia, joissa asiakkaat voivat esimerkiksi ylläpitää vakuutusasioita, hankkia uusia vakuutuksia ja tehdä vahinkoilmoituksia. Asiakkaat hoitavat usein rutiiniasiat itse verkkopalvelussa. Henkilökohtaisessa palvelussa toimistossa tai edustajatapaamisessa hoidetaan henkilö- ja yritysasiakkaiden vaativammat vakuutus- ja sijoitusratkaisut.

Järvisen mukaan vakuutusalan verkkoliiketoiminnassa on pääasiassa kyse erityisesti vakuutusten ylläpitoon liittyvistä palveluista, mutta myös palveluiden myynnistä ja markkinoinnista. Internetin verkkopalvelujen tarkoitus ei siis niinkään ole vakuutusten myyminen, vaan vakuutusten hoitoon liittyvien palveluiden tarjoaminen (Järvinen ym. 2001, 11). Vakuutusten hoitaminen kattaa voimassaolevien vakuutusten koko elinkaaren mittaiseen jatkokäsittelyyn liittyvän asiakaspalvelun. Vakuutusten hoitamiseen tarjottavia palveluita verkkopalvelussa ovat mm. vakuutuskirjan ja -ehtojen tulostaminen, vakuutuksen muutostiedot ja ajankohdat, korvaushakemusten syöttäminen ja korvauskäsittelyn edistymisestä informointi. Näillä palveluilla vakuutusyhtiöt saavat kasvatettua asiakasuskollisuutta ja pienennettyä käsittelykustannuksiaan. (Järvinen ym. 2001, 22.)

Linkola ja Riittinen-Saarno totesivat jo melkein kaksikymmentä vuotta sitten, että palvelut yleensä ovat työvaltaista toimintaa. ”Palvelua ja varsinkin sen kalleinta,

henkilökohtaisinta osaa helpottaa, jos vakuutusasiakas on omatoiminen, selvittää itselleen asiat, ottaa itse yhteyttä yhtiöönsä ja hoitaa kaikin puolin muutenkin asiansa kuten ’huolellinen mies”. Suurin osa vakuutusasiakkaista ei kuitenkaan ryhdy kovin omatoimisiksi. Vakuutustietojen hankinta voi tuntua asiakkaista niin monimutkaiselta, että he menevät mielellään vakuutusyhtiön toimistoon selvittämään asiaa, vaikka se selviäisi esitteitä lukemallakin. (Linkola & Riittinen-Saarno 1992, 146.)

Linkola ja Riittinen-Saarno (1992, 147) uskoivat, että omatoimisuutta voi kasvattaa, jos siitä on asiakkaille etua tai edes aistein havaitsematonta hyötyä. Vakuutusyhtiöt voisivatkin ehkä palkita niitä asiakkaita, jotka omatoimisesti hoitaisivat asioitaan esimerkiksi Internetissä olevan verkkopalvelun välityksellä. Linkola ja Riittinen-Saarno pohtivat kuitenkin, että asiakkaiden ohjaamisessa omatoimisuuteen on vahva este.
Asiakkaan omatoimisuutta vakuutusalalla estää kenties yksinkertaisesti se, että vaikeita vakuutusasioita ei kannata opetella kovin hyvin ja omatoimisesti hoitamaan. Tulevathan ne ajankohtaisiksi melko harvoin ja asiantuntija-apua on silloin saatavissa, palvelu pelaa (Linkola & Riittinen-Saarno 1992, 147).

Pankkipalveluihin verrattuna vakuutusasioita hoidetaankin suhteellisen harvoin verkossa. Tämä saattaa olla eräs syy siihen, että vakuutuksia myydään verkossa rajallisemmin kuin olisi mahdollista. Internetissä tarjottaville vakuutusasioiden lisäpalveluille on kuitenkin kysyntää. Käytännöllisiä lisäpalveluita ovat esimerkiksi vahinkoilmoitusten tekeminen verkon välityksellä sekä yksinkertaisimpien vakuutusten, kuten liikenne- ja matkavakuutusten ostaminen tai erilaiset muutosilmoitukset. Kuten todettua, Internet ei ole niinkään vakuutusten myyntikanava, vaan ennen kaikkea asiakkaiden hoitokanava. Hoitokanavan välityksellä erilaisten ilmoitusten ja muutosten tekeminen vakuutusyhtiöiden ja kuluttajien kesken on ensiarvoisen helppoa. Toistaiseksi Internetiin näyttäisivätkin siis sopivan parhaiten yksinkertaisimmat vakuutuspalvelut sekä erilaiset lisäpalvelut. (Järvinen ym. 2001, 22, 44.)

8.2 Tapiolan verkkopalvelut

Tapiola on suomalainen vakuutus- ja finanssiyhtiöryhmä, johon kuuluu neljä keskinäistä vakuutusyhtiötä – Keskinäinen Vakuutusyhtiö Tapiola, Keskinäinen Eläkevakuutusyhtiö Tapiola, Keskinäinen Henkivakuutusyhtiö Tapiola ja Yritysten Henkivakuutus Oy Tapiola – sekä Tapiola Omaisuudenhoito Oy, Tapiola Rahastoyhtiö Oy ja Tapiola Pankki Oy. Yhtiöryhmän omistavat sen asiakkaat eli vakuutuksenottajat.

Yksityistalousasiakkaiden määrä on jatkanut kasvuaan ja oli vuoden 2007 lopulla runsaat 872 000. Yksityistalouksiin luetaan kotitaloudet, maatilat ja yrittäjät. Yritys- ja yhteisöasiakkaiden määrä oli vuoden lopulla runsaat 30 000. Varainhoitoyhtiössä osuudenomistajien määrän kasvu jatkui. Vuoden 2007 päättyessä osuudenomistajia oli runsaat 29 000. Pankilla puolestaan oli vuoden 2007 lopulla 118 000 asiakasta.

Tapiola-ryhmä tarjoaa asiakkailleen vakuutus-, pankki-, säästö- ja sijoittajapalveluita. Tapiolan toiminta-ajatuksena on edistää kokonaisvaltaisesti asiakkaidensa taloudellista turvaa. Toiminta-ajatustaan Tapiola-ryhmä toteuttaa neljän arvonsa – asiakkaiden etu, yrittäjähenkisyys, eettinen toiminta ja yhdessä menestyminen – avulla. Arvot muodostavat kiinteän kokonaisuuden.

Tapiola-ryhmä palvelee asiakkaitaan useiden eri palvelukanavien välityksellä. Tapiolan palveluja saa yli 160 palvelupaikasta, joista toimistoja on noin 70. Jäljelle jäävät noin 90 palvelupaikkaa ovat yrittäjävetoisia franchising-pisteitä. Harvaan asutulla maaseudulla asiakkaita palvelee puolestaan aktiivinen vakuutusedustajaverkosto. Puhelinpalvelusta asiakkaat saavat neuvoja arkisin klo 8.00–20.00. Tapiolan Internet-sivut palvelevat asiakkaiden tiedontarvetta ympäri vuorokauden. Avoimilta Internet-sivuilta verkkopalvelusopimuksen tehneet henkilö- tai yritysasiakkaat voivat kirjautua verkkopalveluihin. Henkilöasiakkaan verkkopalvelussa näkyvät talouden kaikki vakuutus-, pankki-, säästö- ja sijoitusasiat. Yritysasiakkaan verkkopalvelu on jaettu erillisiin palveluihin, kuten esimerkiksi vakuutus-, rahasto-, pankki- ja työhyvinvointipalvelut. Jokaisessa verkkopalvelussa on oma tunnistamistapa (käyttäjätunnus ja salasanat) ja käyttäjähallinta.

