LAUREA
AMMATTIKORKEAKOULU
Uuden edellä

# Riskit Suomen passin myöntämiseen liittyvässä sähköisessä asioinnissa

Lindfors, Sini

2014 Leppävaara

**Laurea-ammattikorkeakoulu**
Leppävaara

# Riskit Suomen passin myöntämiseen liittyvässä sähköisessä asioinnissa

Lindfors Sini
Turvallisuusosaamisen YAMK
Opinnäytetyö
Toukokuu, 2014

**Laurea-ammattikorkeakoulu** **Tiivistelmä**
Leppävaara
Turvallisuusosaamisen koulutusohjelma (YAMK)

Lindfors Sini

**Riskit Suomen passin myöntämiseen liittyvässä sähköisessä asioinnissa**

Vuosi 2014 Sivumäärä 58

Suomen kansalaisella ja maassa laillisesti oleskelevalla ulkomaalaisella on vapaus liikkua maassa ja valita asuinpaikkansa, ja jokaisella on oikeus lähteä maasta. Matkustusoikeuden osoittamiseksi Suomen kansalaiselle myönnetään hakemuksesta passi, ja Suomessa passin myöntää poliisi. Kehitteillä olevan poliisin sähköisen asioinnin on tarkoitus helpottaa Suomen passin myöntämistä niin kansalaisten kuin poliisinkin näkökulmasta. Tavoitteena on mahdollistaa passihakemuksen jättäminen ja käsittelymaksun maksaminen sähköisesti sekä tietyin edellytyksin uuden passin myöntäminen ilman henkilökohtaista asiointia viranomaisen luona.

Tämän opinnäytetyön tavoitteena on tunnistaa ja arvioida Suomen passin myöntämiseen liittyviä riskejä sähköisessä asioinnissa erityisesti poliisin näkökulmasta, ja kuvata havaittujen riskien hallintakeinoja sekä rakentaa riskienhallintamalli, jota voidaan laajentaa koskemaan tämän työn ulkopuolelle rajattuja riskejä tai kaikkien poliisin hankkeiden riskienhallintaa. Aihe on ajankohtainen parhaillaan käynnissä olevan kehitystyön sekä toisaalta käynnissä olevan passilain muutosesityksen vuoksi.

Riskit Suomen passin myöntämiseen liittyvässä sähköisessä asioinnissa painottuvat tässä konstruktiivisessa tutkimuksessa eniten siihen, että väärä henkilö yrittää suorittaa oikeustoimia sähköisesti kokonaan tai osittain toisen henkilön tiedoilla vahingonteko- tai hyötymistarkoituksessa.

Asiasanat: poliisi, sähköinen asiointi, passi, riski

Laurea University of Applied Sciences
Leppävaara
Master's Degree Programme in Security Management

Abstract

Lindfors Sini

**Risks in issuing Finnish passports via e-services**

Year 2014 Pages 58

A Finnish citizen or a foreign national resident living in Finland legally have a right to move and choose their place of residence. Everyone has a fundamental right to leave the country. To prove the right to travel, the citizen must have a valid passport issued by the Finnish Police. Police is developing its e-services to ease applying and issuing of license services i.e. passport. The goal is to enable e-services for passport application and license fee. If certain criteria are filled, the objective is that police could grant a passport fully via e-services without the applicant visiting the authority in its premises.

The objective of this thesis is to recognize and evaluate the risks in issuing Finnish passports via e-services especially from police's point of view and to describe the ways to manage the recognized risks and to build a model for risk management. The built model can be expanded outside the risks of this thesis or all the project risks within the Finnish Police. The subject is very topical due the ongoing development and the current adjustments of the Passport Act.

The risks in issuing Finnish passports via e-services focuses on this constructive research mostly to the situation where a wrong person is trying to perform legal acts electrically with someone else's full or partially real personal data to achieve benefit or harm.

Keywords: police, e-services, passport, risk

Sisällys

# 1 Johdanto

Ihmisoikeuksiin kuuluva liikkumisvapaus on Suomen perustuslain (11.6.1999/731) 9 § nojalla turvattu, jolloin Suomen kansalaisella ja maassa laillisesti oleskelevalla ulkomaalaisella on vapaus liikkua maassa ja valita asuinpaikkansa, ja jokaisella on oikeus lähteä maasta. Matkustusoikeuden osoittamiseksi Suomen kansalaiselle myönnetään hakemuksesta passi, ja Suomessa passin myöntää poliisi. Nykymuodossaan passilain (21.7.2006/671) 6 § mukaisesti passihakemus on jätettävä henkilökohtaisesti poliisilaitokselle, tai ulkomailla oleskeleva Suomen kansalainen voi hakea passia Suomen ulkomaan edustustosta. Passilain mukaan passihakemusta jätettäessä hakija tunnistetaan henkilöllisyyttä osoittavan asiakirjan avulla tai hakemuksen vastaanottavan viranomainen toimesta. Voimassa olevassa passilaissa ei ole säännöksiä sähköisestä asioinnista tai passin hakemisesta, vaan hakijan täytyy asioida henkilökohtaisesti viranomaisen luona.

Kehitteillä olevan poliisin sähköisen asioinnin on tarkoitus helpottaa tilannetta niin kansalaisten kuin poliisinkin näkökulmasta. Poliisin myöntämien lupien määrä on kasvanut huomattavasti viime vuosina. Valtioneuvosto on 4.4.2012 tekemällään kehyspäätöksellä edellyttänyt poliisin kokonaisrahoituksen turvaamiseksi muun muassa poliisin lupahallinnon kehittämistä, ja kehittämistoimia on määritelty Poliisin lupahallintostrategiassa ja Poliisihallituksen asettamassa Lupa 2016 -hankkeessa. Lupahallintostrategian tavoitteena on, että lupa-asioissa voitaisiin asioida sähköisesti kaikilta niiltä osin kuin se olisi menettelyn turvallisuuden kannalta mahdollista. Henkilökohtaista asiointia edellytettäisiin ainoastaan välttämättömissä tilanteissa. Sähköisten palveluiden kehittämisen tavoitteena on asioinnin helpottuminen ja nopeutuminen, sekä lupahallinnon toimintaprosessien tehostaminen ja yhdenmukaistaminen. Toiminnan kehittäminen liittyy suoraan myös poliittisiin tavoitteisiin, sillä sähköisen asioinnin ja palveluiden asiakaslähtöinen kehittäminen sisältyy myös pääministeri Kataisen hallituksen hallitusohjelmaan. Parhaillaan sisäministeriössä valmisteilla olevan passilain muutosesityksen tavoitteena on valmistella sähköisen asioinnin edellyttämät muutokset passilakiin ja tarvittaessa passeista annettuun valtioneuvoston asetukseen (373/2013). Tavoitteena on mahdollistaa passihakemuksen jättäminen ja käsittelymaksun maksaminen sähköisesti sekä tietyin edellytyksin uuden passin myöntäminen ilman henkilökohtaista asiointia viranomaisen luona. (Sähköinen asiointi passimenettelyssä, 2013.)

# 2 Tavoite ja rajaukset

Tämän opinnäytetyön tavoitteena on tunnistaa Suomen passin myöntämiseen liittyviä riskejä sähköisessä asioinnissa ja rakentaa havaituista riskeistä riskienhallintamalli. Aihe on erittäin ajankohtainen erityisesti parhaillaan käynnissä olevan kehitystyön sekä käynnissä olevan passilain muutosesityksen vuoksi. Tarve riskien kartoittamiselle on tullut työni kautta, koska

työskentelen Poliisihallituksen Lupa 2016-hankkessa, jossa yhtenä keskeisenä tehtävänä on suunnitella ja toteuttaa lupahallinnon sähköistä asiointia vaiheittain. Olen myös toiminut sisäministeriön henkilöllisyyden luomista selvittävän hankkeen teknisenä sihteerinä hankkeen toimikauden ajan vuosina 2008–2010.

Tässä konstruktiivisessa tutkimuksessa kartoitetaan mitä riskejä Suomen passin myöntämiseen liittyvässä sähköisessä asioinnissa on erityisesti poliisin näkökulmasta. Riskien kartoittamisessa on haastateltu mm. poliisihallinnon virkamiehiä. Havaittujen riskien pohjalta olen laatinut riskienhallinnan toimintamallin. Työn lopuksi tuon esiin alustavia käytännön kokemuksia riskienhallinnan toimintamallista, sekä tutkimuksen johtopäätöksiä ja siihen liittyviä kehittämisehdotuksia.

Työssä on keskitytty poliisin myöntämistä luvista nimenomaan passiin sen myöntövolyymin ja ajankohtaisuuden vuoksi. Passi on suunnitelmien mukaisesti ensimmäinen lupa, jonka hakeminen voi tiettyjen kriteerien täytyttyä olla mahdollista kokonaan sähköisesti, vaikka hakeminen on aiemmin edellyttänyt henkilökohtaista asiointia poliisin luona. Tämä edellyttää lainmuutoksen voimaanastumista.

Riskit Suomen passin myöntämiseen liittyvässä sähköisessä asioinnissa painottuvat tässä tutkimuksessa eniten siihen, että väärä henkilö yrittää suorittaa oikeustoimia sähköisesti kokonaan tai osittain toisen henkilön tiedoilla vahingonteko- tai hyötymistarkoituksessa. Näiden riskien lisäksi sähköisessä asioinnissa on myös tietoteknisiä riskejä (kuten hakkerointi, ohjelmistovirheet), mutta ne on jätetty tarkastelun ulkopuolelle. Tietotekniset riskit on huomioitu sähköisen asioinnin teknisessä toteutuksessa joka on poliisin tietoturvalinjausten mukainen. Tietoturvallisuutta ylläpidetään mm. järjestelmäkehityksen ja tietoturva-auditointien myötä. Poliisitoiminnan muilla sektoreilla suunnitellaan myös sähköistä asiointia, mutta niihin liittyvien riskien kartoittaminen ja arviointi on rajattu tämän työn ulkopuolelle. Työstä on rajattu ulkopuolelle myös ulkomailla asuvien Suomen kansalaisten passin hakeminen, jossa toimivalta on ulkoasiainministeriöllä. Työstä on rajattu ulkopuolelle ne havaitut riskit, joiden esiin tuominen julkisessa opinnäytetyössä ei ole mahdollista salassapitovelvoitteiden vuoksi.

## 3 Kohdeorganisaatio

Suomen poliisin tehtävänä on oikeus- ja yhteiskuntajärjestyksen turvaaminen, yleisen järjestyksen ja turvallisuuden ylläpitäminen, sekä rikosten ennalta estäminen, selvittäminen ja syyteharkintaan saattaminen. Poliisihallinnossa työskentelee n. 11 000 henkilöä, joista poliisimiehiä on noin 7 700. (Poliisi Suomessa 2011.)

Valtioneuvosto ohjaa poliisitoimintaa mm. hallitusohjelmaan sisältyvien tavoitteiden ja valtioneuvoston hyväksymien periaatepäätösten avulla. Sisäministeriön tehtävänä on vastata poliisin toimialan ohjauksesta ja valvonnasta. Sisäministeriön alainen Poliisihallitus johtaa ja ohjaa operatiivista poliisitoimintaa. Suoraan Poliisihallituksen alaisuudessa toimivat poliisilaitokset ja poliisin valtakunnalliset yksiköt, joiden tulosohjauksesta Poliisihallitus vastaa. Poliisin valtakunnallisia yksiköitä ovat Keskusrikospoliisi (järjestäytyneen ja ammattimaisen rikollisuuden torjunta), Suojelupoliisi (valtion sisäinen ja ulkoinen turvallisuus) ja Poliisiammattikorkeakoulu (poliisikoulutus sekä poliisialan tutkimus- ja kehittämistoiminta). Paikallispoliisi koostuu 11 poliisilaitoksesta. Paikallispoliisin palveluverkkona toimivat pääpoliisiasema, poliisiasemat, poliisin palvelupisteet sekä yhteispalvelupisteet. Poliisin lupapalveluiden tehtävänä on tukea yleisen järjestyksen ja turvallisuuden ylläpitämistä, rikosten ennalta estämistä ja liikenneturvallisuuden edistämistä. (Poliisin organisaatio 2014.)

Poliisi myöntää vuosittain noin 1,3 miljoonaa lupaa (määrä päivitetty vuoden 2013 toteumatiedolla), joista passit, ajokortit, aseluvat ja henkilökortit ovat yleisimpiä poliisin myöntämiä lupia. Paikallispoliisin tehtävänä on ylläpitää yleistä järjestystä ja turvallisuutta, estää rikoksia ennalta, tutkia rikoksia ja muita yleistä järjestystä tai turvallisuutta vaarantavia tapahtumia, ohjata ja valvoa liikennettä sekä edistää liikenneturvallisuutta. Paikallispoliisi vastaa myös toimialueensa asukkaiden lupapalveluista. (Poliisi Suomessa 2011.)

Viimeaikaisella poliisin hallintorakenteen kehittämisellä on tavoiteltu poliisin toiminnan tehokkuuden lisäämistä vähenevien voimavarojen tilanteessa siten, että poliisi kykenee turvaamaan parhaalla mahdollisella tavalla sisäisen turvallisuuden säilymisen hyvällä tasolla (Poliisin hallintorakenneuudistus Pora III - päälinjaukset 2012, 1).

## 3.1 Poliisin lupahallinnon sähköinen asiointi

Lupahallinnon kokonaiskehittämiseen tähtäävän Lupa 2016-hankkeen tavoitteena on panna täytäntöön lupahallintostrategiassa, sisäasiainhallinnon TTS-asiakirjassa, sisäasiainministeriön ja Poliisihallituksen välisessä tulossopimuksessa sekä lupahallinnon kehittämishankkeen loppuraportissa esitetyt poliisin lupahallinnon kehittämistoimet. Kehittämistoimiin kuuluvat keskeisesti sähköisen asioinnin kehittäminen (ml. ajanvaraus) ja käytön tehostaminen, keskittäminen, ulkoistaminen, sekä näiden kehittämistoimien vaikutusten hallinta. Kehittämistoimet toteutetaan yhdessä mm. Poliisihallituksen Sähkö-hankkeen kanssa, jonka tehtävänä on yhdistää poliisin erilaiset sähköiset palvelut yhdeksi kokonaisuudeksi sekä vastata sen teknisestä toteuttamisesta. Lupa 2016-hankkeen tehtävänä on suunnitella ja toteuttaa yhdessä Sähkö-hankkeen kanssa lupahallinnon sähköistä asiointia vaiheittain. (Lupa 2016-hankkeen asettaminen, 2012.)

Vuosi 2014 on poliisin lupahallinnon sähköisen asioinnin käyttöönottovuosi. Tavoitteena on, että suuri osa poliisin myöntämistä luvista on vuoden lopussa sähköisen asioinnin piirissä. Keväällä 2014 käyttöön otettu uudistettu ajanvarausjärjestelmä tulee olemaan osa kansalaisten käyttämää poliisin sähköistä asiointipalvelua. Ajanvaraus toimii sekä erillisenä palveluna että saumattomana osana lupien sähköisen asioinnin yhteydessä.

Tällä hetkellä Suomi.fi-portaalin kautta pystyy asioimaan joidenkin poliisin palveluiden osalta sähköisesti, eli asian voi laittaa tunnistautuneena vireille. Yksi käytetyimpiä palveluita on rikosilmoituksen tekeminen. Nykyinen sähköinen asiointi on toteutettu teknisesti siten, että portaalissa jätetyt tiedot siirtyvät tiettyyn määriteltyyn poliisin virkasähköpostiosoitteeseen, josta prosessi jatkuu manuaalisena. Tätä ei poliisin kehittämisen alla olevalla sähköisellä asioinnilla tarkoiteta. Tavoitteena on, että asiakas rekisteröityisi sähköisen asiointipalvelun käyttäjäksi, josta asiakas siirtyisi poliisin sähköiseen asiointipalveluun asioimaan. Asiointipalvelussa jätetty (lupa)hakemus tai ilmoitus siirtyisi lähtökohtaisesti suoraan ko. luvan käsittelyjärjestelmän työjonoon. Kaksisuuntainen asiointi, eli asian käsittelyn sähköinen jatkokäsittely, on mahdollista, kun asiakas rekisteröityy sähköiseen asiointipalveluun.

Poliisin sähköisten palvelujen kehittämisellä on myös muita välillisiä tarpeita, kuin ainoastaan suoraan kansalaisille suunnattu palvelun parantaminen. Valtiovarainministeriö asetti tammikuussa 2012 koko julkisen hallinnon kattavan asiakaspalvelun kehittämishankkeen eli Asiakaspalvelu 2014 -hankkeen. Työ perustui hallitusohjelmaan, jossa on määritelty, että kuntatasolle luodaan kattava yhteispalvelupisteiden verkko ja määritellään jokaisessa yhteispalvelupisteessä vähintään etäpalveluna saatavilla olevat valtion, kuntien ja eri viranomaisten palvelut (ns. yhden luukun periaate). Hankkeen loppuraportissa tuotiin esiin useita kehittämisehdotuksia, jonka johdosta päätettiin asettaa tavoitteeksi antaa eduskunnalle vuoden 2014 kevätistuntokaudella hallituksen esitys laiksi julkisen hallinnon yhteisestä asiakaspalvelusta. (Julkisen hallinnon yhteisen asiakaspalveluhankkeen asettamiskirje, 2013.)

Asiakaspalvelun kehittämishankkeen loppuraportin ehdotuksessa yhteisessä asiakaspalvelussa tarjottaviksi poliisin palveluiksi esitetään joko ns. peruspalveluvalikoiman tai laajan valikoiman mukaista palveluvalikoimaa. Peruspalveluvalikoima kattaisi sähköisesti tarjottavat palvelut (eli käytännössä asiakaspalvelu ja -tuki kansalaisen sähköiseen asiointiin) sekä yhteisessä asiakaspalvelussa palveluneuvojan antamana ja etäpalveluna tarjottavat yhteisen asiakaspalvelun palveluvalikoiman mukaiset palvelut. Myös poliisin nykyisin hoitamia löytötavarapalveluita saisi yhteisistä asiakaspalvelupisteistä. Poliisin asiakaspalvelujen laaja valikoima kattaisi edellä mainittujen palvelujen lisäksi poliisin lupapalvelut täysimääräisesti (ajanvarauksella) poliisin oman henkilöstön toimesta. Poliisihallitus jätti kuitenkin eriävän mielipiteensä hankkeen loppuraporttiin 31.5.2013 koskien pääasiassa palvelupisteverkoston laajuutta. Eriävässä mielipiteessä tuotiin esiin myös se, että esitetyistä ratkaisuista ei saisi koitua poliisille pääl-

lekkäisiä kustannuksia. (Julkisen hallinnon asiakaspalvelun kehittämishankkeen loppuraportti 2013, 62-63, 251-252.)

## 3.2 Passi ja sähköinen asiointi

Passi on volyymiltaan poliisin suurin myöntämä yksittäinen lupa lähes 700 000 myönnetyllä passilla vuosittain. Passin myöntäminen, sekä erityisesti siihen liittyvä henkilön tunnistaminen, on yksi poliisin lupahallinnon ydintehtävistä. Näistä syistä passin myöntöprosessia koskeva kehittäminen on ollut yksi tärkeimmistä myös sähköisen asioinnin suunnittelu- ja toteutusjärjestyksessä.

Sähköisen asioinnin käyttöönottojen ensimmäisessä vaiheessa keväällä 2014 otettiin käyttöön uusi ajanvarausjärjestelmä. Jos passilain muutos hyväksytään eduskunnassa suunnitellussa aikataulussa, siirrytään sähköistä asiointia koskevien käyttöönottojen toisessa vaiheessa passien kevennettyyn hakemusmenettelyyn. Kevennetyn hakemusmenettelyn tekninen valmius on suunniteltu syksylle 2014. Kevennetty hakemusmenettely on mahdollista, jos edellinen biometrinen passi on haettu normaalisti eikä hakijan nimi ole vaihtunut. Mikäli hakijalta ei täyty kriteerit kevennettyyn hakemusmenettelyyn, ohjaa asiointipalvelu jättämään hakemuksen perustietoineen sähköisesti, mutta hakemus täytyy viimeistellä käymällä poliisilaitoksella. Hakijan ei välttämättä tarvitse käydä asiointipisteessä lainkaan mikäli kevennetyn hakemismenettelyn kriteerit täyttyvät. Tällöin kansalainen voi hakea passin täysin sähköisesti. Siinä tapauksessa passisirulle talletetaan edellisellä passinhakukerralla otetut sormenjäljet, jotka saadaan passisormenjälkirekisteristä. Passin hakija hankkii uuden passikuvan (enintään 6 kk vanha) ja pyytää valokuvaajalta passikuvaansa koskevan kuvatunnuksen kuvan liittämistä varten. Tämä edellyttää sitä, että valokuvaaja on tallettanut kuvan poliisin lupahallinnon valokuvapalvelimelle. Hakemusta täyttäessä hakija syöttää valokuvaajalta saamansa kuvatunnuksen sähköisen asioinnin yhteydessä sille varattuun kenttään, sekä maksaa hakemuksen. Mikäli hakijalla on passikuva paperiversiona, joutuu hän toimittamaan passikuvan poliisilaitokselle hakemuksen viimeistelyä varten. Passille tuleva nimikirjoitusnäyte on sama kuin edellisen passin hakemisen yhteydessä jätetty nimikirjoitusnäyte.