Yrityksen liiketoiminta on yhä enemmän riskienhallintaa. Tapiola on erikoistunut yritysten riskienhallintaan, vakuuttamiseen ja taloudellisiin ratkaisuihin. Yrityksen liiketoimintaan ja tarpeisiin soveltuvat ratkaisut koostuvat: henkilöstön, omaisuuden ja toiminnan ratkaisuista sekä talouden ratkaisuista. Henkilöstöriskien hallinnan ratkaisut voivat koostua seuraavista vakuutuksista ja palveluista:

1. Lakisääteinen tapaturmavakuutus
2. Työntekijän eläkevakuutus
3. Henkilöstökartoitukset
4. Ratkaisut vaihtuvuuden tai poissaolojen vähentämiseen
5. Työhyvinvoinnin lisääminen
6. Sitouttamisratkaisut

7. Koulutus ja neuvonta
8. Korvauspalvelut.

Omaisuuden ja toiminnan yrityspalvelut puolestaan käsittävät mm. erilaiset riskikartoitukset, vakuuttamisen (sisältäen turvantarkistuksen) ja sen perusteella sopivan vakuutusturvan tarjoamisen, koulutuksen ja neuvonnan sekä korvauspalvelun.

Tapiolan yritysten verkkopalvelujen tarjoamisen liiketoiminnallinen tavoite on, että kaikki yritysasiakkaat käyttävät sähköisiä palveluja rutiiniasioiden hoitamiseen. Jotta tavoitteeseen voidaan päästä, on palvelun käytön oltava vaivatonta, helppoa ja yksinkertaista. Yrityksille tarjotaan Internet-sivuilla olevien lomakkeiden, kuten esimerkiksi erilaisten vahinkoilmoitusten, todistusten ja vuosi-ilmoitusten lisäksi vahvan sähköisen tunnistamisen vaativia verkkopalveluja. Noin 18 000 yritystä hoitaa tavalla tai toisella yrityksensä asioita verkkopalvelussa. Kuukausittain verkkopalveluun kirjaudutaan keskimäärin 4 000 kertaa. Verkkopalvelun voivat ottaa käyttöön kaikki Tapiolan yritysasiakkaat, joilla on vähintään yksi jatkuva vakuutus Tapiolassa. Yritysasiakkaan verkkopalvelu on yritysasiakkaalle maksuton.

8.2.1 Verkkopalvelujen luokat

Tapiolan Internet-sivut yritysasiakkaille (www.tapiola.fi > yritysasiakkaat) ovat informatiivinen sivusto ja sivuston käyttäjät ovat anonyymejä. Sivuston tavoitteena on tiedottaa Tapiolan tarjoamista ratkaisuista ja saada yritysasiakas ottamaan yhteyttä Tapiolaan. Tapiola.fi on siis verkkopalvelutyyppiluokituksen (ks. luku 3) päätyypin A mukainen verkkopalvelu, jossa asiakkaalle tarjotaan tietopalveluita ja jossa asiakkaille tiedotetaan ajankohtaisista asioista.

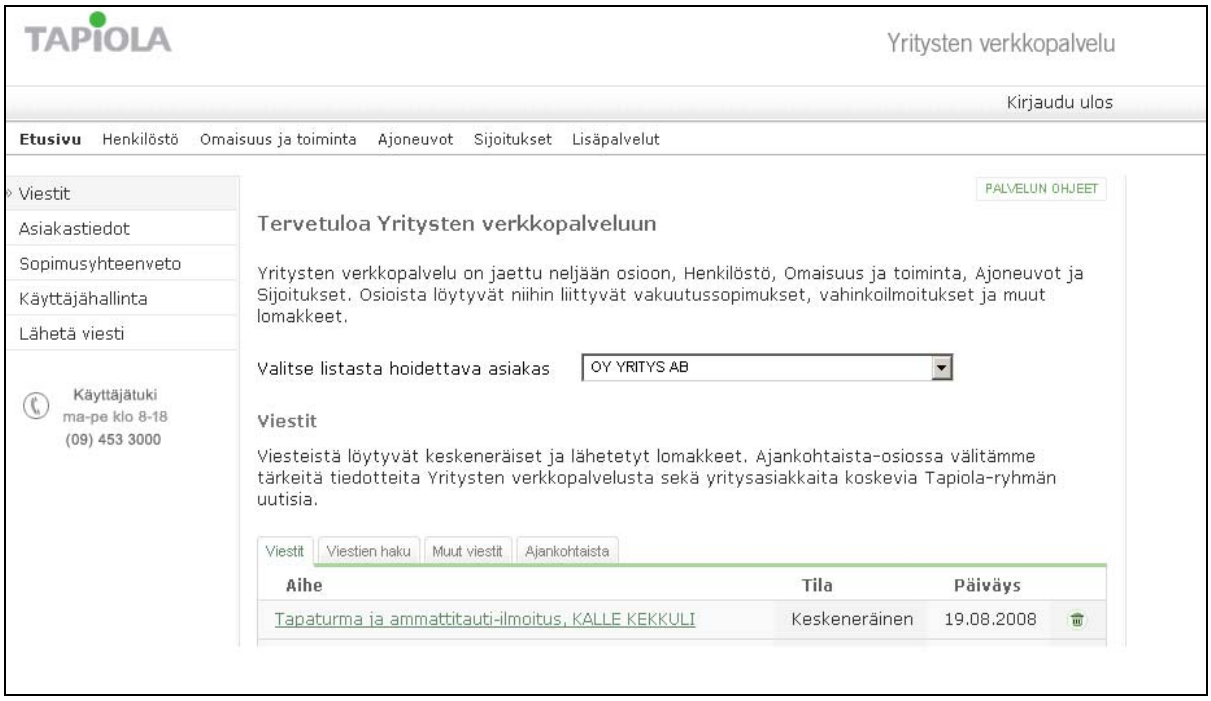
Tapiolan Internet-sivuilta löytyy yhteydenotto- ja palautelomake (https://www2.tapiola.fi/yritykset/yhteydenotto/yhteystiedot.asp), jonka avulla sivustolla vieraileva kävijä voi antaa palautetta sivustolta. Lomakkeella pyydetään käyttäjän yhteystietoja, kuten yrityksen nimi ja yhteyshenkilö mutta puhelinnumeroa tai sähköpostiosoitetta ei ole pakollista antaa, joten palvelu vastaa verkkopalvelu päätyyppiä B, jossa voidaan antaa asiakaspalautetta. Palvelun käyttäjä on anonyymi. Yhteydenotto- ja palautelomake on SSL-suojattu.

Tapiolan Internet-sivujen Asioi verkossa osioon (tapiola.fi > Yritysasiakkaat > Asioi verkossa) on kerätty erilaisia sovelluksia, kuten laskimia, lomakkeita, vahinkoilmoituksia. Esimerkiksi Työtapaturma- ja ammattitauti-ilmoituksen voi lähettää tapiola.fi:n kautta ilman erillistä tunnistautumista. Sovelluksia voi käyttää siis kaikki sivuilla vierailevat käyttäjät. Kaikki sovellukset ovat SSL-salattuja, koska niissä on henkilötietoja ja useimmiten muita arkaluonteisia tietoja. Sovellukset ovat verkkopalvelun päätyyppiä D, jossa asiakkaalle tarjotaan mahdollisuus täyttää ja lähettää lomake sähköisesti.

Tapiolan tarjoama ekstranet-palvelu nimeltään Yritysasiakkaan verkkopalvelu (https://yrityspalvelu.tapiola.fi/a3/YvpAuthWeb/auth) sisältää yritysasiakkaan reaaliaikaista asiakkuus-, vakuutus- ja korvaustietoa. Yritysasiakkaan verkkopalvelu on vuorovaikutteista asiointia ja tiedot ovat luottamuksellisia. Verkkopalvelua voi käyttää vain Tapiolan kanssa verkkopalvelusopimuksen tehneen yrityksen käyttäjät. Yritysasiakkaan verkkopalvelu on päätyyppiä E, jossa käsitellään asiakkaan luottamuksellisia henkilökohtaisia tietoja. Käyttäjät ovat vahvasti todennettuja käyttäjiä.

8.2.2 Verkkopalvelujen sisältö

Yritysasiakkaan verkkopalvelu on jaettu viiteen osioon: Henkilöstö, Omaisuus ja toiminta, Ajoneuvot, Sijoitukset ja Lisäpalvelut. Kuviossa 6 on esitetty verkkopalvelun etusivu, josta selviää palvelun rakenne.