Passin toimitustavan muutos astui voimaan keväällä 2013. Valmista passia ei tarvitse noutaa enää poliisilaitokselta, vaan passin valmistaja toimittaa sen passinhakijan ilmoittamaa toimitusosoitetta lähellä olevalle R-kioskille. Kehitteillä on, että kesäkuusta 2014 alkaen asiakas saa itse valita noutopaikaksi haluamansa R-kioskin. Noutopaikan voi valita jo hakemuksen jättövaiheessa poliisin sähköisessä asiointipalvelussa. Passin noutajan on todistettava henkilöllisyytensä ja ilmoitettava saapumisilmoituksessa mainittu lähetystunnus. Valtaosa saapumisilmoituksista toimitetaan tekstiviestillä asiakkaan hakuvaiheessa ilmoittamaan puhelinnumeroon.

Merkittävää passin myöntämiseen liittyvän sähköisen asioinnin kohdalla on, että poliisi on luomassa ensimmäistä kokonaan sähköistä prosessia, jossa asiakkaalle luovutetaan hänen perusoikeuksiinsa voimakkaasti liittyvä lupa. Tätä lupaa käytetään matkustamisen lisäksi usein tunnistamisen pohjalla kun henkilö suorittaa esimerkiksi erilaisia oikeustoimia.

# 4 Aihepiirin teoria

## 4.1 Riskienhallinta

### 4.1.1 Riskienhallinnan keskeiset käsitteet

Riskin määritelmät vaihtelevat. Työterveyslaitos (2014) määrittelee riskin tarkoittavan haitallisen tapahtuman todennäköisyyttä ja vakavuutta. Valtionhallinnon tietoturvasanasto määrittelee sanan riski (VAHTI 8 2008, 80) seuraavasti:

- todennäköisyys, että uhka toteutuu aiheuttaen tietyn menetyksen tai vahingon
- uhkaan liittyvän vahingon rahallinen arvo tai odotusarvo (= arvo x todennäköisyys).

Hopkin (2010, 11) toteaa, että negatiivisesta olettamastaan huolimatta riskinotto voi johtaa myös positiiviseen lopputulokseen, mutta tätä käytetään yleisemmin liike-elämän puolella.

Tässä työssä riskillä tarkoitetaan poliisin riskienhallintapolitiikan (2013) mukaista määritelmää: riski on haitallisen tapahtuman todennäköisyys ja vakavuus, tai epävarmuutta tapahtumasta, jolla voi olla vaikutusta organisaation tai sen osan tavoitteiden saavuttamiseen.

Riskienhallintaprosessi sisältää Hopkinin (2010, 39) mukaan:

- riskien tunnistamisen
- riskien arvottamisen (toteutumisen todennäköisyys ja vaikutukset)
- merkittävimpien riskien hallintakeinoista päättämisen
- riskienhallintakeinojen resursoinnin
- poikkeustilanteiden hallinnan suunnittelun ja toiminnan jatkuvuuden suunnittelun
- raportoinnin ja valvonnan sekä
- riskienhallintajärjestelmän arvioinnin.

Poliisin riskienhallintapolitiikan (2013) mukaan riskienhallinnan käsitteet määritellään seuraavasti:

| Termi | Määritelmä |
|---|---|
| Tavoite | Organisaation toiminnan odotetut myönteiset tulokset ja vaikutukset. |
| Uhka | Tekijä, tapahtuma tai olosuhde, joka voi |

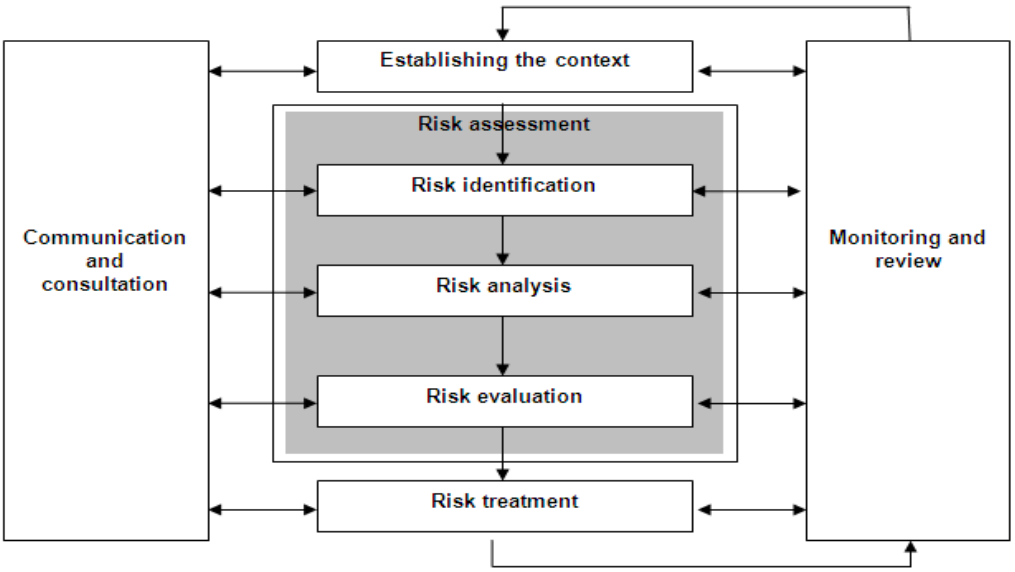
| | |
|---|---|
| | saada aikaan haitallisen tapahtuman. |
| Haavoittuvuus | Heikkous, joka mahdollistaa uhan toteutumisen. |
| Riski | Haitallisen tapahtuman todennäköisyys ja vakavuus. Epävarmuutta tapahtumasta, jolla voi olla vaikutusta organisaation tai sen osan tavoitteiden saavuttamiseen. |
| Bruttoriski | Riski ennen riskienhallinnan toimenpiteitä. |
| Jäännösriski | Riskienhallinnan toimenpiteiden jälkeen jäljelle jäävä riski. |
| Riskienhallinta | Prosessi, jolla pyritään tunnistamaan ja torjumaan tavoitteiden saavuttamista vaarantavia uhkia sekä hallitsemaan avautuneiden mahdollisuuksien menettämistä. Koostuu riskien tunnistamisesta, arvioinnista, riskeihin vastaamisesta sekä seurannasta ja valvonnasta. |
| Riskienhallintaprosessi | Riskienhallintaan liittyvien toimenpiteiden systemaattinen kokonaisuus. |
| Kokonaisvaltainen riskienhallinta | Riskienhallinnan kytkeminen organisaation strategisiin, toiminnallisiin ja taloudellisiin tavoitteisiin. |
| Riskeihin vastaaminen | Organisaation johto päättää, kuinka riskeihin vastataan. Riskit vältetään, hyväksytään (kannetaan), siirretään tai niitä pienennetään. Johto päättää keinoista riskien sopeuttamiseksi organisaation riskienkantokykyyn ja riskienottohalukkuuteen. |
| Riskin hyväksyminen (kantaminen) | Riskin pitäminen omalla vastuulla hyväksymällä siihen liittyvät mahdolliset hyödyt ja haitat. |
| Riskin pienentäminen | Toimenpiteet, joilla vähennetään riskin todennäköisyyttä ja/tai vaikutusta. |
| Riskin siirtäminen | Riskin siirtäminen kokonaan tai osittain toisen kannettavaksi esim. sopimuksellisin keinoin (myös riskin jakaminen). |
| Riskin välttäminen | Päätös olla osallistumatta tilanteeseen, johon liittyy riski. |
| Riskien arviointi | Riskien toteutumisen todennäköisyyden ja toteutumisen vaikutuksen arviointi. Riskit arvioidaan bruttoriskeinä ja jäännösriskeinä. |
| Riskienhallintapolitiikka | Organisaation riskienhallinnan tavoitteita, periaatteita, toimintatapoja, vastuita ja rooleja määrittelevä dokumentti. |

### 4.1.2 Riskienhallintamalli

#### 4.1.2.1 ISO 31000

Riskienhallinnan mallintamiseen on olemassa useita standardeja, joista yksi tunnetuimmista on ISO 31000, jonka tarkoituksena on auttaa kaiken kokoisia organisaatioita kehittämään riskienhallintansa nykyvaatimuksia vastaten sekä luomaan tavan tunnistaa, hallita ja ottaa tietoisia riskejä liiketoiminnan tavoitteisiin pääsemiseksi (Suomen Standardoimisliitto SFS ry 2014).

Hopkin (2010, 61) kuvaa ISO 31000-standardin mukaisessa riskienhallintaprosessissa riskin arvioinnin osiksi riskin tunnistamisen, riskin analysoinnin sekä riskin vaikuttavuuden evaluoinnin. Prosessi on iteratiivinen, jossa viestinnällä ja konsultaatiolla, sekä tarkkailulla ja arvioinnilla on tärkeä merkitys. Esimerkiksi tässä tapauksessa prosesseja tuntematta riskejä olisi vaikeampi löytää.




Kuva 1: Risk management process from ISO 31000. (Hopkin 2010, 61).

#### 4.1.2.2 COSO ERM

Yleinen riskienhallintaan käytetty malli on Committee of Sponsoring Organizations of the Treadway Commissionin (COSO) vuonna 2004 julkaisema kokonaisvaltaisen riskienhallinnan standardi. Standardin myötä saatiin yhtenäinen määritelmä riskienhallinnalle sekä kuvattua sen käyttö koko organisaation kattavana, yhteisenä toimintona. COSO ERM (Enterprise Risk Management) on ollut julkaisustaan lähtien yksi tunnetuimmista riskienhallintastandardeista.

COSO ERM:n mukaan kokonaisvaltaisen riskienhallinta tarkoittaa:
"Organisaation riskienhallinta on sen hallituksen, johdon ja muun henkilökunnan toteuttama prosessi, jota sovelletaan strategian laadinnassa ja koko organisaatiossa. Tarkoituksena sillä on tunnistaa organisaatioon vaikuttavia potentiaalisia tapahtumia ja pitää riskit riskinottohalukkuuden rajoissa, jotta voidaan olla kohtuullisen varmoja organisaation tavoitteiden toteutumisesta" (COSO 2004, 4).

COSO:n määritelmän (2004, 4) mukaisesti:

- Riskienhallinta on koko organisaation kattava jatkuva prosessi
- Riskienhallintaa toteutetaan organisaation kaikilla tasoilla
- Riskienhallintaa sovelletaan strategian laadinnassa
- Riskienhallintaa sovelletaan koko organisaatiossa, kaikilla tasoilla ja kaikissa yksiköissä ja siinä organisaatiota tarkastellaan kokonaisuutena
- Riskienhallinnan tarkoituksena on tunnistaa potentiaalisia tapahtumia, jotka toteutuessaan vaikuttavat organisaatioon, ja hallita riskiä organisaation riskinottohalukkuuden mukaisesti
- Riskienhallinnan avulla johto ja hallitus voivat saavuttaa kohtuullisen varmuuden organisaation tavoitteiden toteutumisesta
- Riskienhallinta on kehitetty toteuttamaan tavoitteita, jotka on ryhmitelty erillisiin, mutta osittain päällekkäisiin luokkiin.


Kuva 2: COSO ERM viitekehys. (COSO 2004, 6.)

COSO ERM määrittelee riskienarviointiprosessin kokonaisvaltaiseksi riskienhallinnaksi. COSO ERM - kuutiossa neljä pystysuoraa pylvästä esittävät yrityksen tavoitteita joita ovat strategia, toiminta, raportointi ja vaatimustenmukaisuus. Kahdeksan vaakariviä kuvaa johtamisjärjes-

telmän riskikomponentteja. Kuution kolmantena ulottuvuutena ovat organisaation yksiköt, joiden läpi kokonaisvaltaista riskienhallintaa toteutetaan.

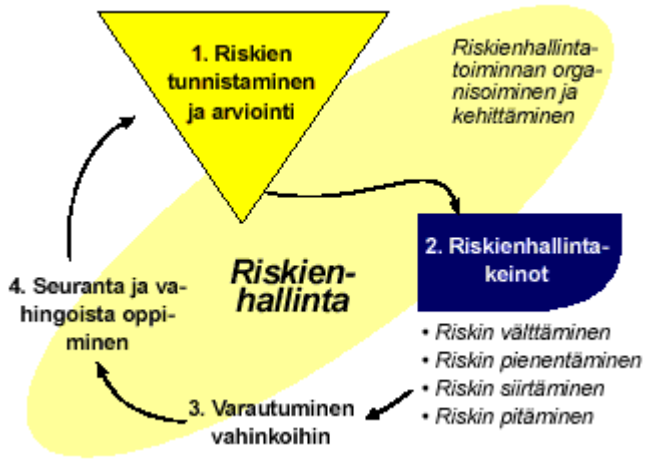
#### 4.1.2.3 PK-RH

Vaikka Suomen Riskienhallintayhdistyksen PK-RH on suunniteltu pienten ja keskisuurten yritysten riskienhallintaan, periaatteet pätevät tarvittaessa myös suurempiin organisaatioihin. PK-RH-riskienhallinnassa (2014) todetaan, että riskienhallinta on organisaation johdon ja muun henkilökunnan toteuttama organisaation johtamiseen ja toimintaan sisältyvä prosessi, jota sovelletaan strategian valinnasta lähtien kaikessa organisaation toiminnassa (yksiköt, prosessit, asiakassuhteet jne.). PK-RH:n mukaan riskienhallinnan tavoitteena on tunnistaa ja hallita organisaatioon vaikuttavia potentiaalisia tapahtumia ja pitää riskit sellaisissa rajoissa, ettei organisaation toiminta ole uhattuna, ja jotta voidaan vähentää epävarmuutta organisaation tavoitteiden toteutumisesta.

PK-RH kuvailee riskienhallintaa työksi yrityksen toiminnan jatkuvuuden ja henkilöstön hyvinvoinnin turvaamiseksi, jolloin riskienhallinnalla tarkoitetaan kaikkea yrityksessä tehtävää toimintaa riskien ja niistä aiheutuvien vahinkojen vähentämiseksi. Riskienhallinta on yksinkertaisuudessaan tilanteiden arviointia, suunnittelua ja käytännön tekoja, johon osallistuu kukin henkilöstön jäsen omassa roolissaan. PK-RH:n mukainen hyvä riskienhallinta on luonteeltaan ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä.

PK-RH:n näkökulmasta riskienhallinta on epäedullisten ja haitallisten tapahtumien välttämistä (vaikutetaan tapahtuman todennäköisyyteen) tai tapahtumien seurausten pienentämistä (vaikutetaan seurauksen suuruuteen). Riskienhallinta on samalla myös potentiaalisten mahdollisuuksien tunnistamista, analysointia ja hyödyntämistä, jolloin kaikki nämä toiminnat tukevat yrityksen tavoitteiden saavuttamista.

PK-RH:n mukaisella riskienhallintaprosessilla on selkeät päävaiheet, jossa riskit ensin tunnistetaan ja arvioidaan. Sen jälkeen suunnitellaan tarvittavat toimenpiteet riskien hallitsemiseksi. Kolmannessa vaiheessa suunnitellaan miten vahingon sattuessa toimitaan, ja miten vahingoista toivutaan. Viimeisessä vaiheessa tilannetta ja toimenpiteiden vaikutusta seurataan, sekä tarvittaessa raportoidaan yrityksen ylimmälle johdolle yrityksen riskitilanteesta (merkittävimmät riskit ja niiden kehitys). Lopuksi toteutuneista riskitapahtumista myös opitaan.




Kuva 3: PK-RH:n riskienhallinta. (Suomen Riskienhallintayhdistys 2014.)

### 4.1.3 Riskimatriisi

Hopkin (2010, 17) toteaa, että riskin todennäköisyyden ja voimakkuuden (tai vaikuttavuuden) hahmottaminen onnistuu parhaiten riskikartan tai riskimatriisin avulla. Tyypillinen riskimatriisi on seuraavanlainen:


Kuva 4: Riskimatriisi - riskin todennäköisyys ja voimakkuus. (Hopkin 2010, 18.)

Riskimatriisien teossa voidaan hyödyntää myös riskien luokittelua eri tyyppeihin. Riskityypit voidaan Ilmosen, Kallion, Koskisen ja Rajalan (2010, 70 - 71) mukaan jakaa:

- Strategisiin riskeihin (mm. taloudelliset, sosiaaliset ja poliittiset riskit)
- Taloudellisiin riskeihin (mm. korkoriskit, valuuttariskit)

- Operatiivisiin riskeihin (mm. organisaatioon tai johtamiseen liittyvät riskit)
- Vahinkoriskeihin (mm. työterveys, työturvallisuus- ja henkilöstöriskit).

Riskien keskinäistä vertailua varten on kehitetty riskitulo, jossa riski määritellään ei-toivotun tapahtuman esiintymistodennäköisyyden ja ei-toivotun tapahtuman kustannusten tuloksi. Riskitulon avulla saadaan lukuarvo, jonka perusteella riskit voidaan asettaa tärkeysjärjestykseen. Korkeimman arvon saavat riskit ovat tärkeimpiä käsiteltäviä, sillä niiden seuraukset ovat vakavimmat. (Berg 1994, 21.)

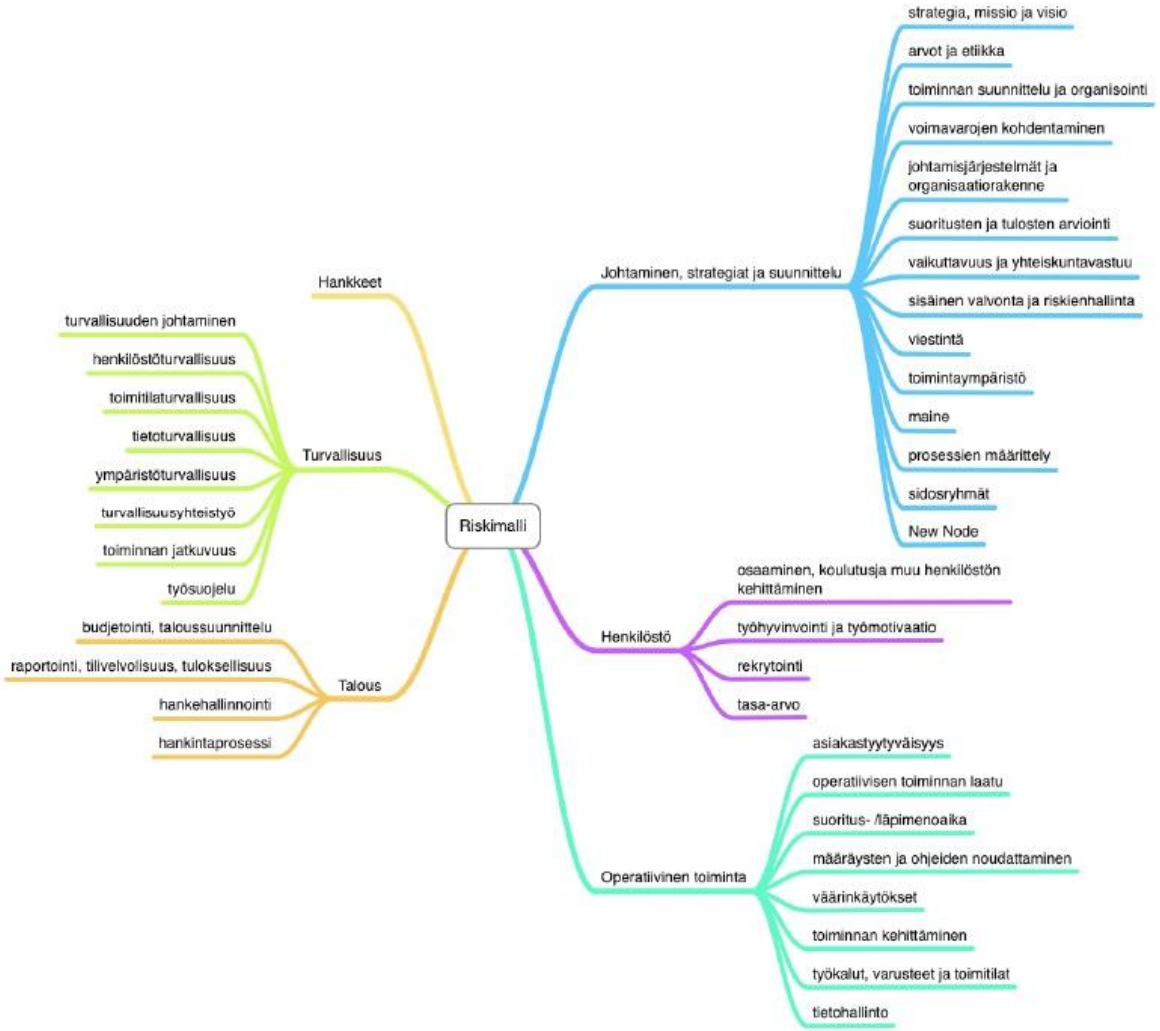
### 4.1.4 Poliisin riskienhallinta

Poliisia koskeva määräys Poliisin riskienhallintapolitiikasta 2020/2013/828 on julkaistu 13.2.2013. Määräyksessä on määritelty poliisihallinnon kokonaisvaltaisessa riskienhallinnassa noudatettavat periaatteet, vastuut, roolit ja käsitteet. Riskienhallinnan tavoitteena on tunnistaa, minimoida ja hallita niitä riskitekijöitä, jotka uhkaavat poliisin toimintaa, toiminta-edellytyksiä ja strategisia tavoitteita. Riskienhallinnan avulla varmistetaan, että poliisihallinnon johtamis-, suunnittelu- ja päätöksentekoprosesseissa on käytettävissä riittävästi tietoa organisaation olemassaoloa ja toimintaa uhkaavista riskeistä. Riskien tunnistamisen, analysoinnin ja hallinnan tulee olla myös osa hanke- ja tapahtumasuunnittelua sekä -ohjausta, eli osa myös Lupa 2016- sekä Sähkö-hankkeiden suunnittelua.