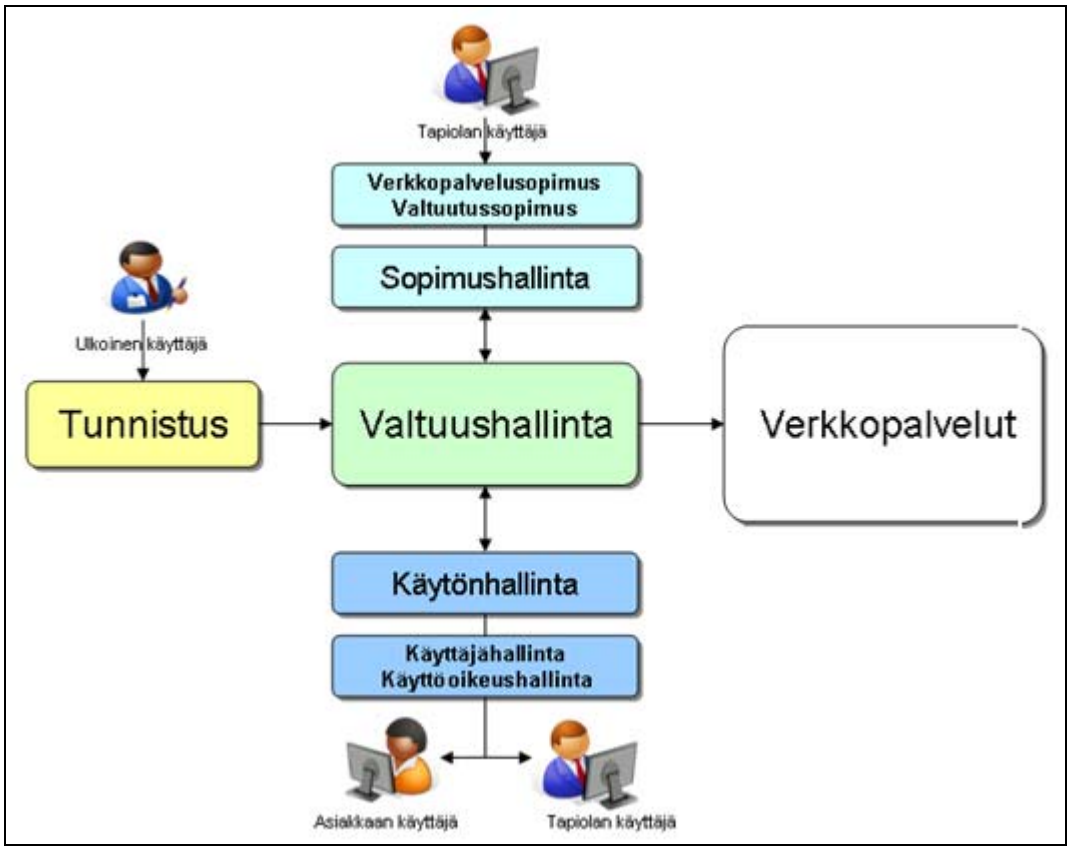


KUVIO 6. Yritysasiakkaan verkkopalvelun etusivu

Yrityksen käyttäjille annetaan käyttöoikeusrooleja verkkopalvelussa. Verkkopalvelussa on tällä hetkellä seitsemän erilaista roolia, jotka rajaavat käyttäjän verkkopalvelu näkymää. Käyttäjäroolit ovat:

- työeläke eli TyEL -vakuutusten hoitaminen
- työtapaturmavakuutusten hoitaminen
- vapaaehtoisten henkilövakuutusten hoitaminen
- lisäeläkevakuutusten hoitaminen
- vakuutussijoitusten hoitaminen
- omaisuuden ja toiminnan vakuutusten hoitaminen sekä
- käyttäjähallinta, joka sisältää käyttöoikeuksien ja käyttäjätietojen ylläpitämisen

Käyttäjät voivat saamiensa käyttöoikeusroolien puitteissa henkilöstö-osiossa esimerkiksi täyttää vahinkoilmoituksia, tehdä muutoksia vakuutustietoihin, ilmoittaa TyEL -vakuutuksen vuosi- tai kuukausi-palkkailmoituksia ja lakisääteiseen tapaturmavakuutukseen liittyviä tapaturma- ja ammattitauti-ilmoituksia. Omaisuus- ja toiminta-osiossa yrityksen käyttäjät voivat tarkastella vakuutuksien tarkempia tietoja, kuten esimerkiksi yritysvakuutuksella vakuutettuja kohteita ja niiden vakuutusmääriä. Omaisuus- ja toiminta-osiosta löytyvät yhteystiedoilla esitäytetyt sähköiset vahinkoilmoitukset. Seuraavassa kuviossa 7 on vielä esitetty Tapiolan yritysten verkkopalvelun tunnistus- ja käyttäjähallinta.



KUVIO 7. Yritysasiakkaan verkkopalvelun tunnistus- ja käyttäjähallinta

8.2.3 Verkkopalvelusopimus

Sopimuksen verkkopalvelun käytöstä Tapiolan kanssa voi tehdä yrityksen nimenkirjoitusoikeudellinen henkilö tai hänen valtuuttama henkilö. Verkkopalvelupalvelusopimukseen liitetään aina yrityksen pääkäyttäjä. Yritys voi valtuuttaa valtakirjalla esimerkiksi meklaritoimiston tai tilitoimiston hoitamaan yrityksen vakuutusasioita verkkopalvelussa. Verkkopalvelun pääkäyttäjä voi lisätä muita henkilöitä verkkopalvelun käyttäjiksi sekä tilata heille käyttöoikeusrooleja. Kaikille käyttäjille pääkäyttäjä mukaan lukien voidaan antaa eritasoisia oikeuksia esimerkiksi sen mukaan, minkälaisia asioita he yrityksessä hoitavat. Palkka-asioita hoitavan henkilön käyttöoikeudet voidaan esimerkiksi rajata koskemaan lakisääteiseen tapaturmavakuutukseen ja työeläkevakuutukseen liittyviä asioita.

8.2.4 Yritysasiakkaan verkkopalvelun tunnistautumisratkaisu

Käyttäjän tunnistautuminen yritysasiakkaan verkkopalveluun tapahtuu käyttäjätunnuksen ja kertakäyttöisen salasanan avulla. Käyttäjille voidaan antaa eritasoisia käyttäjärooleja, joiden mukaan yritysasiakkaan verkkopalvelun etusivu sekä sisältö muodostetaan. Käyttäjäroolien avulla varmistetaan, että esimerkiksi yrityksen palkkatietoja ei näytetä sellaiselle käyttäjälle, joka ei niitä tietoja tarvitse työssään.

Tapiolassa on tehty päätös, jonka mukaan nykyistä vakuutusosion tunnistus- ja käyttöoikeushallintajärjestelmää ei enää jatkossa kehitetä ja siten muun muassa. tunnistustapa on uusittava. Tapiolan liiketoimintavaatimuksina on, että yritysasiakkaalle voidaan tarjota vaihtoehtoisia luotettavia henkilön vahvoja tunnistautumistapoja. Tavoitteena on, että yrityksen pääkäyttäjä voi hallinnoida reaaliaikaisesti yritysasiakkaan verkkopalvelussa yrityksen muiden käyttäjien käyttöoikeuksia. Käyttöoikeuksien ulkoistaminen yritysasiakkaan pääkäyttäjälle nostaa tietoturvan tasoa, koska pääkäyttäjä vastaa siitä, että tiedot ovat ajan tasalla eikä väärinkäytöksiä pääse helposti syntymään.

Kilpailijoiden vastaavista verkkopalveluista voidaan todeta, että useimmilla yhtiöillä on käytössä Tupas-palvelu sekä vaihtoehtoisesti yhtiön omat käyttäjätunnukset. If vakuutusyhtiön If Yrityskansioon kirjaudutaan If Yrityskansiotunnuksilla tai verkkopankkitunnuksilla, samoin Pohjolan e-palveluun voi kirjautua Pohjolan verkkotunnuksilla tai verkkopankkitunnuksilla. Ilmarisen vakuutuspalveluun voi kirjautua joko Ilmarisen verkkopalvelutunnuksilla tai yrittäjät voivat kirjautua vakuutuspalveluun myös verkkopankkitunnuksilla. Työeläke.fi:n palveluun voi kirjautua sähköisellä henkilökortilla tai verkkopankkitunnuksilla eli tupas-palvelulla (www.tyoelake.fi/). Käyttäjät ovat siis tottuneet jo käyttämään verkkopankkitunnuksia vastaavissa verkkopalveluissa.