Poliisin riskienhallinnan päämääränä on tukea toiminnallisten tavoitteiden saavuttamista ja toiminnan jatkuvuutta varmistamalla, että poliisiyksiköillä on:

1. tarpeellinen tieto riskeistä, mukaan lukien menestymisen mahdollisuudet ja toimintaa kohtaavat uhkat
2. riskienhallinnan vastuunjaon selkeä kuvaus
3. systemaattiset menetelmät arvioida ja seurata riskejä sekä keinot hallita niitä. (Poliisin riskienhallintapolitiikka 2013, 1.)

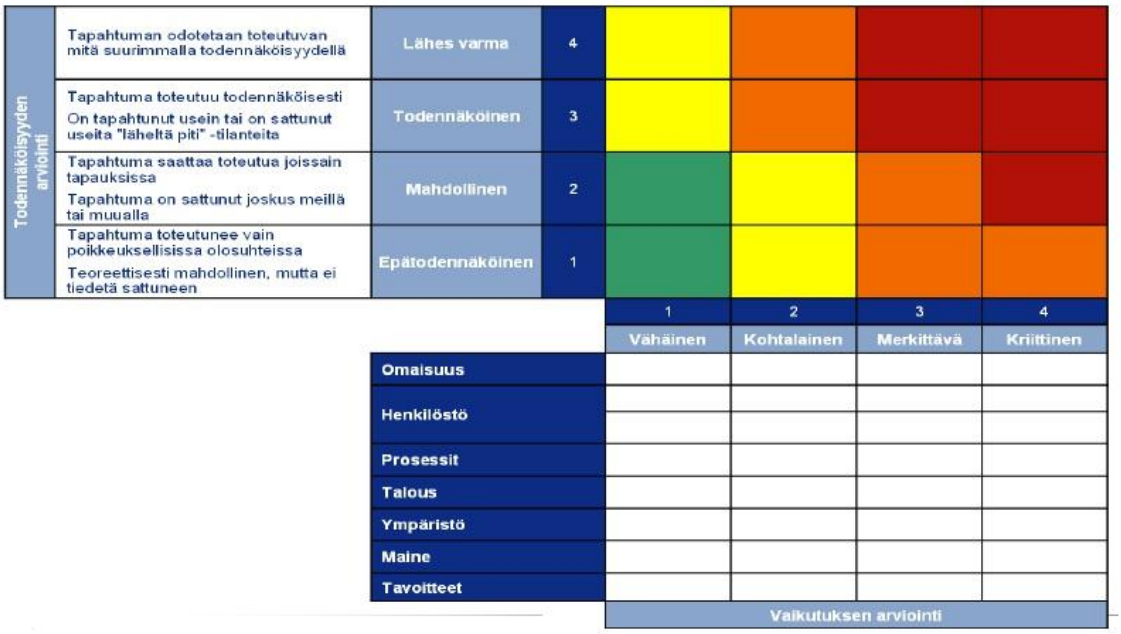
Poliisin riskien luokittelua varten on laadittu malli, jossa riskit luokitellaan osa-alueisiin. Riskimalli toimii apuvälineenä hahmotettaessa loogisia asiakokonaisuuksia, joiden puitteissa riskienarvioinnin ja -hallinnan keinoin tuotetaan tietoa johdon päätöksenteon tueksi. Riskimallia ja sen mukaista riskienhallintarakennetta voidaan tarvittaessa täydentää ja kehittää toimintojen tarpeiden mukaisilla yksityiskohtaisemmilla, tehtäväalakohtaisilla kartoituksilla (esim. työsuojelu, tietoturva).




Kuva 5: Poliisin riskimalli (Poliisin riskienhallintapolitiikka 2013, 2.)

Yhtä ja yhtenäistä riskienhallintaorganisaatiota ohjataan keskitetysti Poliisihallituksesta. Poliisiylijohtajan tehtäviin kuuluu vahvistaa riskienhallintapolitiikka, sekä vastata sen asianmukaisuudesta ja riittävyydestä. Poliisihallituksen turvallisuuspäällikkö vastaa poliisihallinnon riskienhallinnan ohjaamisesta, valvonnasta, kehittämisestä ja yhteensovittamisesta. Turvallisuuspäällikkö toimii myös poliisihallinnon riskienhallintatyöryhmän puheenjohtajana, sekä vastaa poliisiylijohtajalle laadittavasta riskiarviontien kokonaisarviosta. Poliisin yksiköissä riskienhallinnasta ja siihen liittyvästä raportoinnista vastaa yksikön johto, ja lisäksi jokaisessa poliisin yksikössä toimii riskienhallinnan yhteyshenkilö. Riskienhallinta on kiinteä osa poliisiyksiköiden tulossuunnittelu- ja seurantaprosessia. Hankejohtajat vastaavat hankkeen riskien tunnistamisesta ja hallinnasta sekä raportoinnista, kuten myös Lupa 2016-hankkeessa. Hankejohtaja tai hankkeesta muutoin vastaavan tehtävänä on varmistaa, että riskienhallinnan resursointi on riittävää ja asianmukaista ja että se tukee hankkeen tavoitteita. (Poliisin riskienhallintapolitiikka 2013, 3 - 4.)

Riskienhallintapolitiikassa on kuvattu toteuttamistapa riskien tunnistamiseen. Riskien kartoittaminen tehdään yleensä sähköisen riskienhallintatyökalun avulla. Riskien arviointi perustuu riskin toteutumisen todennäköisyyden ja vaikutuksen arviointiin, joiden perusteella riskit jaetaan vähäisiin, kohtalaisiin, merkittäviin ja kriittisiin riskeihin. Politiikan mukaisesti riittävät hallintakeinot on määritettävä, aikataulutettava ja vastuutettava vähintään korkeiden ja kriittisten riskien hallintaan. Sähköisen riskienhallintatyökalun sijasta ja turvallisuuspäällikön hyväksyessä menettelyn, voidaan erityisistä syistä käyttää myös muuta yhteensopivaa menetelmää.




Kuva 6: Poliisin riskien arviointiasteikot.

Poliisin riskien arviointiasteikossa:
1. Arvioidaan riskin todennäköisyys.
2. Arvioidaan riskin toteutumisen vaikutukset. Vaikutuksen arviointia voidaan auttaa miettimällä esim. taloudellisia vaikutuksia, vaikutuksia henkilöstöön, maineeseen jne. (Poliisin riskienhallinnan prosessi, 2014.)

## 4.2 Sähköinen asiointi

### 4.2.1 Sähköinen asiointi Suomessa

Asiakaslähtöiset sähköisen asioinnin yhteiset palvelut ovat yksi julkisen hallinnon keskeisimpiä kehittämiskohteita, jonka tavoitteena on lisätä asiakaskeskeisyyttä, kustannustehokkuutta ja tuottavuutta sekä tukea uusien laadukkaiden palveluiden syntymistä. Sähköinen asiointitili, joka avattiin osana Suomi.fi-portaalia tammikuussa 2011, on viranomaisen ja asiakkaan väli-

sen sähköisen vuorovaikutuksen keskitetty ratkaisu, joka on liitettävissä jo olemassa oleviin viranomaisten sähköisiin asiointipalveluihin. Asiointitilin kautta kansalainen voi saada itseään koskevat päätösasiakirjat ja tiedoksiannot sähköisessä muodossa, toimittaa sähköisiä asiakirjoja viranomaisille ja ylläpitää omia sähköisiä tavoitettavuustietojaan. (Valtiovarainministeriö, 2014.)

Sähköisen asiointipalvelun käyttäjämäärä on kaksinkertaistunut noin puolessa vuodessa. Tällä hetkellä palvelua käyttää jo yli 40 000 kansalaista. Yli 90 julkishallinnon organisaatiota on ilmoittanut haluavansa ottaa asiointitilin käyttöönsä vuoden 2014 aikana. Asiointipalvelun tarkoituksena on korvata sen käyttöön ottaville kansalaisille paperiposti, ja tarjota ajasta ja paikasta riippumaton turvallinen sähköinen viestinvälityskanava ja postilaatikko viranomaisasiointiin. Sähköisen asioinnin yleistymistä halutaan myös vauhdittaa nykyisestä. Tulevaisuudessa myös yritysten asiointia viranomaisten kanssa ohjataan kulkemaan asiointipalvelun kautta. Tanskassa asiointipalvelu on jo pakollinen viranomaisten ja yritysten välisen viestinnän kanava ja kansalaisille se tulee pakolliseksi marraskuussa 2014. (Valtiovarainministeriö 2014.)

Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003) astui voimaan 1.2.2003. Sähköisiä asiointipalveluja ja sähköistä hallintomenettelyä koskevat säännökset ovat olleet voimassa yli 10 vuoden ajan lähes muuttumattomina. Sähköisen asioinnin lainsäädännön seuranta- ja kehittämistutkimus julkistettiin 29.1.2014. Kyseessä on valtiovarainministeriön ja Itä-Suomen yliopiston yhteinen tutkimusprojekti, jonka tarkoituksena oli selvittää millaisia muutostarpeita sähköisen asioinnin sääntelyyn tarvitaan. Erityisesti tutkimuksessa selvitettiin voimassa olevan sääntelyn toimivuus sähköistä asiointia kehitettäessä ja sähköisiä asiointipalveluita käytettäessä. Tutkimuksen johtopäätöksinä esitettiin sähköistä asiointia, sähköistä tunnistamista, sähköistä arkistointia, sähköisten palveluiden tuotantoa sekä määräaikojen laskentaa koskevan lainsäädännön kehittämistä ja uudistamista. Myös Euroopan unionin sääntelykehitys tulee vaikuttamaan Suomessa ainakin sähköisen tunnistamisen sekä sähköisten palveluiden käytön esteettömyyden sääntelyyn. (Sähköisen asioinnin lainsäädännön seuranta- ja kehittämistutkimus 2013, 17 - 22.)

### 4.2.2 Riskit sähköisessä asioinnissa

Heeks (2003, 2) on todennut, että sähköistä asiointia kehitetään vauhdikkaasti julkisen sektorin tehokkuuden paranemisen toivossa. Heeksin mukaan valtaosa projekteista epäonnistuu täysin tai osittain, ja arviolta vain 15 % onnistuu. Sähköisen asioinnin kehittämistä tehdään myös kehittyvissä maissa. Näissä maissa epäonnistumisen vaikutukset ovat suhteellisesti suuremmat taloudellisesta näkökulmasta. Keskeistä sähköisten palveluiden epäonnistumiselle on liian suuri muutos nykyhetkestä tavoitetilaan. Mitä suurempaa muutosta yritetään kerralla,

sitä suuremmalla todennäköisyydellä sähköisen asioinnin hanke epäonnistuu. Heeks on tuonut esiin riskin pienentämistekniikoita ulottuvuuksittain, joita ovat tieto, teknologia, prosessit, tavoitteet ja arvot, henkilöstö ja osaaminen, johtamisjärjestelmät ja -rakenteet sekä muut voimavarat. Heeksin esimerkkitutkimuksen löydösten perusteella yleiset hyvät käytänteet sekä erityisen suurien muutosten havaitseminen ja niihin liittyvien riskien pienentäminen projektin aikaisessa vaiheessa paransivat projektin onnistumisen mahdollisuuksia. (Heeks 2003, 2, 12 - 13, 17.)

Sähköistä asiointia koskeva, myös kansainvälinen, riskejä esiintuova materiaali keskittyy harmittavan usein tietotekniikkaan ennemmin kuin prosessiriskeihin tai käytännön toimintaa koskeviin riskeihin, vaikka riskienhallinnan tulisi olla kokonaisvaltaista. Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI) 4/2001 on antanut yleisohjeen sähköisten palveluiden ja asioinnin tietoturvallisuudesta. Yleisohjeessa todetaan, että sähköisiin palveluihin liittyvät riskit ovat suuremmat kuin perinteisiin palveluihin, koska vahingot tapahtuvat nopeammin ja voivat olla aiempaa vakavampia. Myös varautuminen riskeihin on suhteutettava palvelun tyyppiin. Yleisohjeen mukaan sähköisten palveluiden riskianalyysi tulisi tehdä samoin menetelmin kuin perinteisissä palveluissa, mutta analyysin merkitys on kuitenkin tietyissä palveluissa suurempi. Usein riskin lähteitä ja kohteita on myös enemmän. Ensisijaisesti pyritään välttämään riskejä ja toissijaisesti minimoimaan niiden aiheuttamaa uhkaa. Myös uhkan toteutumisesta aiheutuvaa vahinkoa pyritään rajoittamaan ja vahinkojen korjaamista nopeuttamaan ennakkosuunnittelulla. (VAHTI 4/2001, 7, 21.)

Sähköisen asioinnin lainsäädännön seuranta- ja kehittämistutkimuksessa (2013) ei tuotu esiin merkittävissä määrin riskinäkökulmia. Raportissa on keskitytty sähköisessä asioinnissa enemmän positiivisiin puoliin. Sähköisen asioinnin odotetaan tuovan helppokäyttöiset palvelut kansalaisten ulottuville vuorokauden ympäri samalla kun eri viranomaisten toimipisteverkostoja joudutaan ankarastikin supistamaan. Sähköisen asioinnin muodostamat hyödyt ovat merkittävät niin viranomaisten kustannusten pienentymisen kannalta kuin asiakaspalvelun paranemisen kannalta. Sähköisen asioinnin kehittämisessä tulisi kuitenkin huomioida, että hallintolain soveltaminen sähköisessä asioinnissa ei voi olla silmiinpistävästi väljempää kuin hallintolain soveltaminen henkilökohtaisessa asioinnissa. Hallintolain (6.6.2003/434) tarkoituksena on nimenomaisesti toteuttaa ja edistää hyvää hallintoa sekä oikeusturvaa hallintoasioissa, sekä edistää myös hallinnon palvelujen laatua ja tuloksellisuutta.

Hannu Kytö on todennut artikkelissaan "Verkkopalvelujen turvallisuus kuluttajan näkökulmasta" (2007), että viranomaiset pyrkivät paikkaamaan verkkopalveluilla harvenevaa palveluverkkoaan. Kydön mukaan turvallisuus (tosin koskien myös tietoturvallisuutta) ratkaisee verkkopalvelujen tulevaisuuden. Kydön mukaan lähellä eläkeikää olevat suuret ikäluokat ovat verkkopalvelujen suurin potentiaalinen käyttäjäryhmä, joiden suhtautuminen verkkopalvelujen

turvallisuuteen voi muuttua hyvinkin herkästi. Suuret ikäluokat suhtautuvat nuorempia ikäryhmiä varovaisemmin uusiin palvelumuotoihin. Turvallisuuden lisääminen voi kuitenkin kääntyä helposti itseään vasten. Näin voi käydä, jos tunnistamisesta tulee liian monimutkaista, ja se muuttuu tällöin verkkopalvelujen käytön esteeksi. Kydön mukaan kuluttajat haluavatkin tunnistautumisesta mahdollisimman helppokäyttöisen prosessin, jossa käyttäjäystävällinen ja mahdollisimman pitkälle standardoitu tunnisteteknologia helpottaisi huomattavasti sekä julkisten hyvinvointipalvelujen että yksityisten palvelujen käyttöä. Tunnistamiseen liittyviä haasteita olen kuvannut tarkemmin kappaleessa 4.2.2.2.

Kefallinoksen, Lambroun ja Sykaksen (2009, 10) mukaan sähköisen asioinnin asiantuntijoiden ja tutkijoiden tulee olla oma-aloitteisia, näkemyksellisiä ja tehokkaita kiinnittäessään huomiota relevantteihin haasteisiin ja riskeihin. Heidän myös odotetaan käyttävän tarkoituksenmukaisia strategioita ja työkaluja vaikeuksien ylittämiseksi. Modernit riskienhallintastandardit, menetelmät, viitekehykset, työkalut sekä turvallisuutta ylläpitävät tekniset ICT-ratkaisut turvaavat riskienarvioinnin prosessia. Usein koetaan kuitenkin kyvyttömyyttä havaita niitä riskejä, jotka kumpuavat valtionhallinnon työntekijöiden, johtajien, sopimuskumppaneiden tai yleisen käyttäjäkunnan epäteknisistä organisatorisista, sosiaalisista tai psykologisista ongelmista. Kefallinoksen ym. laajennetussa riskienarviointimallissa huomioidaan yksitoista riskikategoriaa: poliittinen, johdollinen, palveluhenkilökunta, sopimuskumppanit, loppukäyttäjät, sosiaalinen, aikaisemmat toimintapolitiikat, lainopillinen, taloudellinen, hankinta sekä yhteentoimivuus. (Kefallinos ym. 2009, 7 - 10.)

Koska Suomen mittapuulla sähköisessä asioinnissa havaituista prosessiriskeistä ei ollut konkreettista, tai ainakaan julkista materiaalia tarjolla, tämän vuoksi keskitin konkreettisia riskejä koskevan tiedonkeruun sähköpostikyselyihin niille kahdelle suomalaiselle viranomaiselle, joilla on ollut jo jonkin aikaa sähköistä asiointia. Tätä tietoa tuon esiin tutkimusaineiston yhteydessä, kuin myös kansainvälisiä passimenettelyn sähköisen asioinnin riskejä niistä maista, joilla menettelyä on jo olemassa.

#### 4.2.2.1 Sähköisen asioinnin perusta - luotettava tunnistaminen

Sisäministeriön henkilöllisyyden luomista selvittävän hankkeen (jäljempänä Id-ohjelma) työryhmän loppuraportin mukaan (2010, 65) luotettavan henkilöntunnistuksen tarve voidaan jakaa kahteen ryhmään. Ensimmäinen liittyy läsnä olevan henkilön tunnistamiseen ja toinen verkkoasioinnin yhteydessä tapahtuvaan tunnistamiseen. Suurin osa tunnistamiseen liittyvistä riskeistä koskee kuitenkin kumpaakin toimintaympäristöä, kun on kyse itse tunnistamistapahtumasta. Vahvan sähköisen tunnistamisen varmenteet perustuvat viranomaisen myöntämiin fyysisiin asiakirjoihin. Kun sähköisessä asioinnissa pitää varmistua asioijan henkilöllisyydestä, pohjautuu kaikki siis henkilön tunnistamiseen (myyjä tai viranomainen varmistuu asioivan

henkilön henkilöllisyydestä) ja toisaalta tunnistautumiseen (kansalainen tunnistautuu valitsemallaan mahdollisella tavalla viranomaiselle tai yksityiselle taholle).

Henkilöllisyyttä osoittavien asiakirjojen osalta julkisen vallan käyttöala on selvä, koska passin ja henkilökortin myöntämisessä kyse on hallintotoiminnasta ja merkittävästä julkisen vallan käytöstä. Henkilöllisyyttä osoittavien asiakirjojen myöntäminen on osa viranomaisen ydintehtävää eikä sitä voida siirtää yksityiselle toimijalle. Passi ja henkilökortti ovat valtion takaamia henkilöllisyyttä osoittavia asiakirjoja. Henkilöllisyyttä osoittavien asiakirjojen osalta ei ole olemassa kuitenkaan yleistä lainsäädäntöä, jossa olisi määritelty kaikki hyväksyttävät tunnistamisasiakirjat. Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009) säätelee vahvan sähköisen tunnistamisen välinettä haettaessa käytettävistä tunnistusasiakirjoista, jotka ovat passi, henkilökortti ja valinnaisesti myös vuoden 1990 jälkeen myönnetty ETA-maiden ajokortti. Mahdollisuus käyttää ajokorttia nk. ensitunnistamiseen, eli ensimmäistä kertaa tehtävään tunnistamiseen, jonka perusteella sähköinen henkilöllisyys luodaan, oli lakia koskevassa hallituksen esityksessä määräaikainen, mutta eduskunta poisti määräaikaisuuden sen johdosta, että tosiasiallinen vallitseva käytäntö perustuu pitkälti ajokortin käyttöön. (Id-ohjelma 2010, 28, 31.)

Kansalaisten oikeusturvan kannalta sekä viranomaistoiminnan luotettavuuden kannalta keskiössä on henkilön luotettava tunnistaminen kaikissa toimintaympäristöissä. Suoritettavat oikeustoimet ovat yhtä sitovia riippumatta käytettävästä välineestä (Id-ohjelma 2010, 65).

#### 4.2.2.2 Tunnistamisessa piilevät ongelmat

Suomen kansalaisen sähköinen asiointi poliisille tapahtuu Suomi.fi- portaalin sähköisen asiointipalvelun kautta internet-osoitteessa https://asiointitili.suomi.fi. Kansalainen varmentaa henkilöllisyytensä joko:

- henkilökortin kansalaisvarmenteella
- mobiilivarmenteella tai
- verkkopankkitunnuksilla.

Poliisin myöntämän Suomen kansalaisen henkilökortin osana myönnettävä kansalaisvarmenne vaatii toimiakseen kortinlukijalaitteen ja -ohjelmiston. Vain henkilökortin ja sen mukana myönnettävän kansalaisvarmenteen myönnön yhteydessä poliisi on henkilön tunnistamisen suorittava viranomainen, silloin kun tunnistaminen tehdään fyysisessä toimintaympäristössä poliisin toimesta.