Teoria-osuudessa esitettyjen henkilön vahvan sähköisen tunnistamisen vaihtoehdoista varteenotettavin on pankkien tarjoama Tupas-palvelu (ks. luku 7), koska muut vahvat tunnistustavat eivät ole yleistyneet toivotulla tavalla tai niitä ei ole vielä luotu lopulliseen muotoonsa. Tupas-palvelun etuna on, että useimmiten yrityksen käyttäjillä on jo jonkun tai useamman pankin verkkopankkitunnukset käytössä verkkopalvelusopimusta tehtäessä. Tapiolan ei näin ollen tarvitse erikseen jakaa käyttäjätunnusta ja salasanoja postitse tai toimistoilta verkkopalvelun käyttäjälle. Tämä nopeuttaa palvelun

käyttöönottoa huomattavasti sekä säästää kustannuksia mm. painatus- ja postituskuluissa. Tupas-palvelu on luotettava henkilön vahva sähköinen tunnistus. Tupas-palvelu on myös Internet-käyttäjien keskuudessa luotettu ja tunnettu palvelu, koska isot toimijat, kuten Verohallinto ja Kela käyttävät jo Tupas-palvelua käyttäjän tunnistamiseen.

Palveluntarjoajan näkökulmasta Tupas-palvelun heikkoutena on pankkien perimät Tupas-palveluiden käyttökustannuksiin perustuvat maksut, jotka koostuvat palvelun avausmaksusta, kiinteästä kuukausimaksusta sekä tapahtumaveloituskohtaisesta maksusta eli jokaisesta tunnistustapahtumasta palveluntarjoaja maksaa ko. pankille. Toisena heikkoutena on epävarmuus siitä, haluaako työntekijä käyttää omia verkkopankkitunnuksia tunnistautumisessa yrityksen asioiden hoitamista varten. Tämä asia tutkittiin lähettämällä pääkäyttäjille sähköinen asiakaskysely (ks. luku 9.4.1). Saatujen tulosten perusteella ei ole estettä ottaa Tupas-palvelua käyttöön. Tapiolassa yrityksen käyttäjille voidaan antaa Tapiola pankin verkkopankkitunnukset riippumatta siitä, millainen asiakkuus (pankki-, rahasto tai vakuutus) käyttäjällä on Tapiolassa. Käyttäjä voi siis saada käyttöönsä verkkopankkitunnukset, joita käyttäjä käyttää vain asioidessaan yritysten verkkopalvelussa.

Tupas-palvelun eduista huolimatta tunnistuspalvelua ei kuitenkaan ole syytä rajata yksinomaan Tupas-palvelulle, joka käyttää hyväksi yrityksen y-tunnusta ja henkilöasiakkaan henkilötunnusta. Teknisessä ratkaisussa täytyy ottaa huomioon se mahdollisuus, että henkilötunnuksen sijaan käyttäjä voidaan tunnistaa myös jollain muulla tunnuksella, kuten sähköisellä tunnuksella. Uusien tunnistusratkaisujen on oltava helposti liitettävissä tunnistuspalveluun. Tulevaisuudessa on huomioitava myös mahdollisuus luottamusverkkojen yleistymiseen eli siihen, että voidaan luottaa toisen osapuolen esim. kumppanin tekemään tunnistukseen (federointi).

9 TUTKIMUKSEN KULKU TOIMINTATUTKIMUSMETELMÄN MUKAISESTI

9.1 Ongelman tunnistaminen ja määritteleminen

Tapiolan tarjoaman yritysasiakkaan verkkopalvelun nykyistä tunnistusmenetelmää ei enää kehitetä. Nykyisen tunnistuksen tilalle oli löydettävä korvaava ratkaisu. Ratkaisu päätettiin hakea tämän tutkimuksen kautta.

9.2 Toimintatutkimuksen syklit

Seuraavassa esitellään tässä tutkimuksessa toteutuneet vaiheet eli syklit.

9.2.1 Orientoiva vaihe (I-sykli)

Ensimmäisen syklin tavoitteena oli tehdä materiaalin keräyssuunnitelma, hankkia käyttöön kattava materiaali ja tutustua kirjallisuuteen. Tavoitteena oli myös kartoittaa Tapiolan tunnistusratkaisun nykytilanne. Sähköisestä tunnistamisesta löytyi materiaalia hyvin, joten lähdeluettelosta muodostui kohtuullisen laaja. Teoriatietoa oli haettavissa useasta eri lähteestä. Ensimmäinen huomio oli, että sähköistä tunnistamista käsittelevää yleislähdeteosta ei ole olemassa. Materiaaliin tutustuminen ja aihepiirin syvällinen tarkastelu selkeytti aihevalintaa. Tutkimus rajattiin keskittymään vahvaan sähköiseen tunnistamiseen. Orientoivan vaiheen aikana syntyi myös alustava tutkimusraportin runko ja sisällysluettelo. Orientoiva vaihe kesti vuoden 2008 toukokuusta saman vuoden elokuun loppuun asti.

9.2.2 Kirjallisuusselvitys (II-sykli)

Toisen vaiheen tavoitteena oli tehdä suunnittelutieteellinen kirjallisuustutkimus ja raportti vahvasta sähköisestä tunnistamisesta ja sen käyttömahdollisuuksista. Luettu materiaali ei vielä kaikilta osin ollut riittävä, joten lähdemateriaaliin hankkimista ja lukemista jatkettiin tässä vaiheessa. Verkkopalveluiden luokittelun ottaminen mukaan tutkimukseen (ks. luku 3) selkeytti tutkijaa jäsentämään vahvan sähköisen tunnistamisen tarpeellisuuden. Tapiolan projektityö eteni suunnitellusti. Kirjallisuuden ja kilpailija-analyysin perusteella selkeänä suositeltavana valintana uudeksi tunnistusmenetelmäksi oli Tupas-palvelu. Esille tuli kuitenkin epävarmuus Tupas-palvelusta ainoana toteutusvaihtoehtona. Kirjallisuusselvitysvaihe kesti vuoden 2008 syyskuusta saman vuoden lokakuun loppuun asti.

9.2.3 Syventävä vaihe (III-sykli)

Uutta tietoa tutkimuksessa olivat kansalliset vahvan sähköisen tunnistamisen suuntaviivat sekä lakiehdotus sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (ks. luku 7). Näiden tietojen valossa ajatus Tupas-palvelun

käyttöönotosta kyseenalaistui, koska ehdotetut kansalliset toimenpiteet olivat hyvin selkeitä ja voimakkaita. Tästä seurasi, että Tapiolassa tunnistusjärjestelmää ei kehitetä ainoastaan Tupas-palveluun perustuen, vaan tunnistamisjärjestelmässä on varattava myös mahdollisuus muunlaiseen tunnistamiseen tulevaisuudessa. Käytännössä tämä tarkoittaa, että tunnistamisjärjestelmässä on varauduttava esimerkiksi siihen, että sähköisenä tunnisteena toimiikin henkilötunnuksen sijaan jokin muu vastaava yksilöivä sähköinen tunniste. Toteutusajankohta oli vuoden 2008 marras- ja joulukuu.

9.2.4 Asiakasnäkökulmavaihe (IV-sykli)

Asiakasnäkökulma päätettiin varmistaa erillisellä sähköisellä asiakaskyselyllä, jotta voitiin olla varmoja, että ehdotettu ratkaisu on käyttäjien mielestä myös hyvä. Asiakaskyselyn tulokset vahvistivat Tupas-palvelun käyttöönoton. Tässä vaiheessa myös tutkimuksen ulkoasua ja kirjoitustyyliä hiottiin lopulliseen muotoonsa. Toteutusaikataulu oli vuoden 2009 tammi – helmikuu.

9.3 Vaihtoehtojen tarkastelu ongelman ratkaisuksi

Vahvoja sähköisiä tunnistamismenetelmiä on Suomessa yritysten tarjoamat omat käyttäjätunnukset, Tupas-palvelu, kansalaisvarmenne ja Katso-tunniste. Vahvimmaksi vaihtoehdoksi nousi Tupas-palvelu. Tupas-palvelun käyttöönottoon vaikuttaa myös suunniteltu käyttöönotto aikataulu case Tapiolassa, koska nykyinen ratkaisu halutaan korvata kohtuullisen nopeassa aikataulussa.

9.4 Yhden vaihtoehdon valinta ja toimeenpano

Tupas-palvelun käyttöönotto on ensisijainen vaihtoehto, jonka perustelut ovat luvussa 6.2.1. Tupas-palvelun vahvuus on se, että se on olemassa ja se voidaan ottaa käyttöön välittömästi (ks. luku 6.2). Tupas-palvelu vastaa nykyiseen tarpeeseen mutta se ei huomioi tulevaisuuden haasteita. Tunnistuspalvelua rakennettaessa on huomioitava ja varauduttava muihinkin uusiin vahvan tunnistamisen mahdollisuuksiin, kuten sähköiseen tunnisteeseen tai luottamusverkostoon. Asiakasnäkökulma tunnistus-palvelun kehittämiseen saatiin sähköisellä asiakaskaskyselyllä. Asiakaskyselytulos vahvisti ratkaisuehdotusta ottaa Tupas-palvelu käyttöön Tapiolassa.

9.4.1 Asiakaskysely Tupas-palvelusta

Epävarmuus yritysasiakkaiden suhtautumisesta Tupas-palvelun käyttöön ainoana tunnistusmenetelmänä yritysasiakkaan verkkopalvelussa nosti esiin tarpeen tehdä asiakaskysely. Asiakaskyselytutkimuksen tavoitteena oli selvittää, miten asiakkaat suhtautuvat Tupas-palveluun ja sen käyttämiseen. Aikaisempia tutkimuksia aiheesta ei ole käytettävissä, joten päädyttiin tekemään sähköinen kyselytutkimus.

Aihepiirin suppeuden vuoksi kyselylomake sisälsi vain muutamia Tupas-palveluun liittyviä kysymyksiä. Kyselyä laajennettiin käsittämään myös käyttäjähallintaa, mitä ei käsitellä tässä tutkimuksessa. Kysymykset olivat pääasiassa skaala- ja monivalintakysymyksiä. Skaaloihin perustuvissa kysymyksissä oli vaihtoehto ’En osaa sanoa’, jotta kyselytutkimuksen tulos ei vääristyisi. Kyselylomake testattiin henkilökunnasta valitulla pilottiryhmällä ja kysymyksiä muutettiin saadun palautteen perusteella.

Kysely suoritettiin Internet-kyselynä eli sähköisesti Digium Enterprise-ohjelmalla, jota Tapiola käyttää tutkimuksissaan. Digium Enterprise–ohjelma on yritysten organisaatioiden palautteenhallintaan ja tiedonkeruuseen tarkoitettu Internet-pohjainen ohjelmistopalvelu. Internet-kyselyssä vastaukset siirtyvät suoraan vastaajilta tilasto-ohjelmaan käsiteltäviksi, mikä helpottaa tiedon käsittelyä ja analysointia. Ohjelman avulla saadaan myös erilaisia raportteja.

Asiakaskyselyn tavoitteena oli selvittää asiakkaiden mielipide Tupas-palvelusta. Asiakaskyselylomake sisälsi taustakysymysten lisäksi seitsemän varsinaista Tupas-palveluun ja käyttöoikeushallintaa liittyvää kysymystä (ks. liite 1). Kyselyn kohderyhmäksi valittiin yritysasiakkaan verkkopalvelun pääkäyttäjiä. Tutkimusryhmän koko oli 5 500 pääkäyttäjää, jotka edustavat yritysasiakkaan verkkopalvelun vakuutusasioinnin käyttäjiä hyvin. Pääkäyttäjille lähetettiin 9.2.2009 sähköpostiviesti, joka sisälsi ohjeet tutkimuskyselyn täyttämisestä sekä tiedon, miten tietoja tullaan käsittelemään (ks. liite 2). Lisäksi sähköpostiviestissä oli linkki tutkimuskyselyyn ja arvio, kauanko tutkimuskyselyn täyttäminen kestää. Kyselyssä vastaajille kerrottiin ensin, mikä on Tupas-palvelu, minkä jälkeen kysyttiin Tupas-palvelun käytön luotettavuudesta ja vaivattomuudesta sekä halukkuudesta käyttää Tupas-palvelua tunnistautumiseen erilaisissa yrityksille suunnatuissa verkkopalveluissa. Vastaajilta kysyttiin myös taustatietoja, kuten sukupuoli, ikä, yrityksen henkilöstömäärä.

Vastausaikaa annettiin 10 arkipäivää, koska sähköiseen kyselyyn vastataan useimmiten heti. Vastauksia saatiin 1 192 kpl määräaikaan mennessä. Vastausprosentti oli 21,6 %.

Vastaajille esitettiin väite, jonka mukaan pankkien tarjoama Tupas-tunniste on luotettava ja turvallinen. Vastaajista 48 % oli täysin samaa mieltä, 35 % osittain samaa mieltä ja 2 % eri mieltä. Täysin eri mieltä ei ollut juuri kukaan (0,02 %). Vastanneista 15 % vastasi vaihtoehdon ”En osaa sanoa”.

Toisena väitteenä esitettiin, että Tupas-tunnusten käyttö verkkoasioinnissa on vaivatonta ja helppoa. Vastanneista 43 % oli täysin samaa mieltä. Osittain samaa mieltä oli 36 %, kun taas osittain eri mieltä oli 8 % ja täysin erimieltä 2 %. Vastanneista 12 % ei osannut sanoa.

Kolmannessa kohdassa vastaajia pyydettiin valitsemaan ne palvelut, joiden käytössä Tupas-tunnisteiden käyttö helpottaisi työtehtävien hoitoa. Vastaajista 68 %:n mukaan työtehtävien hoidossa auttaisi, jos Tupas-tunneista voisi käyttää Verohallinnon, Kelan, Vakuutusyhtiön, Rahastopalvelun ja Viranomaispalvelujen verkkopalveluissa, kun taas 9 % vastasi, että Tupas-tunniste ei auttaisi työtehtävien hoidossa edellä mainituissa palveluntarjoajien verkkopalveluissa. Vastanneista 24 % ei osannut ottaa kantaa. Tarkasteltaessa vakuutusyhtiön vastauksia tarkemmin, niin 81 % oli sitä mieltä, että työtehtävien hoidossa auttaisi Tupas-tunnisteiden käyttö, kun taas 5 % vastasi, että Tupas-tunniste ei auttaisi. Vastanneista 14 % valitsi vaihtoehdon ”ei osaa sanoa” (ks. kuvio 8).

Työtehtävien hoidossa auttaisi, jos voisin käyttää Tupas-tunnisteita seuraavissa palveluissa:

	Kyllä (Arvo: 2)	Ei (Arvo: 1)	En osaa sanoa (Arvo: 0)	Yhteensä
Verohallinto (avg: 1,89)				100 %
Kela (avg: 1,87)				100 %
Vakuutusyhtiö (avg: 1,94)				100 %
Rahastopalvelu (avg: 1,78)				100 %
Viranomaisten palvelut (avg: 1,89)				100 %
Yhteensä	68 %	9 %	24 %	

Kuvio 8. Tupas-tunnisteiden käyttöhalukkuus verkkopalveluissa

Niille vastaajille, jotka vastasivat edelliseen kysymykseen vakuutusyhtiöiden kohdalle, ei tai en osaa sanoa, esitettiin seuraava lisäkysymys: Miksi et käyttäisi Tupas-tunnisteita työasioiden hoitamisessa?

Suurimaksi syyksi Tupas-tunnisteiden käyttämättä jättämiseen työasioiden hoitamisessa oli se, että vastaajat eivät halua käyttää omia tunnuksia työtehtävien hoitamisessa. Tätä mieltä oli 55 % vastaajista, kun taas 24 % vastaajista oli sitä mieltä, että työnantajan pitää antaa työvälineet työtehtävien hoitamiseen. Vastaajista 21 % säilytti tunnuksia kotonaan ja noin 6 % pelkäsi tunnusten kuluvan loppuun liian pian. Vastaajista 32 % ilmoitti syyksi jonkun muun syyn, joita oli 65 erilaista. Näitä muita syitä oli muun muassa se, ettei Tupas-tunniste ollut tuttu entuudestaan (23 vastaaja). Neljä vastaajaa ilmoitti käyttävänsä jo jotain muita tunnuksia, kuten Katso-tunnistetta. Edelleen erilaisia muita syitä olivat muun muassa se, että tilitoimisto hoitaa asiat ja käyttö on hankalaa ja hidasta.