Mobiilivarmennetta markkinoidaan sähköisenä henkilöllisyystodistuksena kännykässä. Sen avulla voidaan todistaa henkilöllisyys ja luoda allekirjoitus erilaisissa sähköisissä palveluissa,

kuten internetin käytön yhteydessä tai puhelun aikana. Tunnistaminen tehdään mobiilivarmenteen tapauksessa matkapuhelinoperaattorin (DNA, Elisa, Sonera) toimesta.

Henkilökortin kansalaisvarmenne ei ole ollut käytettävyydeltään kansalaisia parhaiten palveleva, joten yleisesti käytössä olevien verkkopankkitunnusten käytön helppous on ajanut helposti kansalaisvarmenteen käytön ohi. Mobiilivarmenteen tapauksessa kuluttajat eivät ole mahdollisesti löytäneet palvelua omakseen vielä, mutta trendi saattaa olla älypuhelinten käytön yleistyessä kasvava. Sekä kansalaisvarmenteen että mobiilivarmenteen käyttö on sähköisissä palveluissa hyvin vähäistä, joten yleisintä on verkkopankkitunnuksilla tunnistautuminen. Henkilön tunnistaminen sähköisessä asioinnissa tapahtuu täten viranomaisen myöntämiin asiakirjoihin pohjautuen hyvin usein pankissa, joka verkkopankkitunnukset antaa.

Pankit noudattavat asiakkaan tunnistamisessa mm. rahanpesun ja terrorismin rahoittamisen estämisestä ja selvittämisestä annettua lakia (503/2008) ja Finanssivalvonnan antamaa standardia 2.4 asiakkaan tuntemisesta ja tunnistamisesta. Rahanpesulain keskeisenä periaatteena on asiakkaan tunteminen ja riskiperusteinen lähestymistapa. Finanssivalvonnan standardin 2.4 mukaan kun asiakassuhde perustetaan siten, että asiakas on henkilökohtaisesti läsnä, henkilöllisyyden todentaminen perustuu viranomaisen antamaan voimassa olevaan henkilöllisyysasiakirjaan. Jos asiakassuhde perustetaan tapaamatta asiakasta henkilökohtaisesti, pankilla tulee olla käytössään menetelmät, joiden avulla se pystyy todentamaan asiakkaan henkilöllisyyden luotettavasti. Yksi todentamismenetelmä on, että pankkiasiakas tunnistautuu sähköisesti käyttäen tunnistusvälinettä, joka täyttää tunnistuslaissa tarkoitetun vahvan sähköisen tunnistusvälineen tai laatuvarmenteen kriteerit. Henkilökohtaisessa asioinnissa asiakas tunnistetaan Suomessa yleisesti käytettyjen henkilöllisyyden todentamisasiakirjojen avulla, joita ovat voimassaolevat, suomalaisen viranomaisen myöntämät ajokortti, henkilökortti, passi, diplomaattipassi, muukalaispassi, pakolaisen matkustusasiakirja ja kuvallinen Kela-kortti. Pankki voi todentaa luonnollisen henkilön henkilöllisyyden myös voimassaolevilla, ulkomaisen viranomaisen myöntämillä asiakirjoilla, kuten kansallinen passi ja matkustusasiakirjana hyväksyttävä henkilökortti. (Finanssivalvonta 2010.)

Finanssialan Keskusliiton antaman ohjeen mukaan Tupas-tunnistuspalvelussa käytettävien pankkitunnusten osalta ensitunnistamisessa noudatetaan vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annettua lakia (617/2009) ja Viestintäviraston määräystä 8C/2010. (Finanssialan keskusliitto 28.3.2011.)

Muiden sähköisten palveluiden osalta tunnistamistavat vaihtelevat. Kansalaiset käyttävät paljon sähköisiä palveluita, joiden tunnistamisaste ja -tavat ovat hyvin erilaisia. Myös palvelujen luotettavuuden arviointi voi olla kansalaisen näkökulmasta vaikeaa. Tietovarkaudet ovat arkipäivää, ja kiinnijäämisen riski on olematon. Poliisin myöntämien henkilöllisyyttä osoittavien

asiakirjojen (passi ja henkilökortti) myöntämisessä henkilön tunnistaminen on prosessin tärkein vaihe ja kaiken perusta. Ensitunnistaminen on kriittinen vaihe niin tunnistamisasiakirjoja kuin sähköisiä varmenteitakin myönnettäessä. Sähköisessä toimintaympäristössä (vahva sähköinen tunnistaminen) ensitunnistaminen on keskeistä, kun viranomainen myöntää tai yksityinen palveluntarjoaja antaa asiakkaalle sähköisiä varmenteita. Tässä tunnistamisasiakirjat ovat olennaisessa roolissa. Luotettava verkkoasiointi on mahdollista vain, jos verkkotunnistautumisessa käytettävä tunniste on riittävän vahva ja se on alun perin luovutettu oikealle henkilölle. Verkkoasioinnin luotettavuus riippuu ratkaisevasti siitä, miten ensimmäistä kertaa sähköistä tunnistetta hakeva on tunnistettu hänen ollessaan fyysisesti läsnä hakemuksenjättöpaikassa. (Id-ohjelma 2010, 65 - 66.)

Ensitunnistamistilanteita voi olla erilaisia. Mikäli kyse ei ole viranomaisen suorittamasta fyysisessä toimintaympäristössä tapahtuvasta tunnistamisesta, kyseessä voi olla esimerkiksi pankkitunnusten tai mobiilivarmenteen myöntämistilanne, jossa pankki tai operaattori varmistuu kyseistä sähköistä varmennetta hakevan henkilön henkilöllisyydestä. Yhtä lailla kyseessä voi olla tilanne, jossa autokoulunopettaja tarkistaa ajo-oppilaan henkilöllisyyden, jonka perusteella henkilölle myönnetään ajokortti, jota henkilö käyttää henkilöllisyytensä osoittamiseen.

Suomessa tavataan harvoin tunnistamisen pohjalla käytettäviä väärennettyjä suomalaisten passeja ja henkilökortteja, sillä niiden turvataso on hyvin korkea ja aidoista asiakirjoista on saatavilla helposti mallikappaleita vertailuja varten. Varsinaisten asiakirjojen tai varmenteiden myöntämiseen liittyvien ongelmien lisäksi tunnistamiseen liittyy myös muita käytännön ongelmia. Näistä ongelmista yksi suurimmista on ns. näennäistunnistaminen. Näennäistunnistamisessa katsotaan esimerkiksi vain tunnistamisasiakirjasta henkilötunnuksen loppuosa, mutta ei verrata nimiä tai katsota onko kuvassa oikea henkilö. Tunnistamiseen käytettäviä asiakirjoja on myös paljon, joten tunnistaminen vaatii erityisosaamista ja koulutettua henkilöstä. Id-ohjelma 2010, 65 - 66.)

Epätoivotussa tapauksessa toinen viranomainen tai yksityinen sektori hyväksyy tunnistamisasiakirjaksi sekä myöntöprosessiltaan että jo fyysisiltä turvatekijöiltään vaatimattoman jonkun viranomaisen myöntämän, täysin eri käyttöön alun perin tarkoitetun asiakirjan. Tätä asiakirjaa voidaan käyttää tarkoituksella tai tahattomasti väärin. Identiteettivarkaus on yleiskielessä käytetty käsite laajalle joukolle erilaisia tekokokonaisuuksia, joille on kuitenkin yhteistä se, että jotakin identiteettitietoa kerätään oikeudetta. Kerättyä tietoa käytetään edelleen oikeudetta joko rikoshyödyn hankkimiseksi tai tavalla, josta aiheutuu identiteetin haltijalle vahinkoa (Id-ohjelma 2010, 47).

Yhtenä keskeisimpänä ongelmana tunnistamisessa pankin tai operaattorin tunnistusprosessin luotettavuuden lisäksi voidaan pitää ajokortin hyväksymistä laajalti henkilöllisyyttä osoittava-

na asiakirjana, vaikka sisäasiainministeriö on asetustasoisesti katsonut, ettei ajokorttia ole tarkoitettu tunnistamisasiakirjaksi, eikä sen myöntöprosessi ole niin turvallinen, että sen käyttö tunnistamisasiakirjana olisi jatkossa perusteltua. ID-ohjelman työryhmä teetti työryhmän loppuraporttia varten osittain luottamuksellisen riskianalyysin tunnistamisprosessiin liittyvistä riskeistä, joista julkiseksi määritellyt riskit on tuotu tässä kohden esiin. Toimeksianto sisälsi myöntöprosessin tarkastelun (tunnistaminen ja siinä käytettävät tunnistamisasiakirjat) passin, henkilökortin ja ajokortin sekä kansalaisvarmenteen osalta. Riskianalyysin teki yksityinen konsulttitoimisto, jonka työtapoina olivat työpajat, haastattelut sekä tehdyt dokumentaatiot. Haastateltavat olivat sisäasiainministeriöstä, ulkoasiainministeriöstä, Maahanmuuttovirastosta sekä poliisilaitoksilta ja kaikilla oli käytännön asiakaspalvelutyöstä kokemusta. Riskianalyysissä tuli mm. esiin, että ajokortin hyväksyminen tunnistamisasiakirjaksi on sietämätön riski. (Id-ohjelma 2010, 66 - 68.)

Ajokortin käyttöön liittyvät ongelmat Id-ohjelman (2010, 69 - 71) mukaan ovat:

1. Myöntöprosessi: Ajokortin myöntöprosessi ei ole samantasoinen kuin passilla ja henkilökortilla, koska siihen ei sisälly viranomaisen tekemää tunnistusta. Ajokortin hakijan henkilöllisyyden tarkistaa ajokorttihakemuksen yhteydessä yleensä autokoulussa yksityinen toimija.
2. Turvataso: Ajokortti on turvatekijöiltään vähäinen ja siten helposti väärennettävä. Houkutus ajokortin väärentämiseen kasvaa, jos/kun sitä voi käyttää tunnistamisasiakirjana, jolla taas voi tehdä sitovia oikeustoimia.
3. Voimassaoloaika: Ajokortin voimassaoloaika (70 vuotta) ei vastaa passin tai henkilökortin voimassaoloaikaa (5 vuotta). (Tässä yhteydessä on huomioitava, että ajokorttilaki muuttui 19.1.2013, jossa muutettiin eräitä ajokorttiluokkia sekä ajokorttien voimassaoloaikoja. Uusien säännösten mukaan ajo-oikeus on voimassa määräajan, joka on ajokorttiluokasta ja kortinhaltijan iästä riippuen 2 – 15 vuotta: henkilöauton ja moottoripyörän ajokortit myönnetään pääsääntöisesti 15 vuodeksi ja kuorma-auton ja linja-auton ajokortit 5 vuodeksi kerrallaan. Ennen 19.1.2013 myönnetyt ajokortit ovat voimassa koko korttiin merkityn voimassaoloajan, kuitenkin enintään vuoteen 2033 asti. Tällöin vanhatkin ajokortit tulee viimeistään uusia.)
4. Kansalaisuus: Ajokortista ei käy ilmi henkilön kansalaisuus, vaan ainoastaan myöntävän valtion kansallistunnus.
5. Ajokortin asema tunnistamisasiakirjana: Tällä hetkellä yleisin tunnistamiseen käytettävä asiakirja on ajokortti, vaikka sitä ei ole sellaiseksi lähtökohtaisesti tarkoitettu. Lähes kaikki palveluntarjoajat hyväksyvät ajokortin, kuten esimerkiksi kaupat ovat laajasti hyväksyneet ajokortin maksutapahtuman varmentamisessa (silloin kun sitä enää nykypäivänä sirukorttimaksun yhteydessä tarvitaan). Tällöin kuitenkin väärällä/väärennetyllä ajokortilla tehdystä ostosta vastaa kauppa tai kortin myöntänyt yhtiö, ei asiakas itse, jolloin kyse on siis yksityisestä riskienhallinnasta. Monissa muissa

tilanteissa kuluttaja voi joutua itse vastuuseen väärinkäytöksistä. Keskeistä on, ettei huonolla tai väärällä asiakirjalla tehdystä tunnistamisesta aiheutuvaa riskiä jätetä kansalaisen kannettavaksi, jolla on olennainen yhteys myös identiteettivarkauksiin.

6. Varmistamaton henkilöllisyys: Muukalaispassiin tai pakolaisen matkustusasiakirjaan mahdollisesti sisältyvä merkintä henkilöllisyyden varmistamattomuudesta ei näy lainkaan ajokortista, jolloin tällainen henkilö, jonka henkilöllisyyttä ei ole voitu varmistaa ja tästä on merkintä hänen oikeassa matkustusasiakirjassaan, voi tieliikennesopimusten mukaan vaihtaa oman maansa ajokortin suomalaiseen. Hän voi käyttää ajokorttia asioinnissa tunnistamisasiakirjan tapaan, vaikka tosiasiassa viranomaisella ei ole varmuutta hänen henkilöllisyydestään.
7. Paperiset ulkomaiset ajokortit: Eräissä EU-maissa on edelleen laajassa tai jopa ainoassa käytössä paperinen ajokortti, jossa on niitattu valokuva, kuten Ranska ja Belgia. Lähtökohtaisesti ulkomaalaisella henkilöllä on maahan tullakseen oltava passi tai henkilökortti, joten ulkomaalaisen ajokortin käyttö on erityisen riskialtista missään tunnistamistarkoituksessa tästä syystä.
8. Ulkomaisen ajokortin vaihtaminen suomalaiseen: Ulkomaalainen henkilö saa Geneven ja Wienin tieliikennesopimusten, joihin lähes kaikki maat ovat liittyneet, mukaan vaihtaa ajokorttinsa suomalaiseen puolen vuoden maassa oleskelun jälkeen, mikäli haluaa ajaa Suomessa ilman uutta kuljettajatutkintoa. Tämän kohdan osalta ongelmana ei ole ajo-oikeus, vaan ajokortin käyttäminen tunnistamisasiakirjana, jossa erityisen ongelmallisia ovat ulkomaalaisille vaihdettavien suomalaisten ajokorttien luotettavuus. Suomalaisiin ajokortteihin vaihdetut kortit ovat fyysisesti täysin samanlaisia Suomessa alun perin myönnettyjen korttien kanssa, ja vain viimeisin vaihtomaa näkyy kortin takana erityisehtokentässä maakoodina. Brysselissä kokoontuvan EU:n Fauxdoc Väärät asiakirjat -työryhmän agendalle on otettu matkustusasiakirjojen ohella myös ajokortit. Työryhmän 23.3.2009 järjestetyssä kokouksessa esitellyn kyselyn tulosten mukaan 84 % jäsenmaista on tavannut kolmansien maiden kansalaisille väärin perustein myönnettyjä ajokortteja, ja 78 % jäsenmaista toivoo, että jatkossakin työryhmä käsittelisi asiaa. Kahdeksalla jäsenmaalla on suuria ongelmia ajokorttien vaihdon osalta, erityisesti Belgialla ja Ranskalla, ja Ranskassa on havaittu, että noin 22 - 30 % kolmansien maiden ajokorteista, joita pyritään vaihtamaan, ovat olleet vääriä tai väärennettyjä. Väärennöksien määrät ovat olleet myös kasvussa. Uhkana on, että petoksen tekijälle annettaisiin viranomaisen myöntämä aito asiakirja, jota voisi käyttää henkilötodistuksena Ranskassa. Belgiassa vastaavat luvut ovat 10 -15 %. Internetissä toimii esimerkiksi eräs palvelu, jonka avulla asiakas voi saada ostotuotteena useimpien maiden, myös Suomen, ajokortin ilman kokeita vain hyödyntämällä eri maiden korttien vaihtokelpoisuutta.
9. Ajokorttien vaihtamisen ketjuttaminen: Väärinkäytöksen muotona esiintyy ulkomaisten ajokorttien vaihtamisen ketjuttamista. Tällöin esimerkiksi kolmannen maan kortti

vaihdetaan johonkin EU-maan korttiin ja tästä edelleen toisen EU-maan korttiin, jolloin kortissa näkyy viimeinen vaihtomaa, eikä alkuperäistä myöntömaata. Kortti näyttää EU-ajokortista vaihdetulta, vaikka onkin alun perin Afrikassa myönnetty, ja näiden ajokorttien ketjuttaminen voi aiheuttaa vakavan vaaran, mikäli niitä käytetään henkilöllisyyttä osoittavina asiakirjoina.

10. Poisottaminen: Ajokortti voidaan ottaa haltijaltaan pois tietyksi ajaksi tai kokonaan, kun taas henkilöllisyyttä osoittavaa asiakirjaa ei voida ottaa rangaistuksen luonteisesti pois.
11. Ajokortin peruuttaminen: Mikäli ajokortti, passi tai henkilökortti varastetaan, tärkeintä on asiakirjan poissaaminen tekijältä. Vaikka tekijä saataisiin kiinni tai hän olisi poliisin tiedossa, väärinkäytöstilanne ei välttämättä korjaannu, mikäli varsinaista asiakirjaa ei saada pois tekijän hallusta. Katoamisilmoituksen voi tehdä poliisille, mutta palveluntarjoajat ja muut viranomaiset eivät saa tietoa kadonneesta tai anastetusta asiakirjasta, ja ilmoitusta ei voi tehdä mihinkään yleisesti nähtävillä olevaan järjestelmään. Kansalaisen kannalta olisi hyvä, mikäli palveluntarjoajalla tai viranomaisella olisi mahdollisuus huomata tunnistamistilanteessa, että tunnistamisasiakirja on ilmoitettu varastetuksi tai kadonneeksi. Erityisen ongelmallinen tilanne on ajokortin osalta, koska mitään tällaista järjestelmää ei ole luotu ajo-oikeutta osoittavalle asiakirjalle. Kadonneeksi ilmoitettu passi ja henkilökortti on mahdollista huomata Euroopan laajuisesti rajanylitystilanteessa, ja näiden asiakirjojen osalta poliisi ja rajavartiolaitos saavat tietokannasta tiedon asiakirjan kadottamisesta, mikäli henkilö on tämän ilmoituksen asianmukaisesti tehnyt.

Tunnistamisen nykykäytäntöihin liittyvistä riskeistä on kuitenkin todettava, että jokainen viranomainen kohtaa saman riskin mahdollistaessaan sähköisen asioinnin, kuten luonnollisesti myös yksityinen toimija, joka käyttää mm. pankkien tarjoamia tunnistuspalveluja sähköisessä kaupankäynnissään, joten poliisi ei ole tunnistamiseen liittyvien riskien kanssa yksin.

#### 4.2.2.3 Muita sähköiseen asiointiin liittyviä haasteita poliisin näkökulmasta

Poliisin haasteena on mm. arvioida, kuinka paljon sähköinen asiointi alentaa kynnystä väärinkäytösyrityksille. Internet toimintaympäristönä aiheuttaa oman haasteensa, koska sähköinen media voi tuoda joissain henkilöissä esiin huonompia puolia. Internetissä kasvoton kommunikointi on myös psykologisesti haastavaa. Ihmiset ovat verkossa myös hyvin luottavaisia, ja henkilö- ja tunnistetietoja luovutetaan helposti edelleen. (Kasvi 2012.)

Nuorten rikoskäyttäytymistä ja uhriksi joutumista koskevissa tutkimuksissa on havaittu, että samalla kun nuorten ajanvietto ja yhteydenpito on yhä enemmän siirtynyt internetiin myös nuorten rikoskäyttäytyminen ja uhrikokemukset ovat laajentuneet tälle kentälle. Esimerkiksi

vertaisverkkojen käyttö tiedostojen lataamiseen ja jakamiseen on useiden kyselytutkimusten mukaan varsin yleistä suomalaisten nuorten keskuudessa. Samalla nuoret ovat kuitenkin olleet varsin hyvin tietoisia siitä, että tekijänoikeudella suojattujen tiedostojen luvaton lataaminen on vastoin Suomen lakia. Aktiivisimmat vertaisverkkolataajat ovat syyllistyneet muita useammin myös muuhun rikollisuuteen. Tutkimuksen mukaan vertaisverkkojen aktiivikäyttäjät eivät olekaan "nettinörttejä", vaan pikemminkin riskikäyttäytymisnuoria. Heille esimerkiksi alkoholinkäyttö, väkivalta ja kaupoista varastelu on muita nuoria yleisempää. Nuorten vertaisverkkolataamisesta ei voida kuitenkaan vetää kauaskantoisia johtopäätöksiä internetrikollisuuden yleisiä asenteita kohtaan. Internetrikollisuudesta tarvitaan edelleen lisää tutkimustietoa, joka tarkastelee nykyistä syvemmin ilmiön yleisyyttä, teonpiirteitä ja riskitekijöitä. (Nuorten rikoskäyttäytyminen ja uhrikokemukset internetissä 2010.)

Sähköisten palvelujen tarjonnan lisäämisen kannalta ongelmana tietoyhteiskunnan muutoksessa on myös kansalaisten kyky pysyä mukana kehityksessä – niin teknisesti kuin sosiaalisestikin. Uusien viestintävalmiuksien omaksuminen koostuu välineistä, taidoista ja motivaatiosta. Sähköisiä palveluja rakennettaessa on myös huomioitava, ettei kaikilla kansalaisilla kuitenkaan löydy tarvittavaa osaamista eikä valmiuksia hyödyntää uutta teknologiaa, mikä aiheuttaa eriarvoisuutta käyttäjien kesken. Tätä digitalisoitumisesta johtuvaa eriarvoisuutta kutsutaan digitaaliseksi kuiluksi tai digitaaliseksi kahtiajakautumiseksi. Tilastotietojen valossa voidaankin todeta, että vaikka suomalaiset ovat aktiivisia Internetin käyttäjiä, joukossamme on vielä runsaasti kansalaisia, jotka eivät halua, osaa tai pysty hyödyntämään tieto- ja viestintätekniikkaa. (Rasmus 2010, 10 - 15.)