Miksi et käyttäisi Tupas-tunnisteita työasioiden hoitamisessa? Voit valita useamman kuin yhden vaihtoehdon.

	Vastaus	Lukumäärä	Prosentti	20%	40%	60%	80%	100%
1.	Työnantajan pitää antaa työvälineet työtehtävien hoitamiseen.	50	24,39%					
2.	En halua käyttää omia tunnuksia työtehtävien hoitamisessa.	112	54,63%					
3.	Pelkään, että verkkopankkitunnukset kuluvat liian pian loppuun.	14	6,83%					
4.	Säilytän tunnuksia kotona.	42	20,49%					
5.	Jokin muu syy, mikä?	65	31,71%					
	Yhteensä							

Kuvio 9. Miksi käyttäjä ei käyttäisi Tupas-tunnisteita työasioiden hoitamiseen vakuutusyhtiön verkkopalvelussa

Tutkimukseen vastanneista pääkäyttäjistä naisia oli 62 % ja miehiä 28 %. Vastanneiden ikäjakauma on esitetty kuviossa 10.

Ikä

	Vastaus	Lukumäärä	Prosentti	20%	40%	60%	80%	100%
1.	< 25 vuotta	10	0,84%					
2.	26 - 34 vuotta	106	8,89%					
3.	35 - 44 vuotta	261	21,90%					
4.	45 - 50 vuotta	256	21,48%					
5.	50 < vuotta	559	46,90%					
	Yhteensä	**1192**	**100%**					

Kuvio 10. Vastaajien ikäjakauma

Vastanneista 26 % ilmoitti, että yrityksen päätoimipaikka oli pääkaupunkiseudulla. Päätoimipaikoista 17 % sijaitsi Etelä-Suomen läänissä, 32 % Länsi-Suomessa, 14 % Itä-Suomessa, 9 % Oulun läänissä ja 4 % Lapin läänissä. Ahvenanmaalla ei ollut yhtään päätoimipaikkaa. Yritysten henkilöstömäärän jakauma on esitetty kuviossa 11.

Yrityksen henkilöstömäärä

	Vastaus	Lukumäärä	Prosentti	20%	40%	60%	80%	100%
1.	1 - 9 henkilöä	724	60,74%					
2.	10 - 49 henkilöä	328	27,52%					
3.	50 - 99 henkilöä	67	5,62%					
4.	100 - 249 henkilöä	36	3,02%					
5.	yli 250 henkilöä	37	3,10%					
	Yhteensä	**1192**	**100%**					

Kuvio 11. Kyselyyn vastanneiden henkilöiden sijoittuminen erikokoisiin yrityksiin

Asiakaskyselyn tulos poisti epävarmuuden Tupas-palvelun käyttöönotosta Tapiolassa. Valtaosa vastaajista koki, että Tupas-tunnisteiden käyttö vakuutusyhtiön palvelujen käytössä helpottaisi työtehtävien hoitamista.

9.5 Toimenpiteiden seurausten tutkiminen

Valitun tunnistusmenetelmän käyttöönottoon ja sen jälkeiseen palvelutilanteeseen Tapiolan verkkopalveluissa liittyvä seuranta ei enää sisälly tämän tutkimuksen piiriin.

9.6 Oppiminen ja yleisten löydösten tunnistaminen

Internetistä, vahvasta sähköisestä tunnistamisesta ja verkkopalvelusta käytetään hyvin erilaisia termejä. Yleistä alan yhtenäistä käsitteistöä ei ole vielä muodostunut.

Käsitteistö helpottaisi asioiden kehittämistä, kun olisi varmuus siitä, että kaikki tarkoittavat termeillä samoja asioita.

Tunnistusmalli, jossa huomioidaan, että käyttäjä voi tunnistaa palveluun useammalla eri tavalla, kuten esimerkiksi Tupas-palvelun, sähköisen tunnisteen (HST) tai sormenjäljen avulla, on välttämätöntä. Tällaista tunnistusmallia voitaisiin kutsua monitunnistusmalliksi. Malli sisältää vähintään yhden tunnistusmenetelmän ja lisäksi se sisältää vähintään valmiuden useamman menetelmän käyttöönottoon. Suomen kansalliset linjaukset ja lakiesitykset voivat vaikuttaa nopeastikin uusien vahvojen sähköisten tunnisteiden syntymiseen ja käyttöönottoon, jotka sitten voitaisiin sisällyttää tähän uuteen malliin.

Monitunnistusmalli soveltuu kaikkiin Suomessa tarjottaviin vahvan sähköisen tunnistamisen vaativiin palveluihin. Monitunnistusmallissa käyttäjä tunnistetaan, jonka jälkeen käyttäjä siirtyy ko. palvelun käyttöoikeushallintaa, jossa käyttäjälle annetaan käyttäjälle kuuluvat käyttövaltuudet. Käyttöoikeushallinta on rajattu tämän tutkimuksen ulkopuolelle. Monitunnistusmalli toimii vastaavasti myös Suomen ulkopuolella esimerkiksi EU-alueella.

9.7 Oppiminen

Toimintatutkimus soveltuu hyvin tällaisten tutkimusten tutkimusmenetelmäksi. Hyvin suunnitellut ja tavoitteelliset syklit varmistavat tutkimuksen etenemisen suunnitellusti. Reflektointi syklin päättyessä antaa mahdollisuuden korjata tutkimuksen suuntaa tai lisätä siihen oleellista tietoa, kuten tässä tutkimuksessa tehtiin ottamalla tutkimukseen mukaan myös asiakasnäkökulma. Toimintatutkimus soveltuu hyvin myös liiketoiminnan eri kehitystehtävien suunnitteluun ja toteutukseen.

10 JOHTOPÄÄTÖKSET

Yritysten tarjoamat ekstranet-palvelut käsittävät sellaisia palvelukokonaisuuksia, jotka sisältävät yksityiskohtaista tietoa asiakkaasta ja asiakassuhteesta. Verkkopalveluiden käyttö edellyttää, että asiakas luottaa siihen, että käyttö on turvallista ja luotettavaa. Luotettavuus ja turvallisuus puolestaan taataan sillä, että käyttäjä tunnistetaan mahdollisimman luotettavalla tavalla. Niin sanotussa vahvassa tunnistamisessa

käytetään vähintään kahta todentamismenetelmää yhtä aikaa. Esimerkiksi verkkopankkitunnuksiin ja vaihtuviin salasanalistoihin perustuva Tupas-tunnistus on tällainen menetelmä. Henkilön vahva sähköinen tunnistaminen on tarpeen silloin, kun palveluntarjoajan verkkopalvelu on tarkoitettu luottamukselliseen vuorovaikutteiseen asiointiin ja se sisältää asiakkaan luottamuksellisia henkilökohtaisia tietoja.

Yritysten liiketoiminnallisena tavoitteena on, että henkilö- ja yritysasiakkaat yhä enenemissä määrin hoitaisivat itse rutiiniasiat verkkopalveluissa. Ekstranet- palvelut ovat laajoja palvelukokonaisuuksia, joissa asiakas näkee omia tai yrityksen tietoja ja voi muuttaa sekä ylläpitää niitä. Koska Ekstranet- palvelut sisältävät asiakkuuteen liittyviä tietoja, niihin pitää liittää vahva sähköinen tunnistaminen. Vahvoja sähköisiä tunnistamismenetelmiä on Suomessa useita, kuten kansalaisvarmenne, Tupas-palvelu, Katso-organisaatiotunniste, mutta esimerkiksi kansalaisvarmennetta ei ole otettu käyttöön kuten alun perin suunniteltiin.

Toistaiseksi käyttökelpoisin henkilön vahva sähköinen tunnistamistapa on pankkien tarjoama Tupas-palvelu. Tupas-palvelu on otettu laajasti käyttöön. Käyttäjät tuntevat ja luottavat Tupas-palveluun. Käyttäjiltä kysyttiin asiakaskyselylle, että mitä mieltä he ovat Tupas-palvelun käyttöönotosta, kyselyn tulos vahvisti käsitystä siitä, että käyttäjät ovat valmiita ottamaan Tupas-palvelun käyttöön ekstranet-palveluissa. Tupas-palvelun käyttöönottoa on mietitty myös Tapiolassa. Tällä hetkellä vahvan sähköisen tunnistamisen yhtenäistämiselle onkin selkeä tarve ja tahtotila. Suomen kansalliset linjaukset sekä lakiesitykset edistävät tätä hanketta voimakkaasti. Tunnistuspalvelua uusittaessa on kuitenkin myös huomioitava tulevaisuuden mahdolliset muutokset vahvan sähköisen tunnistamisen alueella. Vahva sähköinen tunnistaminen nojautuu tällä hetkellä voimakkaasti henkilötunnukseen, mutta lähitulevaisuudessa henkilötunnuksen saattaa korvata jokin muu sähköinen tunniste. Tällaista tunnistusmallia voitaisiin kutsua monitunnistusmalliksi. Malli sisältää vähintään yhden tunnistusmenetelmän ja lisäksi se sisältää vähintään valmiuden useamman menetelmän käyttöönottoon. Monitunnistusmalli voidaan ottaa käyttöön vahvan tunnistuksen vaativissa ekstranet-palveluissa. Monitunnistusmalli soveltuu käytettäväksi EU-maissa, koska tunnistustavoille haetaan muutenkin yhtenäisempää linjausta EU-maissa. Jatkotutkimuksen aiheena voisi olla monitunnistusmallin tekninen mallintaminen ja sen käyttöönotto.

Toinen jatkotutkimuksen kohde olisi käsitteistön luominen. Internetistä, vahvasta sähköisestä tunnistamisesta ja verkkopalvelusta käytetään hyvin erilaisia termejä. Yleistä alan yhtenäistä käsitteistöä ei ole vielä muodostunut. Käsitteistö helpottaisi asioiden kehittämistä, kun olisi varmuus siitä, että kaikki tarkoittavat termeillä samoja asioita.

Jatkossa verkkopalvelujen edelleen kehittyessä olisi mielenkiintoista selvittää, miten asiakkaiden verkkopalvelujen käyttö vaikuttaa verkkopalveluja tarjoavan organisaation työtehtäviin ja resursseihin. Toisaalta olisi mielenkiintoista selvittää, miten verkkopalvelujen käyttö vastaavasti vaikuttaa käyttäjäorganisaatioon.

LÄHTEET

Ahonen, A., 2007. From Complex to Simple : Designing a Customer-Friendly Electronic Insurance Servicescape. Tampereen yliopisto. Väitöskirja.

Arjentietoyhteiskunnan neuvottelukunta. 2008. Sähköisen tunnistamisen kehittämistyöryhmän 1. väliraportti arjen tietoyhteiskunnan neuvottelukunnalle Sähköisen tunnistamisen nykytila Suomessa 15.1.2008. www.arjentietoyhteiskunta.fi/files/36/Sahkoinen_tunnistamisen_ nykytila_lopullinen_080115.pdf. (Viitattu 7.8.2008).

Arjentietoyhteiskunnan neuvottelukunta. 2008. Sähköisen tunnistamisen suuntaviivoista yhteinen näkemys – monipuoliset tunnistamispalvelut tehostamaan sähköistä asiointia. http://lato.poutapilvi.fi/p4 arjenty/?38 m=262&s=109. (Viitattu 28.10.2008).

Carr, W & Kemmis, S. 1986. Becoming Critical. Education, Knowledge and Action Research. London: The Falmer Press.

Davison, R & Martinsons, M & Kock, N. 2004. Principles of canonical action research. Information Systems Journal (141) pp 65-86.

FiCom Tietoliikenteen ja tietotekniikan keskusliitto. 2008. Mobiili Asiointivarmenne 30.6.2008.

Finanssialan keskusliitto FK. 2007. Pankkien TUPAS-varmennepavelu palveluntarjoajille, Palvelun kuvaus ja palvelun tarjoajan ohje, versio 2.2. http://www.fkl.fi/asp/ida/download.asp?prm1=wwuser fklo&doci=1167&sec=&ext=.pdf. (Viitattu 15.9.2008).

Finanssialan keskusliitto FK. 2008. Pankkien Tupas-varmennepalvelun varmenneperiaatteet v1.0. http://www.fkl.fi/asp/ida/download.asp?prm1=wwuser fkl&docid=11266&sec=&ext=.pdf. (Viitattu 15.9.2008).

Fräntti, M. & Pirinen, R. 2005. Tutkiva oppinen integratiivisissa oppimisympäristöissä – Bar Laurea ja REDLabs.

Hevner, A. et al 2004. Design Science in Information Systems Research. MIS Quarterly Vol. 28 No. 1, pp. 75-105.

Julkisen tietohallintaneuvottelukunta JUHTA:n asettama projektiryhmä. 2007. Kuntien työntekijöiden tunnistaminen ja käyttövaltuuksien hallinta raportti. http://www.kunnat.net/attachment.asp?path=1;55264;122868;354;46247;116762;124212. (Viitattu 8.9.2008).

Järvinen, P. 2005. Action research as an approach in design science. Presented in the EURAM Conference, Munich, May 4 – 7, 2005 in track 28: Design, Collaboration and Relevance in Management Research.

Järvinen, P. 2008. Petteri Järvinen, Kansallinen muistitikku. Tietokone, kesä-heinäkuu 2008. http://www.tietokone.fi/uutta/uutinen.asp?news id=34295&tyyppi=1. (Viitattu 2.7.2008).

Järvinen, P. 2003. Salausmenetelmät. Suomi: Docendo Finland oy.

Järvinen, P. & Järvinen, A. 2004. Tutkimustyön metodeista. Tampere: Opinpajan kirja.

Järvinen, R., Eriksson, P., Saastamoinen, M. & Lystimäki, M. 2001. Vakuutukset verkossa: vakuutusyhtiöiden tarjonta ja kuluttajien odotukset. Helsinki: Kuluttajatutkimuskeskus.

Kalakota, R. & Robinson, M. 2001. e-Business 2.0: Roadmap for Success. US: Addison-Wesley.

Keskinäinen Eläkevakuutusyhtiö Ilmarinen. https://www.ilmarinen.fi/Production/fi/etusivu/index.jsp.

Kuusela, H. & Rintamäki, T. 2002. Arvoa tuottava asiointikokemus: hyödyt ja uhraukset henkilökohtaisen ja sähköisen asioinnin kehittämisessä. Tampere: Tampere University.

Lehtinen, J. 2008. Sähköinen tunnistusfloppi on käynyt kalliiksi. www.digitoday.fi/p/200811104. (Viitattu 8.8.2008).

Levi, A. & Ufuk Caglayan, M & Koc, C K. 2004. Use of Nested Certificates for Efficient, Dynamic, and Trust Preserving Public Key Infrastructure. ACM Transactions on Information and System Security, Vol. 7. 1, February 2004.

Liikenne- ja viestintäministeriö. 2008. Laki sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista. http://www.lvm.fi/web/fi/lakihanke/view/634204. (Viitattu 12.12.2008).

Linden, M. 2007. Julkisen avaimen järjestelmä, toimikortit ja niiden soveltaminen organisaatiossa. Tampereen teknillinen korkeakoulu, lisensiaattityö.

Linkola, P. & Riittinen-Saarnio, E. 1993. Vakuutuspalvelujen markkinointi. Helsinki: Suomen vakuutusalan koulutus ja kustannus.

Männikkö, P. 2008. Tietosuoja Tietotuvan ja tietosuojan erikoislehti. 4/2008. (Viitattu 20.1.2009).

Nikulainen, K. 2008. Sirullinen henkilökortti vain murto-osalla. Digitoday-lehti. www.digitoday.fi/p/200816355. (Viitattu 8.8.2008).

Pohjola vakuutus oy. www.pohjola.fi.

Rawles, PT. & Baker, KA. 2003. Developing a Public Key Infrastructure for Use in Teaching Laboratory. Lafayette, Indiana, USA. Copyright 2003 ACM-1-58113-770-2/03/00100.

Rinne, T. 2002. Älykortit – tekniikka, sovellusalueet ja käyttöönotto. Helsinki: Gummerrus kirjapaino.