# 5 Tutkimusmenetelmä ja -aineisto

## 5.1 Konstruktiivinen tutkimus

Konstruktiivisen tutkimuksen tavoitteena on käytännön ongelmien ratkaiseminen luomalla uusi konkreettinen tuotos kuten esimerkiksi suunnitelma, malli tai menetelmä, ja muutos kohdistuu johonkin konkreettiseen kohteeseen (Ojasalo, Moilanen & Ritalahti 2009, 38). Konstruktiivinen tutkimusote on kehitetty nimenomaan liiketaloustieteen alueella, mutta sen mahdollinen soveltamisala on laaja (Lukka 2001).

Lukka (2001) kuvailee konstruktiivisen tutkimusotteen olevan innovatiivisia konstruktioita tuottava metodologia, jolla pyritään ratkaisemaan reaalimaailman ongelmia ja tällä tavoin tuottamaan kontribuutioita sovellettavalle tieteenalalle. Konstruktiivisen tutkimusotteen ydinkäsitteenä on (uusi) konstruktio, joka on abstrakti käsite, jolla on loputon määrä mahdollisia toteutumia. Konstruktioita ovat kaikki ihmisen luomat artefaktit, kuten mallit, diagrammit, suunnitelmat, organisaatiorakenteet, kaupalliset tuotteet ja tietojärjestelmämallit. Niil-

le on tunnusomaista se, että ne eivät ole löydettyjä, vaan ne ovat keksittyjä ja kehitettyjä. Sellaisen konstruktion kehittäminen, joka poikkeaa kaikesta jo olemassa olevasta, luo jotain uutta.


Kuva 7: Konstruktiivisen tutkimusotteen keskeiset elementit (Kasanen, Lukka & Siitonen 1993, 246.)

Konstruktiivisen lähestymistavan luonteeseen kuuluu Kasasen ym. (1993, 246) mukaan prosessin jakaminen vaiheisiin, joiden järjestys voi tapauskohtaisesti vaihdella:

1. Etsi käytännönläheinen ongelma, jossa on tutkimuspotentiaalia.
2. Hanki yleinen ja kattava ymmärrys käsillä olevasta ongelmasta.
3. Innovoi tai esimerkiksi mallinna ratkaisuvaihtoehto.
4. Osoita, että ratkaisu toimii.
5. Esittele teoreettiset yhteydet ja tutkimuksellinen panos laaditusta ratkaisuvaihtoehdosta.
6. Tutki ratkaisun sovellettavuuden laajuus.

Tässä työssä käytännönläheinen ongelma oli noussut esiin työni kautta. Kun olimme sopineet työnantajan kanssa opinnäytetyön aiheesta ja laajuudesta, lähdin hankkimaan lisätietoa aihepiiriin liittyvistä riskeistä. Havaittujen riskien ja niiden luokittelun perusteella halusin mallintaa prosessin, jotta sitä voisi laajentaa lupahallinnon tai poliisin hankkeiden riskienhallintaan laajemminkin.

Konstruktiivisen tutkimuksen avulla löydetyn ratkaisun toimivuutta voidaan arvioida myöhemminkin - etenkin silloin, kun kyse on kehittämistyöstä, joka on sidottu joltakin osin muun kuin kehittämisen kohteena olevan organisaation aikatauluihin (Ojasalo ym. 2009, 68). Tässä työssä on huomioitava, että passilainsäädäntöä ei ole ehditty käsitellä, ja passia koskeva sähköinen asiointi otetaan aikaisintaan käyttöön vasta syksyllä 2014.

## 5.2 Riskien kartoittaminen

Yleisen ja kattavan ymmärryksen hankkimiseksi, eli aihepiiriin liittyvien riskien kartoittamiseksi, tein tiedonkeruuta eri menetelmin. Tiedonkeruun perusteella sekä haastattelujen avulla muodostin kokonaiskäsityksen riskeistä Suomen passin myöntämiseen liittyvässä sähköisessä asioinnissa.

### 5.2.1 Viranomaisten kokemuksia sähköisestä asioinnista ja siihen liittyvistä riskeistä

Pitkäaikaisinta ja laajinta kokemusta viranomaisten sähköisestä asioinnista Suomessa on Verohallinnolla ja Kansaneläkelaitoksella, joten päätin lähestyä ko. organisaatioiden turvallisuudesta vastaavia henkilöitä sähköpostitse kysymysten muodossa. Tarkoituksena oli saada näkemys siitä, minkälaisia riskitilanteita he ovat toiminnassaan mahdollisesti havainneet.

Selvitin myös, onko missään muussa maassa tällä hetkellä passeihin liittyvää sähköistä asiointia. Tämänhetkisen tiedon mukaan passeihin liittyvää osittaista tai kokonaan sähköistä asiointia on käytössä Kanadassa ja Uudessa-Seelannissa. Sain molemmista maista ko. projekteista vastaavilta henkilöiltä riskeihin liittyviin kysymyksiini vastauksia sähköpostin välityksellä.

#### 5.2.1.1 Verohallinto

Verohallinnon sähköisillä palveluilla on paljon käyttäjiä. Yli puolet verokorttia tarvitsevista Verohallinnon asiakkaista tilaavat verokortin verkosta. Veroilmoitus verkossa -palvelussa henkilöasiakas voi korjata ja täydentää veroilmoituksen tietoja. Asiakkaan ei tarvitse palauttaa paperista veroilmoitusta tai liitelomakkeita lainkaan, jos ilmoittaa tiedot verkossa. Verohallinto kannustaa myös yhteisöasiakkaiden veroilmoituksen paperi-ilmoittajia sähköiseen asiointiin, jota tehdään mm. soittokampanjan avulla maaliskuussa 2014. Verohallinnon mukaan sähköisesti annetut ilmoitukset ovat laadultaan parempia kuin paperilla annetut, koska sähköiset palvelut ohjaavat ilmoituksen antamisessa sekä tekevät laskutoimituksia ja tarkistuksia ilmoittajan puolesta. Paperilomakkeilla tehdyissä osakeyhtiöiden veroilmoituksissa on virheellisiä tietoja huomattavasti enemmän kuin sähköisesti annetuilla ilmoituksilla. Virheselvittelystä saattaa aiheutua asiakkaille tarpeettomia selvityspyyntöjä, sekä viiveitä ilmoituksen käsittelyssä. Verohallinnon sähköisen asioinnin käyttäjät ovat olleet hyvin tyytyväisiä sähköisiin asiointipalveluihin - esimerkiksi vuonna 2013 tehdyssä asiakastyytyväisyystutkimuksessa 99 % yhteisöasiakkaista oli erittäin tai melko tyytyväisiä asioiden hoitumiseen sähköisissä palveluissa. (Verohallinto 2014.)

Lähetin Verohallinnon turvallisuusjohtaja Petri Puhakaiselle kysymyksiä sähköistä asiointia koskien sähköpostitse helmikuussa 2014. Esittämäni kysymykset olivat:

1) Milloin Verohallinnolla on otettu käyttöön ensimmäiset sähköiset palvelut kansalaisille?
2) Onko Verohallinnossa törmätty väärinkäytösyrityksiin siten, että väärä henkilö yrittää suorittaa oikeustoimia sähköisesti toisen henkilön tiedoilla vahingonteko- tai hyötymistarkoituksessa (esimerkiksi yritetty käyttää jonkun toisen henkilön pankkitunnuksia tunnistautumisessa tai kansalaisvarmennetta tai mobiilivarmennetta)? Minkä tyyppisiä nämä väärinkäytökset tai väärinkäytösyritykset ovat olleet, tai mitä hyötyä näillä väärinkäytösyrityksillä on pyritty saavuttamaan?
3) Kuinka suuri osa sähköisiin palveluihin kirjautumisista tapahtuu pankkitunnusten avulla vs. kansalaisvarmenne (henkilökortti) tai mobiilivarmenne?
4) Onko Verohallinnolle tullut vastaan väärinkäytösyrityksiä siten, että "pohjalla" olisi pankissa väärälle henkilölle myönnetty virtuaalinen henkilöllisyys (eli annettu pankkitunnukset), esimerkiksi siten, että henkilö olisi esittäytynyt pankissa väärennetyllä asiakirjalla toiseksi henkilöksi tai käyttänyt jonkun toisen henkilön oikeaa asiakirjaa tunnistautumisen yhteydessä, ja tätä väärää henkilöllisyyttä olisi käytetty Verohallinnon sähköissä palveluissa vahingonteko- tai hyötymistarkoituksessa?
5) Mitä toimia Verohallinnossa on tehty väärinkäytösten estämiseksi, jos tällaisiin tilanteisiin on törmätty?

Puhakainen vastasi, että Verohallinto on ottanut käyttöön ensimmäiset sähköiset palvelut 2000-luvun puolivälissä; veroilmoitus verkossa 2005 ja palkka.fi 2006. Verohallinnossa ei ole törmätty väärinkäytösyrityksiin siten, että väärä henkilö olisi yrittänyt suorittaa oikeustoimia sähköisesti toisen henkilön tiedoilla vahingonteko- tai hyötymistarkoituksessa. Vahingossa käyttämisiä on tiedossa parin tapauksen verran. Fyysisen toimintaympäristön puolella väärinkäytösyrityksiä on joitakin tapauksia viime vuosina. Verohallinnon sähköisiin palveluihin kirjaudutaan pankkitunnusten avulla 99 % ja muiden tunnisteiden avulla 1 % kirjautumisista.

#### 5.2.1.2 Kansaneläkelaitos

Kansaneläkelaitoksen eli Kelan sähköinen asiointipalvelu on julkishallinnon käytetyin, johon tunnistaudutaan noin miljoona kertaa kuukaudessa. Palvelussa lähetetään kuukausittain noin 280 000 etuushakemusta ja yli 50 000 liitettä, joten Kelan verkkoasioinnissa on suuret volyymit. Asiointipalveluiden käyttömäärä on kasvanut joka vuosi noin 25 %. Valtaosa Kelan etuuksista on haettavissa sähköisesti Kelan asiointipalvelun kautta. (Kansaneläkelaitos 2014.)

Kelan sähköistä asiointia koskien lähetin sähköpostitse kysymyksiä Kelan tietoturvapäällikkö Ville Taposelle helmikuussa 2014. Esittämäni kysymykset olivat hyvin samankaltaiset kuin Verohallinnollekin:
1) Milloin Kelassa on otettu käyttöön ensimmäiset sähköiset palvelut kansalaisille?

2) Onko Kelassa törmätty väärinkäytösyrityksiin siten, että väärä henkilö yrittää suorittaa oikeustoimia sähköisesti toisen henkilön tiedoilla vahingonteko- tai hyötymistarkoituksessa (esimerkiksi yritetty käyttää jonkun toisen henkilön pankkitunnuksia tunnistautumisessa tai kansalaisvarmennetta tai mobiilivarmennetta)? Minkä tyyppisiä nämä väärinkäytökset tai väärinkäytösyritykset ovat olleet, tai mitä hyötyä näillä väärinkäytösyrityksillä on pyritty saavuttamaan?
3) Kuinka iso osa sähköisiin palveluihin kirjautumisista tapahtuu pankkitunnusten avulla vs. kansalaisvarmenne (henkilökortti) tai mobiilivarmenne?
4) Onko Kelalle tullut vastaan väärinkäytösyrityksiä siten, että "pohjalla" olisi pankissa väärälle henkilölle myönnetty virtuaalinen henkilöllisyys (eli myönnetty pankkitunnukset), esimerkiksi siten, että henkilö olisi esittäytynyt pankissa väärennetyllä asiakirjalla toiseksi henkilöksi tai käyttänyt jonkun toisen henkilön oikeaa asiakirjaa tunnistautumisen yhteydessä, ja tätä väärää henkilöllisyyttä olisi käytetty Kelan sähköissä palveluissa vahingonteko- tai hyötymistarkoituksessa?
5) Mitä toimia Kelassa on tehty väärinkäytösten estämiseksi, jos tällaisiin tilanteisiin on törmätty?

Taponen vastasi, että Kela on aloittanut sähköiset asiointipalvelut vuonna 2005. Suurin osa kansalaisista tunnistautuu Kelan palveluihin verkkopankkitunnuksilla. Henkilökortilla ja mobiilivarmenteella tunnistautuminen on alle promille kokonaistunnistautumismäärästä. Keskinäisessä vertailussa henkilökortin käyttö jää alle puoleen mobiilitunnistamisen määrästä.

Taponen kertoi, ettei Kelalla ole kokemuksia tuottamuksellisesta vahingonteosta, joka liittyisi sähköiseen identiteettiin. Kelassa on ollut muutamia tapauksia, jossa jonkun perheenjäsenen verkkopankkitunnuksilla on yritetty hoitaa omia tai kolmannen perheenjäsenen asioita, joissa on pikemminkin ollut kyse perheen sisäisestä suostumuksesta tai työnjaosta, kuin vilpillisestä toiminnasta. Toisen puolesta sähköinen asiointi ei toistaiseksi ole mahdollista, mutta kehitys vie Kelassakin siihen suuntaan. Tällä hetkellä etuuskäsittelyn prosessissa on kontrolleja, joilla toisen puolesta sähköinen asiointi pystytään havaitsemaan ja ryhtymään tarvittaviin toimenpiteisiin, jotka ovat lähtökohtaisesti opastavia.

Taposen mukaan Kelalle ole tullut vastaan sellaisia väärinkäytösyrityksiä, joiden taustalla olisi esimerkiksi pankissa väärälle henkilölle myönnetty virtuaalinen henkilöllisyys. Kelalle asiakkaan sähköinen identiteetti on oikea, ellei toisin ilmoiteta tai varmenne ole sulkulistalla. Taponen totesi, että kehityksen kannalta nähtäväksi jää, onko valmisteilla olevasta EU:n tietosuoja-asetuksella vaikutusta tämäntyyppiseen tilanteeseen, sillä asetus tuo mukanaan henkilötietorikosten ilmoitusvelvollisuuden, jossa rekisterinpitäjä joutuu ilmoittamaan ainakin rekisteröidyille mahdollisesta väärinkäytöksistä.

### 5.2.2 Kansainvälisiä kokemuksia passin sähköisessä asioinnissa

Tämänhetkisten tietojen mukaan biometrisiin passeihin liittyvää osittaista tai kokonaan sähköistä asiointia on käytössä Kanadassa ja Uudessa-Seelannissa.

Sekä Kanadassa ja Uudessa-Seelannissa passin myöntämä viranomainen ei ole poliisi kuten Suomessa. Suomessa henkilöllisyyttä osoittavien asiakirjojen myöntäminen on katsottu osaksi poliisin ydintoimintaa, jolla on katsottu olevan myös merkittäviä vaikutuksia ennalta estävään toimintaan. Kanadan ja Uuden-Seelannin valtionhallinnoissa on henkilöllisyyttä osoittavia lupia varten omanlaisensa viranomaisrakenne, jolla on merkittävä funktio luvanmyöntämisen lisäksi tutkiessaan ja päättäessään myös henkilön oikeudesta kansalaisuuteen. Tällöin henkilöllisyyden osoittamiseksi vaaditaan lähtökohtaisesti huomattavasti enemmän dokumentaatiota, kun näiden maiden passin myöntöprosessissa kansalainen joutuu todistamaan samalla oikeutensa kyseiseen asiakirjaan. Syynä on se, ettei tietoa voida lähtökohtaisesti tarkistaa yhdestä luotettavasta rekisteristä. Jos menettelyä vertaa Suomeen, niin kansalaisen henkilöllisyys muodostuu käytännössä syntymän tai maahanmuuton kautta silloin kun henkilö merkitään väestötietojärjestelmään. Jos passia hakevaa henkilöä ei löydy väestötietojärjestelmästä, passimyöntöprosessi ei käynnisty, ja tällöin henkilön on asioitava ensin maistraatissa koskien väestötietojärjestelmämerkintöjään. Suomessa on yksi maailman parhaista ja kattavimmista väestötietojärjestelmistä (Id-ohjelma 2010, 21).

#### 5.2.2.1 Kanada

Kanadan passin sähköistä asiointia koskien lähetin tietopyyntöjä Kanadan valtionhallinnon kansalaisuus- ja ulkomaalaislupa-asioista vastaavalle apulaisjohtaja Justin Ikuralle tammikuussa 2014. Kysymykseni koskivat Kanadan passinmyöntöprosessia sekä siihen liittyviä riskejä, Kanadan viranomaistoimintaa sekä kokemuksia sähköisestä asioinnista.

Ikura kertoi, että Kanadan yksinkertaistettu passinuusimisprosessi sallii tiettyjen kriteerien täyttävien kanadalaisten uusia passinsa käyttäen yksinkertaistettua hakumenettelyä. Hakemuslomake kriteereineen on nähtävissä osoitteessa http://www.ppt.gc.ca/form/pdfs/pptc054.pdf. Hakijalta ei vaadita yhtä paljon tietoja ja pakollisia liitteitä hakuvaiheessa verrattuna normaalimenettelyyn, jos hakija on oikeutettu yksinkertaistettuun uusimismenettelyyn. Hakemus voidaan täyttää osittain verkossa, mutta se vaatii silti käynnin valtionhallinnon omassa Passport Programin lupatoimistossa, hakemuksen lähettämistä postitse tai käyntiä valtionhallinnon sopimuskumppanin eli Kanadan Postin toimistossa. Kanada on ottanut biometriset passit käyttöön kesäkuussa 2013. Kanadassa käytettiin yksinkertaistettua passinuusimismenettelyä jo ennen biometristen passien käyttöönottoa.

Noin 30 % Kanadassa tai Yhdysvalloissa asuvista kanadalaisista lähettävät passihakemuksena postin välityksellä. Postitetut hakemukset keskitetään Passport Canada Program:n käsittelykeskukseen tutkimuksia varten. Postitusmahdollisuus on erityisen hyödyllinen niille kanadalaisille, jotka asuvat Kanadan syrjäseuduilla. Postitusmahdollisuudesta huolimatta suurin osa kanadalaisista jättää passihakemuksensa paikallisessa passinmyöntötoimistossa tai Kanadan Postin tai Service Canadan valtuutetussa toimistoissa, joissa he voivat hyödyntää henkilökohtaista palvelua. Kanadalaiset voivat asioida joko 34:ssä täyden palvelun Passport Program toimipisteessä, tai 144:ssä Service Canada toimipisteessä, tai 46:ssa Kanadan Postin toimipisteessä jotka tarjoavat valtuutetusti palvelua passinhakuun liittyen. Tällä hetkellä valtuutetut pisteet voivat ottaa vastaan ainoastaan yksinkertaisia hakemuksia, ja heidän tehtävänään on tarkistaa, että hakemus on täytetty oikein. Valtuutetut toimipisteet eivät kuitenkaan voi käsitellä tai myöntää passeja, jolloin tarkastetut hakemukset välitetään varsinaisiin Passport Programin toimipisteisiin käsiteltäviksi ja päätettäviksi. Ulkomailla (pl. Yhdysvallat) asuvat kanadalaiset asioivat passinhaussaan Kanadan lähetystöissä, jotka toimivat yhteistyössä Passport Canada Programin kanssa passiasioihin liittyvissä hakemuksien hyväksymisessä, tutkimisessa ja päätöksenteossa. (Ikura 2014.)

Ikuran toimittamien tietojen perusteella Kanadassa varmistetaan passia myönnettäessä henkilöllisyys, kansalaisuus, matkustamisrajoitukset ja turvallisuuteen liittyvät asiat. Kanadan passinmyöntöprosessi nojautuu:

- asiakirjavaatimuksiin (kansalaisuuden osoittaminen, henkilöllisyyden osoittaminen, vanhemmuuden osoittaminen)
- suosittelijoihin ja laillisiin takaajiin (jotka ovat jo passinhaltijoita)
- kokoelmaan sosiaalisen elämän jalanjäljistä (työllisyys, asumishistoria, äidin tyttönimi)
- päätöksentekijän taitoihin (dokumenttien analysointi, kasvojenvertailu, haastattelutaidot)
- dokumenttien laillisuuden varmistamiseen
- kasvojentunnistusohjelmiston hyödyntämiseen
- rikollisen toiminnan havaitsemiseen.

Yksinkertaistettuun passinuusimismenettelyyn oikeutettujen kanadalaisten ei tarvitse yleensä osoittaa kansalaisuustodistusta tai vastaavaa kansalaisuutta osoittavaa dokumenttia, eikä heillä tarvitse olla hakemuksen laillista takaajaa tai allekirjoituksella varmennettua passikuvaa (nämä menetelmät ovat varsinaisen passinhakumenettelyn osia, joita käytetään hakijan oikean identiteetin takaamiseen). Pääosin uusimismenettelyn piirissä olevat kansalaiset tunnistetaan passinmyöntörekisterin tai aikaisemman passin avulla sekä hakemuslomakkeen tietojen perusteella, sekä hakemuslomakkeella oleviin referensseihin yhteyttä ottamalla. Yksinkertaistettu passinuusimismenettely edellyttää aiemmin myönnettyä passia. Uuden hakemuk-

sen kuvaa verrataan aina edellisen passin kuvaan myös koneellisen kasvojenvertailun avulla, sekä kasvoja verrataan kaikkiin passikuvarekisterissä oleviin kuviin. Passport Program saa tarvittaessa lisätietoja yksittäisten tutkinnan kohteena olevien kohdalla Kanadan poliisin tietokeskuksesta (CPIC), joka on yhteydessä mm. Interpoliin. Passport Program toimii myös yhteistyössä Correctional Services Canadan kanssa, joka toimii tiedonlähteenä esimerkiksi vangittavien tai oikeuden päätöksellä matkustuskieltoon tai -rajoituksiin asetettujen henkilöiden osalta. (Ikura 2014.)

Ikura totesi myös, että Kanadassa on kohdattu väärinkäytösyrityksiä passinhakumenettelyssä. Useimmiten väärinkäytöstä yritetään jonkun toisen oikealla henkilöllisyydellä. Kanadassa havaittuja väärinkäytösyrityksiä on yritetty seuraavin menetelmin:

- Henkilöllisyyden kaappaaminen: henkilö kaappaa olemassa olevan, elävän tai kuolleen henkilön, henkilöllisyyden
- Henkilöllisyyden luominen: henkilö luo fiktiivisen tai teennäisen henkilöllisyyden
- Henkilöllisyyden manipuloinen: henkilö muokkaa yhtä tai useampaa elementtiä omasta henkilöllisyydestään
- Henkilöllisyyden kaappaus ja manipulaatio: henkilö kaappaa olemassa olevan henkilöllisyyden ja muokkaa yhtä tai useampaa elementtiä henkilöllisyydestä

Suurimmassa osassa tapauksista huijari on yrittänyt kaapata olevassa olevan kanadalaisen henkilöllisyyden. Hakemuksen liitteenä on usein oikea kuva huijarista, aito syntymätodistus ja toissijainen tunnistus, jolloin vaatimukset sekä oikeudesta henkilöllisyyteen että henkilöllisyyden osoittamisesta täyttyvät. Harvemmissa tapauksissa, saatuaan käsiinsä henkilöllisyyden, huijari yrittää muuttaa nimeään passia vastaavaksi laillisin keinoin.

Ikura totesi, että Kanadassa on myös tavattu passinhaltijoita, jotka käyttävät omaa passiaan väärin, tai antavat oman passinsa toiselle väärinkäytettäväksi. Tähän on vaikeaa passinmyöntämisprosessin näkökulmasta puuttua, koska virheet tapahtuvat varsinaisen passinmyöntöprosessin jälkeen. Näissä väärinkäytöstapauksissa passin edelleen välittänyt henkilö jää kuitenkin yleensä kiinni uutta passia haettaessa.

Ikuran mukaan Kanadan Passport Program Integrity Branch suorittaa tutkintaa henkilöllisyyteen, passin väärinkäyttöön ja vääriin todistuksiin liittyen. Kanadan passilaki antaa Passport Program:lle toimivallan suorittaa hallinnollisia sanktioita niitä passinhaltijoita kohtaan, jotka ovat toimineet väärin. Keinoja ovat kielteinen päätös passin myöntämisestä, passin peruuttaminen tai kieltäytyminen antamasta palveluja passin myöntämiseksi maksimissaan viiden vuoden ajalle.

#### 5.2.2.2 Uusi-Seelanti

Uuden Seelannin passiasioiden sähköistä asiointia koskien esitin kysymyksiä sähköpostitse Business Support Officer Lesley Tse:lle (Passports Uruwhenua, Department of Internal Affairs Te Tari Taiwhenua). Kysymykset koskivat passinmyöntöprosessia, siihen liittyvää viranomaistoimintaa sekä heidän havaitsemiaan tai kokemiaan riskejä koskien passien sähköistä asiointia.

Tse kertoi, että Uuden Seelannin Department of Internal Affairs on antanut yli 16 vuotiaiden uusiseelantilaisten uusia passinsa täysin sähköisen menettelyn avulla 2.11.2012 alkaen. Kasvojentunnistusteknologian hyödyntäminen tukee merkittävimmin sähköistä prosessia. Kasvojen tunnistamista pidetään avainasemassa passin myöntöprosessin turvallisuudessa.

Tse kertoi, että passinmyöntöpalvelu hyödyntää 1:1 kasvojenvertailua hakijan aiemman passikuvan ja hakemuksen yhteydessä toimitetun passikuvan välillä, ja tämä on prosessin merkittävin vaihe henkilöllisyyden varmistamisessa. Jotta kasvokuvien vertailua voidaan käyttää tehokkaasti, Uudessa Seelannissa panostettiin merkittävästi aikaa ja resursseja tietojärjestelmän siivoamiseen. Siivoamisen myötä poistettiin huonolaatuisia kasvokuvia, yhdistettiin päällekkäisiä tietoja, tunnistettiin henkilöllisyyteen liittyvää rikollista toimintaa ja muovattiin riskiprofiileja. Tietojärjestelmän siivoaminen auttoi myös harjoittelemaan 1:1 kasvokuvien vertailua sekä kuvan vertaamista moneen kuvaan ennen varsinaista sähköisen asioinnin käyttöönottoa (ns. yksi moneen vertailu). Kaikkien passien uusimisen kohdalla 70 % kuvista on täsmännyt aiempaan passikuvaan. Lopuissa 30 % syinä on ollut tietojärjestelmän kyvyttömyys verrata aiempaan kuvaan (kuva ei täyttänyt etukäteen määriteltyjä vaatimuksia) sekä se, ettei järjestelmä ole pystynyt käyttämään aiempaa kuvaa (laadun tai kuvan iän vuoksi).

Tse totesi, että Uudessa Seelannissa on havaittu yksi huijausyritys, jossa henkilö yritti anoa passia toisen henkilön tiedoilla, mutta omalla kuvallaan. Uudessa Seelannissa ei ole tietoa, että mikään muu maa käyttäisi parhaillaan samankaltaista sähköistä passin uusimismenettelyä.

### 5.2.3 Riskien kartoittaminen Lupa2016-hankkeen näkökulmasta

Riskejä Suomen passien myöntämiseen liittyvässä sähköisessä asioinnissa kartoitettiin ryhmähaastattelun avulla, jonka myös tallensin äänitteenä älypuhelimella. Ryhmähaastattelu oli keskustelunomainen. Osanottajat kommentoivat asioita melko spontaanisti, tekivät erinäisiä huomioita ja tuottivat monipuolista tietoa käsillä olleesta aiheesta.

Ryhmähaastattelussa olivat läsnä Poliisihallituksen Lupa2016-hankkelta hankepäällikkö Mika Hansson, projektipäällikkö Eero Konttaniemi sekä projektipäällikkö Kari Kanto. Kaikilla kol-

mella on vuosien kokemus poliisin lupahallinnosta ja passin myöntämiseen liittyvistä asioista. Erityisosaamisalueenaan Hanssonilla on varmenteet ja biometria, Konttaniemellä poliisin tietojärjestelmät ja niiden käsittelyprosessit, sekä Kannolla erityisesti sähköiseen asiointiin ja passivalokuviin liittyvä erityisosaaminen. Ryhmähaastattelu pidettiin Poliisihallituksen neuvottelutiloissa 13.3.2014 iltapäivällä. Haastattelu kesti lähes 1,5 tuntia.

Alussa keskusteltiin siitä, mitä työn julkisuusnäkökulman vuoksi voidaan nostaa riskeinä esiin, jottei esiin tuodut riskit kannusta tai alenna kynnystä yrittää väärinkäytöksiä. Todettiin, että suurin osa havaituista riskeistä on julkista tietoa.

Todettiin, että sähköistä asiointia koskevien väärinkäytösten lähtökohtana on oltava joka tapauksessa luonnollinen henkilö. Muutoin kirjautuminen sähköiseen asiointipalveluun ei ole mahdollista, koska se perustuu Väestötietojärjestelmästä (VTJ) saatuihin tietoihin. Jos verrataan tilannetta Kanadan väärinkäytösyritysten vaihtoehtoihin, niin Suomen tilanne on selkeämpi, sillä mikäli näitä tietoja haluttaisiin muuttaa, (edes osittain,) olisi se tehtävä Maistraatissa, jotta ne päivittyisivät VTJ:n puolelle. Lisäksi tietojen osittaisestakaan muuttamisesta on vaikea nähdä siitä saavutettavaa hyötyä, sikäli kun on tarkoitus kaapata jonkun toisen henkilöllisyys väärinkäytöstarkoituksessa.

Aloitimme keskustelun pohtimalla vääriin käsiin päätyvää varmennetta (kansalaisvarmenne, mobiilivarmenne tai verkkopankkitunnukset), jonka todettiin olevan merkittävä riski. Anastetun varmenteen avulla voidaan kirjautua kyseisen kansalaisen asiointitilille suorittamaan erilaisia oikeustoimia, kuten anoa passia, mikäli henkilö on oikeutettu passien kevennettyyn hakemusmenettelyyn. Esimerkiksi lompakon varastamisen yhteydessä voitaisiin käyttää lompakosta löytyneitä verkkopankkitunnuksia (mikäli lompakosta löytyisi sekä käyttäjätunnus, salasana että vaadittava avainlukulista tms.) väärin ennen kuin niiden varsinainen haltija huomaisi niiden kadonneen ja ilmoittaneen pankkiin niiden katoamisesta. Sama pätee myös muihin varmenteisiin. Uhkakuvana on myös varmenteen hankkiminen esimerkiksi ajokortin tai lompakosta löytyvän muun henkilöllisyyden osoittamiseksi kelpaavan asiakirjan avulla, jolloin saataisiin tarpeeksi samannäköisen henkilön avulla pankista verkkopankkitunnukset tai puhelinoperaattorilta mobiilivarmenne. Haltuun saadulla varmenteella voitaisiin kirjautua sähköiseen asiointipalveluun. (Tokikin teoriassa olisi mahdollista yrittää hakea myös poliisilta henkilökorttia ja sen myötä kansalaisvarmennetta, mutta yritys olisi hyvin riskialtis ottaen huomioon, että poliisi saattaa olla tietoinen lompakon varastamisesta ja henkilön ei kuuluisi läpäistä poliisin tunnistamismenettelyä.) Mikäli väärinkäytöstä yrittävä huomaisi, että kaapatun henkilöllisyyden omaava henkilö on passin kevennetyn hakemusmenettelyn piirissä, voisi väärinkäytöstä yrittävä yrittää hakea uutta biometrista passia kyseisen henkilön tiedoilla ja esimerkiksi oikealla kasvokuvalla (vaikkapa lompakosta tai internetistä löytyneellä kyseisen henkilön valokuvalla) tai väärällä kasvokuvalla (kuten väärinkäytöstä yrittävän omalla tai passia

tarvitsevan henkilön valokuvalla). Todettiin, että sähköisesti asioidessa kasvokuva on ainoa tieto minkä passista voi vaihtaa. Syitä passin hankkimiseksi toisen henkilön VTJ-tiedoilla voivat olla esimerkiksi:

- passin edelleen myyminen
- toisen henkilöllisyyden kaappaaminen matkustustarkoituksessa (edellyttäen, ettei henkilö tiedä, että hänen tiedoillaan on haettu mahdollisesti uusi passi, ja/tai edellyttäen ettei poliisi tiedä henkilön henkilöllisyyden olevan anastettu)
- henkilöllisyyden kaappaaminen rahallisista syistä tai oikeustoimien suorittamiseksi vaikkapa kiusantekotarkoituksessa.

Oman riskinsä muodostavat myös sähköisen asioinnin kautta poliisille toimitettavat liitteet ja niiden aitouden arviointi. Mikäli passin myöntöön liittyy erityisvaatimuksia, esimerkiksi asevelvollisuuden osoittamiseksi, on sähköiseen asiointiin suunniteltu toiminnallisuutta, jossa hakija voi liittää tarvittavat liitteet hakemuksen yhteyteen. Näiden liitteiden oikeellisuuden tarkastaminen ja arvioiminen ovat tärkeä osa päätöksentekoprosessia, ja asia on otettava lupahallinnon henkilöstöä koulutettaessa erityisesti huomioon.

Riskeistä keskusteltaessa todettiin, että hakijan tunnistaminen ja hakijan kuva ovat kriittisimmät vaiheet passin myöntämisessä poliisin näkökulmasta passien kevennetyssä hakemusmenettelyssä. Erityisen merkityksellisiä ne ovat siksi, koska passit toimitetaan valtaosin suoratoimituksena R-kioskin kautta asiakkaalle, eikä poliisi tunnista henkilöä enää uudelleen passia luovutettaessa. Täten hakijan tunnistamisen merkitys on selkeästi poliisin henkilöstön koulutuksessa painotettava asia.

Haastattelussa todettiin, että erityisen hankalaksi tilanteen tekee, jos sähköinen henkilöllisyys on luovutettu vapaaehtoisesti väärin käytettäväksi. Tämä tosin on rangaistava rikos. Myös sähköinen toimintaympäristö saattaa laskea kynnystä väärinkäytösten yrityksiin.

### 5.2.4 Riskit kansalaisoikeusnäkökulmasta

Passin sähköistä asiointia koskevassa riskien kartoittamisessa mennään melko syvälle viranomaistoimintaan ja siihen liittyviin prosesseihin. Tämän vuoksi tulin siihen tulokseen, että kansalaisoikeusnäkökulmaa varten minun tulisi selvittää näkemyksiä riskejä kohtaan erityisin haastatteluin, joille poliisin toiminta ja kansalaisoikeusnäkökulmista huolehtiminen ovat lähtökohtaisesti tutumpia. Siksi päätin valita haastattelukohteiksi Tietosuojavaltuutetun toimiston ja Electronic Frontier Finland ry:n (EFFI). EFFI:lle esitin kysymyksiä sähköpostitse välimatkan takia.

#### 5.2.4.1 Tietosuojavaltuutetun toimisto

Yksilöhaastattelussa haastattelin Tietosuojavaltuutetun toimiston ylitarkastaja Heikki Huhtiniemeä koskien riskejä Suomen passin myöntämiseen liittyvässä sähköisessä asioinnissa erityisesti kansalaisen oikeusturvanäkökulmasta. Haastattelu pidettiin Tietosuojavaltuutetun toimiston tiloissa 21.3.2014 iltapäivällä. Haastattelu kesti noin 1,5 tuntia.

Huhtiniemi totesi, että kansalaisten näkökulmasta poliisin kehitys sähköisen asioinnin saralla on erittäin toivottavaa. Kuitenkin on huomioitava, että sähköinen asiointi on vain osa prosessia, jossa lopulta korostuu ihmistyön merkitys päätöksentekovaiheessa. Koska tunnistaminen kulminoituu kasvokuvaan ja niiden vertailuun, ja sähköisessä asioinnissa fyysinen asiakaskontakti puuttuu kokonaan, on erityisen tärkeää kouluttaa henkilöstöä havaitsemaan ne tilanteet, missä väärinkäytöstä yritetään. Tämä vaatii päätöksentekijältä arviointikykyä sen suhteen, ketkä henkilöt pitää pyytää käymään poliisilaitoksella esimerkiksi tunnistamisen varmistamiseksi ja päätöksenteon loppuun saattamiseksi. Huhtiniemen mukaan riskinä on, että varsinaisen asiakirjan vääriin käsiin päätymisen lisäksi vaarana on myös aiemmin kerättyjen passisormenjälkien päätyminen väärän passin sirulle. Kansalaisen oikeusturvaa palvelevat parhaiten turvallinen asioimisväylä, onnistunut riskitilanteiden tunnistaminen sekä laadukas henkilöstön koulutus ja riskiarviointi.

Haastattelussa kävimme läpi väärinkäytösten mahdollisuuksia sähköisessä asioinnissa. Käytännössä ne perustuvat aina siihen, että joku toinen varastaa jonkun toisen henkilön oikeat tiedot, koska kuvitteellisella henkilöllisyydellä ei pystytä asioimaan sähköisessä asiointipalvelussa. Huhtiniemi jakoi saman huolen kuin poliisi siitä, että internet toimintaympäristönä saattaa alentaa kynnystä väärinkäytösyrityksille. Mikäli passipäätöstä valmistelevalle virkailijalle tulee erityisesti kasvokuvavertailussa pientäkään epäselvyyttä hakijan tunnistamisen suhteen, niin hakija pitäisi kutsua paikalle. Kynnys tähän pitäisi olla virkailijan päästä matala.

Yhteisesti todettiin, ettei kehitys saa johtaa siihen, että Suomen kansalaisten silmissä ja kansainvälisellä mittapuulla luotettava passi menettäisi arvoaan porsaanreikiä sisältävällä sähköisen asioinnin ratkaisulla. Tämä johtaisi myös kehittämistoimissa askelia taaksepäin, jolloin palveluihin jo satsattu kehittäminen menisi hukkaan. Myös passin luotettavuus kärsisi kovan kolauksen.

Huhtiniemi piti tärkeänä, että kansalaisia on tiedotettava sähköiseen asiointiin liittyvistä käytänteistä. Haastattelun lomassa kerroin, että kevennetyn hakemusmenettelyn aikataulun varmistuessa tiedotuskampanjan aikataulusta päätetään. On kaikkien etu, että asiasta tiedotetaan mahdollisimman ytimekkäästi mutta informatiivisesti. Tietosuojavaltuutetun toimisto saa paljon sähköiseen asiointiin liittyviä kysymyksiä kansalaisilta.

Huhtiniemi nosti esiin, että sähköisen asioinnin sijaan vaihtoehtona olisi voinut olla myös passinmyöntöprosessin ulkoistaminen yhteispalvelupisteisiin. Tämä olisi kuitenkin vastoin poliisin strategisia linjauksia, jossa virallisten henkilöllisyyttä osoittavien asiakirjojen myöntäminen ja siihen liittyvä tunnistaminen on katsottu olevan yksi poliisin lupahallinnon ydintehtävistä. Huhtiniemen mielestä kansalaisten hyvän oikeusturvan toteutumisen tulkinta on sama kuin poliisilla, eli oikea ihminen saa oikean passin, ja sen hakeminen on mahdollisimman turvallista niin sähköisessä kuin fyysisessä prosessissa. Tästä poliisin kuuluukin huolehtia.

Huhtiniemi totesi, että Tietosuojavaltuutetun toimisto on nostanut jo aiemmin esiin erityisesti mobiilivarmenteen myöntämiseen liittyvät mahdolliset puutteet tai heikkoudet. Onkin aiheellista kysyä onko tarkoituksenmukaista, että esimerkiksi ajokorttia käyttämällä henkilöllisyyden osoittamiseksi saadaan vahvempi virallinen sähköinen henkilöllisyys sähköiselle toimintakentälle.

Huhtiniemi piti erityisen hyvänä kehityssuuntana sitä, että lupahallinnon henkilöstölle on ryhdytty tarjoamaan Poliisiammattikorkeakoulun järjestämää ammatillista tutkintoa muun koulutuksen lisäksi. Lupahallinnon arvostuksen nostamiseksi ja työn merkityksen korostamiseksi koulutukseen panostamisella on varmasti hyötyä pitkällä aikajänteellä.

Haastattelun lopuksi todettiin, että koko prosessin turvallisuus nojautuu turvalliseen tunnistamiseen, joka tulee olla kaiken luvanmyönnön perusta huolimatta siitä missä toimintaympäristössä lupaa on haettu. Tunnistamisprosessi pitäisi olla kunnossa kansalaisten edun nimissä niin viranomaisten kuin yksityisellä puolella, ja tunnistamisen pohjana tulisi käyttää niitä asiakirjoja, joissa poliisi on suorittanut henkilön ensitunnistamisen.

#### 5.2.4.2 Electronic Frontier Finland ry

Riskien kartoittamisessa kansalaisnäkökulmasta lähetin sähköpostitse kysymyksiä Electronic Frontier Finland ry:n puheenjohtaja Timo Karjalaiselle 22.3.2014. Kerroin Karjalaiselle pohjatietoa käsillä olevasta asiasta, poliisin sähköisen asioinnin tulevaisuudensuunnitelmista sekä sähköisen asiointipalvelun toimintaperiaatteista. Kysyin, miten Karjalainen suhtautuu viranomaisten tarjoamiin sähköisiin palveluihin kansalaisille ja poliisin sähköisen palvelutarjonnan laajentumiseen. Kysyin Karjalaiselta, onko tunnistamiseen tarjottu vaihtoehtovalikoima kansalaisnäkökulmasta riittävä, vai toivoisiko hän, että vaihtoehtoja olisi enemmän, ja kysyin myös onko tunnistautumistavalla ylipäätään merkitystä kansalaisnäkökulmasta. Kysyin Karjalaiselta myös mitä mieltä hän on siitä, että lain tasolla on katsottu varmenteen myönnön olevan mahdollista myös muun kuin viranomaisen toimesta, ja siitä, että henkilöllisyyden todentamisessa passin ja henkilökortin lisäksi kelpaa myös ajokortti. Kysyin myös onko Karjalainen

huolissaan siitä, että sähköisten viranomaispalvelujen yleistyessä myös identiteettivarkaudet tai niiden yritykset saattavat lisääntyä sähköisen asioinnin puolella. Lisäksi kysyin pitäisikö viranomaisen parantaa mahdollisuuksia ilmoittaa henkilöllisyyttä osoittavia asiakirjoja tai siihen tarkoitukseen yleisesti hyväksyttyjä asiakirjoja varastetuksi tai hävinneiksi. Lopuksi kysyin millaisia kehittämisehdotuksia Karjalaiselle tulee mieleen, jotta kansalaisen asema voidaan parhaalla mahdollisella tavalla turvata myös poliisin sähköisessä viranomaisasioinnissa ja erityisesti passinhaun tapauksessa.