Susman, G.I. & Evered, R.D. 1978. An assessment of the scientific merits of action research. Administrative Science Quarterly 23, 582–603.

Tardo, J.& Alagappan, K. 1991. SPX: Gobal Authentication Using Public Key Certificates. USA: Proseedings of the 1991 IEEE Symposium on Security and Privacy.

Tietoliikenteen ja tietotekniikan keskusliitto FiCom, 2008. Mobiili Asiointivarmenne 30.6.2008. (Tulostettu 15.10.2008).
Työeläke.fi –palvelu. http://www.tyoelake.fi/.

Vainio, M. 2008. Mobiilivarmenne tunnistus- ja allekirjoitusvälineenä B2C-Pro seminaari. http://b2cpro.vtt.fi/documents/seminar/b2c-pro-seminaari-vainio.pdf. (Tulostettu 30.6.2008).

Vahinkovakuutusyhtiö If. www.if.fi.

Valtiovarainministeriö Hallinnon Kehittämisosasto. 2006. Tunnistaminen julkishallinnon verkkopalveluissa. Helsinki: Edita Prima Oy.

Valtionvarainministeriö Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI. 2006. Tunnistaminen julkishallinnon verkkopalvelussa. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20061204Tunnis/Vahti_12_06.pdf. (Viitattu 15.9.2008).

Valtiovarainministeriö. 2008. Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/09_Tietoturvallisuus/01_tietoturvaryhma_VAHTI/index.jsp. (Luettu 30.12.2008).

Van Aken, J. 2005 Management Research as a Design Science - British Journal of Management, Vol. 16. 19–36.

Väestörekisterikeskus. 2008. Mikä on kansalaisvarmenne. http://www.vaestorekisterikeskus.fi/vrk/fineid/home.nsf/pages/4DC96862A6BFA292C2256FFF00379DE9. (Viitattu 7.8.2008).

Wilson, S. 2008. Public Key Superstructure ”It’s PKI Jim, But Not As We Know It!”. IDtrust 08 March 4 - 6 2008 Gaithersburg, MD. Copyright 2008 ACM 978-1-60558-066-1.

KUVIOT

LIITTEET

Liite 1 Asiakaskyselymalli

Kysely Tupas-tunnisteiden käytöstä

Kyselyyn vastaamisen menee aikaa alle 5 minuuttia.

Tupas on suomalaisten pankkien yhteinen varmennepalvelu, jonka avulla verkkopalvelujen käyttäjä tunnistetaan pankkien tarjoamilla verkkopankkitunnuksilla.

Tupas-varmennepalvelun käyttäminen tapahtuu pankin asiakkaalleen luomilla ja antamilla pankkikohtaisilla tunnisteilla, siis verkkopankkitunnuksilla, joilla hoidat omia pankkiasioita.

Pankkien tarjoama Tupas-tunniste on luotettava ja turvallinen.

Täysin samaa mieltä	Osittain samaa mieltä	Osittain eri mieltä	Täysin eri mieltä	En osaa sanoa
( )	( )	( )	( )	( )

Tupas-tunnusten käyttö verkkoasioinnissa on vaivatonta ja helppoa.

Täysin samaa mieltä	Osittain samaa mieltä	Osittain eri mieltä	Täysin eri mieltä	En osaa sanoa
( )	( )	( )	( )	( )

Työtehtävien hoidossa auttaisi, jos voisin käyttää Tupas-tunnisteita seuraavissa palveluissa:

	Kyllä	**Ei**	**En osaa sanoa**
Verohallinto	**( )**	**( )**	**( )**
Kela	**( )**	**( )**	**( )**
Vakuutusyhtiö	**( )**	**( )**	**( )**
Rahastopalvelu	**( )**	**( )**	**( )**
Viranomaisten palvelut	**( )**	**( )**	**( )**

Miksi et käyttäisi Tupas-tunnisteita työasioiden hoitamisessa? Voit valita useamman kuin yhden vaihtoehdon.

[ ] Työnantajan pitää antaa työvälineet työtehtävien hoitamiseen.
[ ] En halua käyttää omia tunnuksia työtehtävien hoitamisessa.
[ ] Pelkään, että verkkopankkitunnukset kuluvat liian pian loppuun.
[ ] Säilytän tunnuksia kotona.
[ ] Jokin muu syy, mikä? _____

Tupas-palvelun etuna on se, että useimmilla henkilöillä on jo valmiiksi verkkopalvelutunnukset. Siten uusi käyttäjä voisi ottaa Tapiolan verkkopalvelun käyttöönsä välittömästi, kun pääkäyttäjänä olisit antanut käyttöoikeudet palveluun.

Mitä hyötyjä koet saavasi siitä, että pääkäyttäjänä ylläpitäisit itse reaaliaikaisesti verkkopalvelun käyttöoikeuksia?

[ ] Uusien käyttäjien lisääminen palveluun olisi nopeampaa
[ ] Käyttäjien tietojen päivittäminen olisi helpompaa ja joustavampaa
[ ] Käyttäjärekisteri pysyisi aina ajan tasalla
[ ] Olisin aina perillä siitä, kenellä kaikilla on käyttöoikeus palveluun
[ ] Uusien käyttäjien salasanapakettien odotteluun ei kulu turhaa aikaa
[ ] Jokin muu, mikä? _____

Mitä seuraavista vaihtoehdoista kaipaat verkkopalvelun pääkäyttäjänä työsi tueksi? Voit valita useamman kuin yhden vaihtoehdon.

[ ] Ohjeistusta
[ ] Koulutusta
[ ] Puhelintukea
[ ] Jokin muu, mikä? _____

Nyt voit antaa vapaamuotoista palautetta tai kehitysehdotuksia Tapiolan verkkopalvelujen kehittämiseen.

_____
_____
_____
_____

Täytäthän vielä taustatiedot.

Sukupuoli

( ) Nainen
( ) Mies

Ikä

( ) < 25 vuotta
( ) 26 - 34 vuotta
( ) 35 - 44 vuotta
( ) 45 - 50 vuotta
( ) 50 < vuotta

Yrityksen päätoimipaikka

( ) Pääkaupunkiseutu
( ) Etelä-Suomen lääni
( ) Länsi-Suomen lääni
( ) Itä-Suomen lääni
( ) Oulun lääni

( ) Lapin lääni
( ) Ahvenanmaan lääni

Yrityksen henkilöstömäärä

( ) 1 - 9 henkilöä
( ) 10 - 49 henkilöä
( ) 50 - 99 henkilöä
( ) 100 - 249 henkilöä
( ) yli 250 henkilöä

Liite 2 Sähköposti saate-malli

Hei!

Sinut on yrityksenne verkkopalvelun pääkäyttäjänä valittu vastaajaksi tutkimukseen, jossa kartoitetaan Tapiolan tunnistusratkaisua.

Vastauksesi ovat meille tärkeitä, sillä tutkimustulosten perusteella kehitämme tunnistusratkaisua ja toimintaamme yritysasiakkaita paremmin palvelevaksi. Antamasi vastaukset kirjautuvat järjestelmään nimettöminä ja ne käsitellään ehdottoman luottamuksellisesti. Tulokset esitetään kokonaistuloksina, joten yksittäisen vastaajan tiedot eivät paljastu.

Toivomme, että Sinulla on mahdollisuus vastata viimeistään **20.2.2009**. Vastaamiseen kuluu aikaa alle 5 minuuttia.

Pääset vastaamaan kyselyyn suoraan alla olevasta linkistä tai kopioimalla osoitteen ja siirtämällä sen Internet-selaimen osoitekenttään. Huomaa, että kyselyyn voi vastata vain kerran, eli kun avaat kyselyn, älä sulje sitä ennen kuin olet vastannut.

Linkki kyselyyn:

https://digiumenterprise.com/answer/?sid=300451&chk=675NPNW3

Kiitämme etukäteen vastauksistasi. Mikäli haluat lisätietoja tutkimuksesta, voit ottaa yhteyttä Tapiolaan, yritystenverkkopalvelu@tapiola.fi.

Ystävällisin terveisin

Teija Mikkola
Kehityspäällikkö
Tapiola-ryhmä
Verkkoliiketoimintayksikkö

Osoitelähde: Tapiola-ryhmän asiakasrekisteri, 02010 TAPIOLA