Karjalaisen mukaan sähköinen asiointimahdollisuus pitäisi olla jo arkipäivää 2010-luvulla, ja on hyvä, että poliisikin on tulossa tältä osin nykyaikaan. Karjalaisen mielestä kansalaisen näkökulmasta olisi vaivatonta, mikäli passivalokuvien toimittamisessa olisi mahdollisuus otattaa kuva poliisilaitoksella käydessä silloin, kun kansalainen joutuu asioimaan henkilökohtaisesti poliisilaitoksella lupa-asiassaan. Vastasin Karjalaiselle, että passikuvien toimittamisen uudistuksen tarkoituksena oli vähentää työn määrää poliisin lupapalveluissa, koska aiemmin kaikki passihakemuksen yhteydessä toimitetut kuvat skannattiin hakemuksen jätön yhteydessä. Skannauksen yhteydessä kuvan laatu myös heikkenee. Koska asiakkaan valokuvaaminen ei ole poliisin ydintoimintaa ja palvelu on ulkoistettavissa (ja on aina ollut ulkoistettuna) alan ammattilaisille, joilla on laitteiden, koulutuksen ja kuvausolosuhteiden kannalta huomattavasti paremmat edellytykset ottaa laadukkaita kuvia kuin poliisilla, kuvausta ei ole haluttu siirtää yksityisiltä elinkeinonharjoittajilta poliisille. Vastauksessani Karjalaiselle toin myös esiin, ettei kokonaista elinkeinoa voida siirtää viranomaiselle kevyin perustein. Passikuviin liittyen Karjalainen toi esiin huolenaiheena vakavan loukkauksen kansalaisen yksityisyydelle, mikäli valokuvaamo lähettää ottamansa passikuvat viranomaisen arkistoon automaattitoimenpiteenä, josta asiakas ei voi kieltäytyä. Poliisi on tällaisen toiminnan ohjeistuksessaan kieltänyt. Karjalaisen mukaan kiellon toteutumista olisi hyvä valvoa.

Karjalaisen mielestä varmenteiden tarjonnan valikoima vaikuttaa riittävältä. Tunnistautumistavalla on lähinnä merkitystä siten, että mahdollisimman monelta löytyisi vähintään jokin tarjolla oleva vaihtoehto. Karjalainen muistutti, että vaikka käytännössä verkkopankki lienee ylivoimaisesti käytetyin vaihtoehto Suomessa, niin sitäkään ei aivan kaikilla ole.

Ajokortin käytöstä tunnistamisasiakirjana Karjalainen totesi, että hän on ihmetellyt ajokortin kelpaamattomuutta, koska pahimmillaan sama poliisilaitos, joka on ajokortin myöntänyt, ei itsekään ole uskonut myöntäneensä ajokorttia oikealle henkilölle kun on haettu henkilökorttia. Päällekkäisyyksien vähentämiseksi Karjalaisen mielestä olisi hyvä asia, että ajokortilla voisi tunnistautua. Tilannehan on eittämättä hullunkurinen kansalaisen näkökulmasta, mutta riskeistä ajokortin käytöstä tunnistamisasiakirjana on avattu enemmän kappaleessa 4.2.2., ja esitin tietoa asiasta vastauksessani Karjalaiselle.

Karjalainen ei nähnyt periaatetasolla ongelmaa siinä, että sähköisen varmenteen on myöntänyt jokin muu kuin viranomainen, mutta tässä tulee arvioitavaksi tunnisteen myöntäjän luotettavuus, joka ei suomalaisissa pankeissa perinteisesti ole ollut ongelma.

Karjalaisen mielestä on täysin selvää, että sähköisten viranomaispalvelujen yleistyessä myös identiteettivarkaudet tai niiden yritykset tulevat lisääntymään sähköisen asioinnin myötä jo yksistään siitä syystä, että palveluiden ja niiden käyttäjien määrä kasvaa huimasti. Karjalainen ei kuitenkaan usko, että identiteettivarkauksista muodostuu vakavaa ongelmaa, kunhan toimitaan perustasolla järkevästi ennaltaehkäisyn suhteen sekä toisaalta jälkiselvittelyn tulee olla kohtuullista uhrin näkökulmasta.

Kysyin Karjalaiselta, pitäisikö ihmisiä kehottaa pitämään enemmän erityistä huolta jo myönnetyistä varmenteista ja esim. niistä tunnistamisasiakirjoista, joiden avulla varmenteita voidaan hankkia, ja jos kyllä, niin miten. Karjalainen vastasi, että yleisenä valistuksena omista tiedoista ja tietoja sisältävistä korteista, papereista ym. hyvän huolen pitäminen on tietenkin paikallaan, mutta tällä ei voida ratkaista identiteettivarkauksien ongelmaa. Karjalainen toi esiin huolensa siitä, että erityisesti syyllisyyttä omien henkilötietojen käytöstä toisen tekemässä petoksessa tms. rikoksessa ei saa kaataa identiteettivarkauden uhrin niskaan, ellei ole kyse tarkoituksella luovutetuista tiedosta.

Karjalainen totesi, että viranomaiset voisivat parantaa mahdollisuuksia ilmoittaa henkilöllisyyttä osoittavia asiakirjoja tai siihen tarkoitukseen yleisesti hyväksyttyjä asiakirjoja varastetuksi tai hävinneiksi. Pankeilla ja luottolaitoksillahan tietysti on omia ilmoituskanaviaan, jotka ovat valitettavan hajanaisia ja potentiaalisesti vaikea löytää juuri sillä hetkellä kun tarvittaisiin. Karjalainen esitti, että jokin 112-hätänumeron vastine - yksi keskitetty palvelu johon voisi ilmoittaa minkä tahansa kortin, tunnusten tai varmenteen katoamisen - voisi olla hyvä kehitysidea. Tämän palvelun yhteystietoja voitaisiin mainostaa niin monessa paikassa, että siitä tulisi yleistietoa vastaavasti kuin 112-numero on.

## 5.3 Riskienhallinnan toimintamalli

### 5.3.1 Havaitut riskit ja niiden luokittelu

Haastattelujen sekä erinäisten tiedonkeruumenetelmien perusteella muodostin kokonaiskäsityksen niistä passien sähköistä asiointia koskevista riskeistä, joiden julkituominen ei ole salassapitosäännösten vastaista. Luokittelin havaitut riskit eri riskityyppeihin. Ylätasolla riskityypit kuuluvat poliisin riskimallin mukaisiin hankeriskeihin.

Keskeisimpiä havaittuja julkisia riskejä ovat:

1. OSAAMIS- JA PROSESSIRISKIT
    - Haasteiksi voi muodostua sähköisen asioinnin ja jo aiemmin toteutetun passien suoratoimituksen mukanaan tuomat prosessimuutokset, joiden johdosta passin kevennetyssä hakemismenettelyssä prosessin turvallisuus kulminoituu henkilön tunnistamiseen ja valokuvien vertailuun. Keskeistä on poliisilaitoksen henkilöstön kyky havaita väärinkäytösyrityksiä: kasvokuvien vertailu ja mm. sähköisen asioinnin kautta tulevien hakemusten liitteiden aitouden ja eheyden varmistaminen voi olla vaikeaa, jolloin päätöksentekijän osaamiselle asetetaan korkeita vaatimuksia. Riskinä on, että myönnettäisiin aito biometrinen passi toisen henkilön oikeilla tiedoilla ja sormenjäljillä, mutta väärällä kuvalla ja väärälle henkilölle, tai väärennettyjen liitteiden avulla hakija saavuttaisi sellaista hyötyä, joka ei olisi normaalissa fyysisessä prosessissa mahdollista.
    - Passien ja henkilökorttien myöntömäärien jatkuva kasvu; muistetaanko tunnistamisen tärkeys?
2. LAINSÄÄDÄNTÖRISKIT
    - Erilaisten varmenteiden myöntämisen pohjalla käytettävät tunnistamisasiakirjat eivät ole välttämättä poliisin takaamia virallisia henkilöllisyyttä osoittavia asiakirjoja, vaikka tarjottavan varmenteen asema sähköisessä toimintaympäristössä olisikin vahva - eli ns. "vähemmällä saadaan enemmän", kuten ajokortilla pankkitunnusten tai mobiilivarmenteen kautta passi.
3. ASIAKASRISKIT
    - Varmenteiden päätyminen esimerkiksi varastamisen vuoksi vääriin käsiin ja siten henkilötietojen päätyminen vääriin käsiin.
    - Väärinkäytösyritysten yleistyminen sähköisen toimintaympäristön alentaessa kynnystä toimimiselle.
4. MAINERISKIT
    - Epäonnistumisten myötä kansalaisten arvostus poliisin toimintaa ja kehittämishankkeita kohtaan laskee.
    - Kansainväliselläkin mittapuulla erittäin korkealle luotettu ja arvostettu Suomen passi menettää arvoaan väärinkäytöstapausten vuoksi, jonka johdosta myös suomalaisten matkustaminen voi pahimmassa tapauksessa vaikeutua.

### 5.3.2 Havaittujen riskien arvioiminen

Seuraavaksi arvioin riskien todennäköisyyttä ja vaikuttavuutta haastattelujen ja tietojenkeruun perusteella sekä poliisin riskienhallintatyökalun periaatteiden mukaisesti:

| Todennäköisyyden arviointi | | | | | |
|---|---|---|---|---|---|
| Lähes varma | 4 | | | | |
| Todennäköinen | 3 | | Asiakasriskit (6) | | Osaamis- ja prosessiriskit (12) |
| Mahdollinen | 2 | | | Lainsäädäntöriskit (6) | |
| Epätodennäköinen | 1 | | | Maineriskit (3) | |
| | | 1 | 2 | 3 | 4 |
| | | Vähäinen | Kohtalainen | Merkittävä | Kriittinen |
| | | Vaikutuksen arviointi | | | |

**Maineriskien** riskituloksi muodostui 3. Maineriskien vaikutuksen arvioin merkittäväksi, mutta kuitenkin epätodennäköiseksi. Poliisin henkilöstön ammattitaidon pitäisi jossakin määrin jopa rapautua, jotta ongelma pääsisi niin pahaksi, että toistuvat epäonnistumiset vaikuttaisivat poliisin maineeseen kansallisesti tai suomalaisen passin luotettavuuteen kansainvälisesti.

**Asiakasriskien** riskituloksi muodostui 6. Arvioin näiden riskien olevan todennäköisiä, mutta vaikutukseltaan kohtalaisia, koska passinmyöntöprosessissa ammattitaitoisten virkailijoiden tehtävänä on havaita väärinkäytösyritykset.

**Lainsäädäntöriskien** riskituloksi muodostui 6. Arvioin ne merkittäviksi ja mahdollisiksi, koska nykylainsäädännön mahdollistama vahvojen sähköisten tunnisteiden myöntäminen ajokortin avulla on iso riski sähköisessä toimintaympäristössä toimiville. Poliisin pitäisi kuitenkin selviytyä näistä lainsäädännön pohjalta kumpuavista riskeistä osaamis- ja prosessiriskien hallinnan avulla.

Punaiselle alueelle riskienhallintatyökalussa päätyi arviointini mukaisesti osaamis- ja prosessiriskit. **Osaamis- ja prosessiriskit,** riskituloltaan 12, arvioin todennäköisiksi, koska passeja myönnetään niin paljon, että inhimillisille tunnistamiseen liittyviin virheisiin täytyy varautua - ja näitä on käynyt aikojen saatossa myös nykyisen fyysisen prosessin puolella. Viimeisin tapaus nousi keltaisen lehdistön tietoon huhtikuun alussa 2014, jossa passia hakeneelle henkilölle ilmeni noudettuaan passinsa läheiseltä R-kioskilta, että passin henkilötiedot olivat hänen, mutta kuva oli eri henkilön. Taustalta löytyi passivalokuvaamon tekninen ratkaisu passikuvien toimittamiseksi poliisille, mutta poliisin virkailijan tulisi aina verrata hakijan kasvoja esitettyyn kuvaan, ja sähköisen asioinnin kautta tulevissa hakemuksissa vertailu tehdään aiemman passin kuvaan. Osaamisriskien suhteen myös hakemuksen liitteiden aitouden varmistamisessa on varauduttava inhimillisiin virheisiin. Osaamisriskien osalta on toki huomioitava sekin mahdollisuus, tunnistaminen saattaa olla parempilaatuista sähköisesti vireille tulevan hakemusten käsittelyssä. Fyysisessä toimintaympäristössä tilanne on kiireinen ja palveluhenkisyys saattaa kannustaa hoitamaan tunnistuspuolen mahdollisimman sujuvasti ja nopeasti. Läsnä olevan

asiakkaan kasvoja verrataan hänen toimittamaansa pieneen paperikuvaan ja tunnistusasiakirjassa olevaan kuvaan. Sähköisesti vireille tulevassa hakemuksessa virkailija saa eteensä kaksi isohkoa sähköistä kuvaa, ja hänen tehtävänsä on verrata, esittävätkö ne samaa henkilöä. Virkailijalla ei ole yksittäistapauksessa kiirettä, hän voi epävarmoissa tapauksissa käyttää enemmän aikaa, pyytää apua kollegoilta tai kutsua asiakkaan paikanpäälle tunnistettavaksi. Kynnys väärinkäytösyrityksille on kuitenkin sähköisessä toimintaympäristössä luultavasti matalampi, koska hakijan ei tarvitse olla henkilökohtaisesti paikalla.

### 5.3.3 Riskienhallintatoimenpiteet

**Maineriskien** hallintaan paras keino olisi minimoida epäonnistumiset, eli erityisesti passin myöntämisessä tapahtuvat virheet. Mikäli epäonnistumisia kuitenkin sattuu, voidaan tehokkaalla ja oikein suunnitellulla viestinnällä vaikuttaa ongelmasta selviytymiseen. Parasta mainosta poliisin sähköisille palveluille on helppokäyttöiset, varmatoimiset ja luotettavat sähköiset asiointikanavat, joiden pohjalta tehdään laadukkaita lupapäätöksiä mahdollisimman vähäisin virhein. Epäonnistumisten minimointi koskettaa koko prosessia hakemuksen jättövaiheesta valmiin asiakirjan toimittamiseen. Jo ulkoistetussa passinluovutustoiminnallisuudessakin tapahtuvat virheet mielletään helposti poliisin imagoa vahingoittaviksi virheiksi, vaikka valmiin asiakirjan toimittaja on yksityinen taho eli R-kioski.

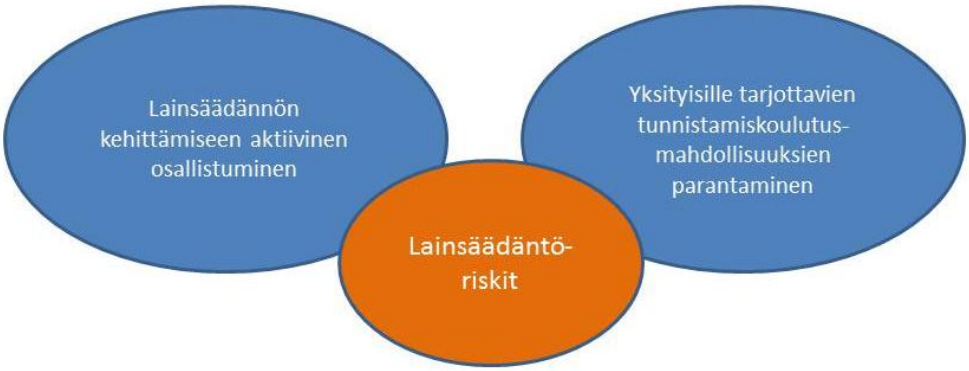

Kuva 8: Maineriskien hallinta.

**Asiakasriskien** hallitsemisessa tärkeimmäksi nousee virkailijoiden koulutus ja osaaminen, koska luvan päätöksentekovaiheessa väärinkäytösyritykset pitäisi viimeistään havaita. Myös eri-

laisista varmenteista huolehtimista tulisi markkinoida kansalaisille samalla kun neuvotaan esimerkiksi pankkikorttien jäädyttämisestä lompakon kadottua tai puhelinliittymän sulkemista kännykän kadottua. Poliisilla ja kaikilla muillakin viranomaisilla pitäisi olla myös viranomaisten myöntämiä kortteja varten sulkupalvelu, koska esimerkiksi tällä hetkellä ajokortteja ei pystytä ilmoittamaan kattavasti sulkulistalle, joka olisi kauppojen tai mobiilivarmenteita myöntävien palveluntarjoajien käytettävissä.


Kuva 9: Asiakasriskien hallitsemiskeinot.

**Lainsäädäntöriskeihin** vaikuttaminen on poliisin kannalta vaikeampaa, koska voimassaoleva lainsäädäntö vahvasta sähköisestä tunnistamisesta on liikenne- ja viestintäministeriön alaista lainsäädäntöä, joka pohjautuu eduskunnan tahtotilaan lain käsittelyvaiheessa. Vallitsevan tilanteen ja sähköisen asioinnin yleistyessä on äärimmäisen tärkeää, että poliisin on lainsäädännön kehittämisessä aktiivisesti mukana. Havaittuja riskejä tulee tuoda aktiivisesti esiin, mikäli nykytilannetta halutaan muuttaa ja kaikkia sähköisen asioinnin toimijoita koskevia riskejä pienentää. Tilannetta voitaisiin lainsäädäntömuutosten lisäksi esimerkiksi parantaa operaattoreille ja pankin henkilöstölle tarjottavalla säännöllisellä ja systemaattisella tunnistamiskoulutuksella, jonka tarjoaisi poliisi. Vahvoja sähköisiä tunnisteita myöntävillä firmoilla on oikeus käyttää poliisin tarjoamaa tunnistamisratkaisua, ja monet pankit ja operaattorit ovat sen lisenssin hankkineetkin, mutta tilannetta voitaisiin parantaa entisestään koulutusta ja yhteistyötä lisäämällä. Nykylainsäädännön kuitenkin vallitessa, poliisin kannattaa keskittää suurimmat voimavaransa omiin riskienhallintatoimenpiteisiinsä.




Kuva 10: Lainsäädäntöriskien hallitsemiskeinot.

On selvää, että sähköisen asioinnin käyttöönotto tuo mukanaan merkittäviä prosessimuutoksia sekä sitä myötä riskejä passin myöntöön liittyvässä toiminnassa. **Osaamis- ja prosessiriskien** hallitsemiseksi on käännettävä katse päätöksentekijän tunnistamisosaamiseen. Valokuvien vertailuun sekä ylipäätään tunnistamiseen liittyvä henkilöstön osaaminen nousevat korkeaan merkitykseen tällöin, kun asiakkaalla ei ole lainkaan fyysistä asiointia poliisissa. Henkilöstön apuna tulee olla käytössä kaikki mahdolliset tekniset toiminnallisuudet tunnistamisessa, kuten kasvokuvien vertailussa. Henkilöstön on oltava tietoinen prosessissa vallitsevista riskeistä, sekä omista toimintatavoistaan ja riskienarvioinnin merkityksestä. Henkilöstön on oltava varautunutta siihen, että sähköinen asiointi saattaa nostaa väärinkäytösyritysten määrää. Poliisilaitoksen henkilöstön tulisi havaita herkästi mahdollisia väärinkäytösyrityksiä niin asiointiprosessiin liittyen kuin esimerkiksi hakemuksen mukana toimitettuihin liitteisiin liittyen. Nykykäytännön mukaan poliisilaitosten pitää huolehtia siitä, että kaikki passi- ja henkilökorttihakemuksia vastaanottavat ja tunnistamista suorittavat henkilöt ovat suorittaneet tunnistamiskoulutuksen, ja että jokainen näissä tehtävissä työskentelevä päivittää osaamisensa säännöllisin väliajoin. Ohjeistuksen mukaan uuden henkilön pitää suorittaa sähköinen itseopiskelukurssi henkilön tunnistamisesta ennen kuin hän voi aloittaa passi- ja henkilökorttihakemusten vastaanottamisen ja/tai hakijoiden tunnistamisen. Nykykäytännön toteutumista voitaisiin valvoa paremmin, sekä suunnitella koulutuksen päivittämistä ja selvittää säännöllisen pakollisen lisäkoulutuksen tarvetta.

Valitettavasti kaikkia riskienhallinnan toimenpiteitä ei voida salassapitosäännösten vuoksi tuoda esiin tai avata tarkasti.

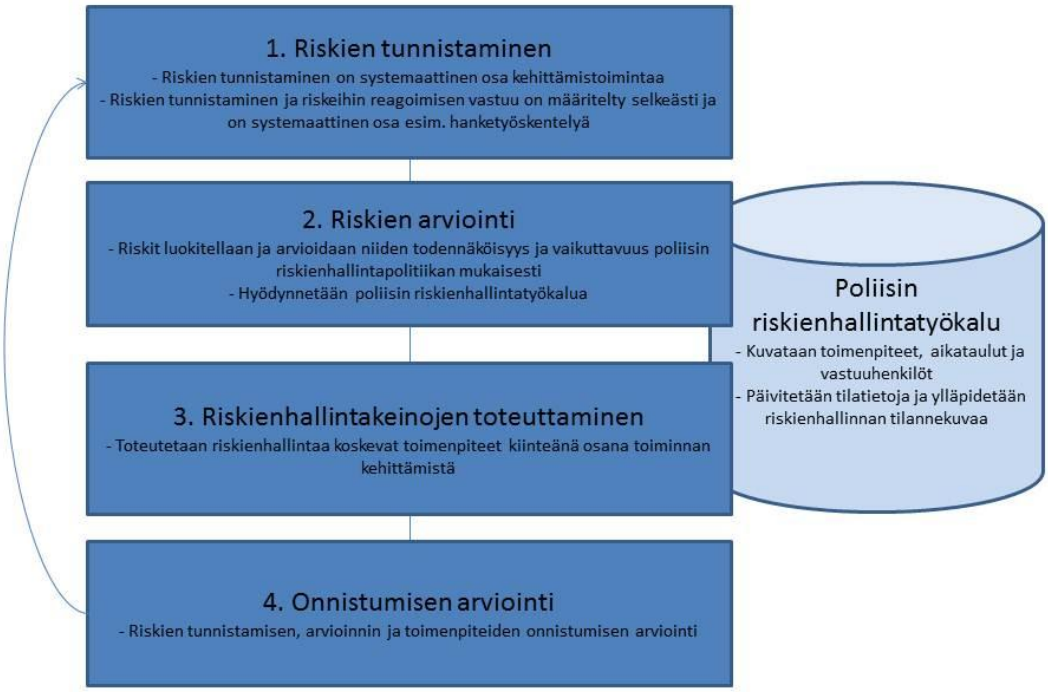

Kuva 11: Osaamis- ja prosessiriskien hallitsemiskeinot.

### 5.3.4 Riskienhallintamalli

Työn lopputuloksena syntyi passin sähköistä asiointia koskevien riskien hallintamalli, jota voi laajentaa koskemaan esimerkiksi koko poliisin (lupahallinnon) sähköisen asioinnin riskienhallintaa tai laajemmin esimerkiksi poliisin hankkeiden riskienhallintaa.

Toteutusmalli koostuu prosessista (kuva 8), jossa hyödynnetään poliisin riskienhallintatyökalua. Poliisin sähköisen riskienhallintatyökalun hyödyntämisen avulla kuvataan konkreettiset riskit, niiden hallitsemiseksi laaditut toimenpiteet sekä vastuuhenkilöt ja tilatiedot.

Lopuksi arvioidaan riskienhallinnassa onnistuminen, havaitaan mahdolliset jatkotoimenpiteet tai arvioinnin seurauksena havaitut uudet riskit.




Kuva 12: Riskienhallintamalli.

Ensimmäinen vaihe, riskien tunnistaminen, tulee olla systemaattinen osa kehittämistoimintaa, ja tässä tapauksessa Lupa2016-hankkeen toimintaa. Poliisin riskienhallintapolitiikan mukaisesti hankkeiden riskienhallinnasta vastaa hankepäällikkö, joten hankepäällikön tehtäväksi jää jalkauttaa riskien tunnistaminen kiinteäksi osaksi hankkeen normaalia toimintaa ja kehittämistä. Riskien tunnistaminen ja riskeihin reagoimisen vastuut ja merkitykset tulee saada systemaattiseksi osaksi hanketyöskentelyä, ja hankkeen sisällä vallitsevan työskentelykulttuurin tulisi olla lähtökohtaisesti riskejä havaitseva ja riskitietoinen. Kommunikaation toimivuuteen tulee myös kiinnittää erityistä huomiota, koska muutoin havaitut riskit eivät nouse esiin normaalin toiminnan tiimellyksessä. Riskejä voidaan kartoittaa tai tunnistaa myös erillisten riskisessioiden avulla, kuten vaikkapa erillisissä sisäisissä kehittämistilaisuuksissa. Monet poliisin kehittämishankkeista nivoutuvat yhteen, joten yhä tiiviimmästä hankkeiden välisestä riskien kartoittamisesta ja kommunikaation toimivuuden huolehtimisesta olisi varmasti hyötyä.

Riskien arviointia voidaan tehdä joko yksin hankepäällikön toimesta tai yhdessä hankkeen työntekijöiden kanssa. Riskien todennäköisyys ja vaikuttavuus luokitellaan ja arvioidaan, hyödyntäen poliisin riskienhallintatyökalua. Riskienhallintatyökaluun merkitään myös riskin tilatieto, jota käytetään riskin tilanteen seuraamiseen. Tilatiedon asteikko on:
1. Arvioimatta = Arviointi on kesken (toimenpiteitä ei ole aloitettu).
2. Arvioitu = Arviointi on valmis (toimenpiteitä ei ole aloitettu).

3. Odottaa = Toimenpiteet on aloitettu, mutta ei suoritettu loppuun.
4. Valmis = Kaikki toimenpiteet on tehty.
Tilatiedon lisäksi riskien arvioinnissa määritellään määräaika ja vastuuhenkilö.

Riskienhallintakeinojen toteuttamisen tulisi olla kiinteä osa kehittämistoimintaa. Havaittujen riskien vaikutukset esimerkiksi aikatauluihin huomioidaan välittömästi niin hankesuunnittelussa kuin laajemmin poliisitoiminnan kehittämisen suunnittelussa ja sen aikataulutuksessa. Hankkeessa havaituista muutoksista tulee tiedottaa aktiivisesti mm. muiden, liittyvien hankkeiden, henkilöstöä. Riskienhallintatyökalu auttaa ylläpitämään kokonaistilannekuvaa käsillä olevan kokonaisuuden riskienhallinnasta.

Kun riskienhallintakeinot ovat toteutettu, on aika arvioida onnistuminen. Onnistumista voidaan toki arvioida myös jokaisen prosessin välivaiheessa, mutta arviointi tehdään viimeistään tässä vaiheessa. Mikäli arvioinnin yhteydessä havaitaan, että prosessin tuotoksena on havaittu mahdollisia uusia riskejä, siirtyvät nämä prosessin alkuvaiheeseen kartoitettaviksi ja arvioitaviksi. Havaitut virheet tai epäonnistumiset puretaan, jotta niistä voidaan ottaa opiksi, ja havaituista onnistumisista annetaan positiivista palautetta.

### 5.4 Alustavia käytännön kokemuksia

Alustavia käytännön kokemuksia on tässä vaiheessa hankkeen toteutusaikataulua todella vaikeaa todeta, koska käyttöönotot ajoittuvat suunnitelmien mukaan syksylle 2014. Kuitenkin riskien kartoittamisen, luokittelun ja arvioinnin tuloksena havaitut kriittiset pisteet - kuten henkilöstön osaaminen tunnistamisessa ja väärinkäytösepäilysten havaitsemisessa - tullaan ottamaan henkilöstön koulutuksessa huomioon. Myös yhteistyötä Poliisihallituksen viestinnän kanssa tullaan tiivistämään, joka on suunniteltu osaksi toteutusaikataulua.

## 6 Johtopäätökset ja pohdinta

### 6.1 Hakijan tunnistaminen ja tulevaisuuden tunnistamisratkaisut

Yksi suurimmista riskeistä sähköisessä asioinnissa liittyy passinkin hakemisen tapauksessa hakijan luotettavaan tunnistamiseen. Tunnistamiseen ja tunnistamisasiakirjoihin liittyvää problematiikkaa on tuotu tässä työssä laajalti esiin. Aikanaan vuonna 2009 laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista sekä eräiksi siihen liittyviksi laeiksi käsittelyn yhteydessä tehdyillä päätöksillä on ollut kauaskantoiset vaikutukset tähän päivään saakka ja tästä edelleen. Näiden ratkaisujen aiheuttamat riskit ovat nykypäivää kaikessa viranomaisten sähköisessä asioinnissa, niin kauan kun sallitaan ajokortin käyttö tunnistamisasiakirjana vahvoja sähköisiä varmenteita myönnettäessä, ja sallitaan yksityisten toimijoiden suorittama

ensitunnistaminen. Vaikka yleisimpänä tunnistautumistapana sähköisessä asioinnissa ovatkin verkkopankkitunnukset, ja vaikka mobiilivarmenne on varmenteena hyvin vähän käytössä, se ei silti poista sitä riskiä, mitkä sähköisen identiteetiin myöntämiseen liittyy.

Yhtenä merkittävimpänä ja potentiaalisena tulevaisuuden kehittämisnäkymänä voidaan varmenteita koskevissa riskeissä kuitenkin pitää Valtiovarainministeriön vetämää Palveluväylä -hanketta. Useammat viranomaiset poliisin lisäksi, kuten esimerkiksi Kela, ovat mukana rakentamassa yhteistä palveluarkkitehtuuria ja tunnistusratkaisua. Palveluväylän tavoitteena on tarjota kansalaisille ja yrityksille helpompaa verkkoasiointia eri toimijoiden palveluissa. Kansallinen palveluväylä kokoaa yhteen valtion, kuntien ja yksityisten toimijoiden sähköiset palvelut ja sen kehittämistä johtaa valtiovarainministeriö. Palveluväylä on määrä ottaa käyttöön asteittain vuosina 2015–2018. Erityisesti Kela on nähnyt, että kansallisen tunnistusratkaisun ja palveluväylän kehittäminen on välttämätöntä sähköisen asioinnin edistämisessä. Palveluväylän yhtenä merkittävänä tavoitteena on tarjota muun muassa eri toimijoiden verkkoasiointipalveluille yhteinen tunnistusratkaisu, jossa käytetään valtion tarjoamaa sähköistä tunnistetta. Samalla tulisi luoda roolit ja valtuudet, joilla asiakas voisi asioida myös toisen puolesta sähköisesti. Sähköistä asiointia tulisi kehittää taloudellisesti kestävällä tavalla, jossa yhteinen tunnistusjärjestelmä olisi kustannuksiltaan nykyistä pankkitunnuksiin nojaavaa järjestelmää edullisempi ja vapauttaisi resursseja tärkeimpään eli sähköisten palveluiden kehittämiseen. (Kela mukana rakentamassa yhteistä palveluarkkitehtuuria ja tunnistusratkaisua 2013.)

Mikäli helppokäyttöisen kansallisen tunnistusratkaisun levittäminen onnistuisi yhtä hyvin Suomessa kuin Virossa, voisi se helposti johtaa laajakäyttöisyyteen tunnistamisratkaisuun, joka olisi käytössä sekä julkishallinnon että yksityisen puolen sähköisissä palveluissa. Tällöin sähköinen asiointi ja siihen liittyvä tunnistaminen saataisiin rakennettua kansallisen tunnistusratkaisun varaan. Virossa fyysisen ja sähköisen henkilöllisyyden varmenteen laajalle leviämisen vauhdittajana on ollut todella edullinen hinta, ja tämä pitäisi huomioida Suomessakin. Kuten Tietosuojavaltuutetun toimiston Huhtiniemi asian haastattelussaan ilmaisi; kustannusten lasku tässä päässä saattaisi tuottaa toisaalla.

### 6.2 Mitä jos riskit toteutuvat?

Mikäli poliisi epäonnistuu sähköisen asioinnin kautta vireille tulleen passin myöntöprosessiin liittyvässä tunnistamisessa, kasvokuvan vertailussa, riskien havaitsemisessa tai riskien käsittelyssä, se voi johtaa esimerkiksi passin päätymiseen vääriin käsiin, henkilötietojen päätymiseen väärän henkilön passille tai alkuperäisen passin hakuvaiheessa kerättyjen biometristen tunnisteiden päätymisen väärälle henkilölle myönnetylle passille. Nämä ovat jo itsessään todella epätoivottuja skenaarioita. Näiden riskien toteutumisella saattaisi olla merkittäviä vaikutuksia myös Suomen passiin liittyvään luotettavuuteen sekä Suomen poliisin luotettavuu-

teen. Yllä mainittujen riskiskenaarioiden perusteella voidaan todeta, että Suomen passin myöntämiseen liittyvän sähköiseen asioinnin riskejä tulee hallita jollain tavalla. Yhtenä esimerkkinä on tässä työssä esitetty riskienhallintamalli, jossa riskit havaitaan, arvioidaan ja niiden vähentämiseksi, poistamiseksi tai muuttamiseksi suunnitellaan ja toteutetaan erilaisia toimenpiteitä.

Tässä työssä laadittua riskienhallintamallia voi laajentaa koskemaan myös tämän työn ulkopuolelle rajattuja riskejä, koko Lupa2016-hanketta tai kaikkien poliisin hankkeiden riskienhallintaa.

Lähteet

Aaltonen, M. & Salmi, V. 2010. Nuorten rikoskäyttäytyminen ja uhrikokemukset internetissä. Viitattu 15.3.2014.
http://www.haaste.om.fi/fi/index/lehtiarkisto/haaste32010/nuortenrikoskayttaytyminenjauhrikokemuksetinternetissa.html

Berg, K-E. 1994. Yrityksen riskienhallinta. Jyväskylä: Gummerus.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2004. Enterprise Risk Management – Integrated Framework. Viitattu 6.4.2014.
http://www.coso.org/documents/coso_erm_executivesummary_finnish.pdf

Finanssialan keskusliitto. 28.3.2011. Pankkien Tupas–tunnistuspalvelun tunnistusperiaatteet. Viitattu 1.3.2014. http://www.fkl.fi/teemasivut/sahkoinen_asiointi/Dokumentit/Tupas-tunnnistusperiaatteet_v20b.pdf

Finanssivalvonta. 22.6.2010 (muutettu 10.6.2013). Standardi 2.4: Asiakkaan tunteminen - rahanpesun, terrorismin rahoittamisen sekä markkinoiden väärinkäytön estäminen. Viitattu 1.3.2014.
http://www.finanssivalvonta.fi/fi/Saantely/Maarayskokoelma/Rahoitussektori/2_Menettelytavat/Documents/2.4.std5.pdf

Hallintovaliokunnan lausunto 9/2009 vp.

Heeks, R. 2003. Most eGovernment-for-Development Projects Fail: How Can Risks be Reduced? Institute for Development Policy and Management, University of Manchester. Viitattu 9.4.2014.
http://unpan1.un.org/intradoc/groups/public/documents/NISPAcee/UNPAN015488.pdf

Hopkin, P. 2010. Fundamentals of Risk Management — understanding, evaluating and implementing effective risk management.

Ilmonen, I., Kallio, J., Koskinen, J., Rajala M. 2010. Johda riskejä – käytännön opas yrityksen riskienhallintaan. Helsinki: Kustannusosakeyhtiö Tammi.

Kansaneläkelaitos. 2014. Tiedote 3.12.2013: Kela mukana rakentamassa yhteistä palveluarkkitehtuuria ja tunnistusratkaisua. Viitattu 18.3.2014. http://www.kela.fi/ajankohtaista/-/asset_publisher/mHBZ5fHNro4S/content/id/1373457

Kasanen, E., Lukka, K. & Siitonen, A. 1993. Journal of Management Accounting Research: The Constructive Approach in Management Accounting Research.

Kasvi, J. 2012. Tietoturva ja käyttäytyminen intranetissä. Viitattu 15.3.2014.
http://www.slideshare.net/AnnaUu/tietoturva-ja-kytttytyminen-intranetiss-tieke-jyrki-kasvi

Kefallinos, D., Lambrou, M. & Sykas, E. 2009. An Extended Risk Assessment Model for Secure E-Government Projects. International Journal of Electronic Government Research 5.2., 72 - 92.

Kytö, H. 2007. Verkkopalvelujen turvallisuus kuluttajan näkökulmasta. Viitattu 7.4.2014.
http://www.kuluttajatutkimuskeskus.fi/files/5137/09_Verkkopalvelujen_turvallisuus_kuluttajan_nakokulmasta.pdf

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 7.8.2009/617.

Lukka, K. 2011. Konstruktiivinen tutkimusote. Viitattu 11.4.2014.
http://www.metodix.com/fi/sisallys/01_menetelmat/02_metodiartikkelit/lukka_const_research_app/kooste

Passilaki 21.7.2006/671.

Poliisihallitus. 2011. Esite: Poliisi Suomessa. Viitattu 15.2.2014. http://www.poliisi.fi/poliisi/home.nsf/ExternalFiles/poliisisuomessa/$file/poliisisuomessa.pdf

Poliisihallitus. 23.1.2012. Lupa 2016-hankkeen asettaminen.

Poliisihallitus. 2013. Määräys: Poliisin riskienhallintapolitiikka (2020/2013/828).

Poliisihallitus. 2014. Riskienhallinnan prosessi.

Poliisin organisaatio. 2014. Viitattu 15.3.2014. https://www.poliisi.fi/poliisi/home.nsf/pages/E9D8E3C4F56C4927C2256B8700455C96?opendocument

Rasmus, A-M. 2009. Kansalaisten sähköinen asiointi viranomaistoiminnassa - haasteena digitaalinen kuilu. Viitattu 15.3.2014. https://jyx.jyu.fi/dspace/bitstream/handle/123456789/22924/Anna-Mari%20Rasmus.pdf?sequence=1

Sisäministeriö. 2013. Asettamispäätös: Sähköinen asiointi passimenettelyssä. Viitattu 15.2.2014. http://www.intermin.fi/download/47998_PassiL_sahkoinen_asiointi_asettamispaatos_141013.pdf?899c11cf29f5d088

Sisäministeriö. 2012. Esite: Uudistuva poliisi 2014. Viitattu 15.3.2014. http://www.kopijyva.fi/ejulkaisut/sisaasiainministerio/uudistuva_poliisi/

Sisäministeriö. 2012. Hanketyöryhmän esitys: Poliisin hallintorakenneuudistus Pora III - päälinjaukset. Viitattu 15.2.2014. http://www.intermin.fi/julkaisu/342012?docID=36149

Sisäministeriö. 2010. Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma), työryhmän loppuraportti. Viitattu 8.3.2014. http://www.intermin.fi/julkaisu/322010?docID=24918

Suomen perustuslaki 11.6.1999/731.

Suomen riskienhallintayhdistys. 2014. Riskienhallintaprosessi. Viitattu 6.4.2014. http://www.pk-rh.fi/index.php?page=riskienhallintaprosessi

Suomen Standardoimisliitto SFS ry. 2014. ISO 31000 Riskienhallinta. Viitattu 7.3.2014. http://www.sfs.fi/julkaisut_ja_palvelut/tuotteet_valokeilassa/iso_31000_riskienhallinta

Työterveyslaitos. 2014. Termejä ja määritelmiä. Viitattu 17.2.2014. http://www.ttl.fi/fi/tyoturvallisuus_ja_riskien_hallinta/tapaturmien_ehkaisy/tietoa_tapaturmista/termeja_ja_maaritelmia/sivut/default.aspx

VAHTI - Valtionhallinnon tietoturvasanasto. 2008. Valtiovarainministeriö. Viitattu 19.3.2014. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20081211Valtio/Vahti_8_NETTI%2b_KANNET.pdf

Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI). 2001. Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje. Viitattu 7.4.2014. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/3371/3372_fi.pdf

Valtiovarainministeriö. 2013. Asiakaspalvelu 2014 - Yhdessä palvelut lähelle (julkisen hallinnon asiakaspalvelun kehittämishankkeen loppuraportti). Viitattu 8.3.2014. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/04_hallinnon_kehittaminen/20130612Asiaka/Asiakaspalvelu_2014_netti.pdf

Valtiovarainministeriö. 2014. Sähköisen asioinnin palvelut. Viitattu 17.2.2014. http://www.vm.fi/vm/fi/16_ict_toiminta/04_sahkoinen_asiointi/index.jsp

Valtiovarainministeriö. 2013. Sähköisen asioinnin lainsäädännön seuranta- ja kehittämistutkimus. Viitattu 17.2.2014. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/076_ict/20140117Saehkoei/Saetke-raportti.pdf

Valtiovarainministeriö. 2014. Valtio haluaa laajentaa sähköistä asiointia Suomessa: Kansalaisen asiointitilin käyttäjämäärä kaksinkertaistunut. Viitattu 17.2.2014. http://www.vm.fi/vm/fi/03_tiedotteet_ja_puheet/01_tiedotteet/20140121Kansal/name.jsp

Verohallinto. 2014. Tiedote 5.3.2014: Lähes 60 prosenttia osakeyhtiöiden veroilmoituksista annetaan verkossa - Verohallinto kannustaa paperi-ilmoittajia sähköiseen ilmoittamiseen. Viitattu 15.3.2014. https://www.vero.fi/fi-FI/Tietoa_Verohallinnosta/Tiedotteet/Yritys_ja_yhteisoasiakkaat/Lahes_60_prosenttia_osakeyhtioiden_veroi(31965)

Verohallinto. 2014. Tiedote 22.1.2014: Verkossa tehtyjen verokorttien määrä hurjassa kasvussa. Viitattu 15.3.2014. http://www.vero.fi/fi-FI/Tietoa_Verohallinnosta/Tiedotteet/Henkiloasiakkaat/Verkossa_tehtyjen_verokorttien_maara_hur(30911)

Verohallinto. 2014. Veroilmoitus. Viitattu 15.3.2014. http://www.vero.fi/fi-FI/Henkiloasiakkaat/Veroilmoitus

Julkaisemattomat lähteet

Ikura, J. 2014. Sähköpostit 24.1.2014 & 6.2.2014. NHQ - Admissibility: Citizenship and Immigration Canada, Government of Canada.

Karjalainen, T. 2014. Sähköposti 22.3.2014. Electronic Frontier Finland ry.

Puhakainen, P. 2014. Sähköposti 27.2.2014. Verohallinto.

Taponen, V. 2014. Sähköposti 19.3.2014. Kansaneläkelaitos.

Tse, L. 2014. Sähköposti 18.2.2014. Passports Uruwhenua, Department of Internal Affairs Te Tari Taiwhenua, Government of New Zealand.

Kuvat