Tarja Nylander

E-passin teknologiaratkaisu

Tietotekniikan
pro gradu -tutkielma
12. huhtikuuta 2017

Jyväskylän yliopisto

Tietotekniikan laitos

Kokkolan yliopistokeskus Chydenius

Tekijä: Tarja Nylander
Yhteystiedot: tarja.t.nylander@student.jyu.fi
Puhelinnumero: 040-1870 540
Ohjaaja: Ismo Hakala
Työn nimi: E-passin teknologiaratkaisu
Title in English: E-passport's technological solution
Työ: Tietotekniikan pro gradu -tutkielma
Sivumäärä: 77+4
Tiivistelmä: Tutkielmassa kerrotaan passin kehitys tavallisesta matkustusasiakirjasta e-passiksi. Työssä esitellään e-passin sovelluksen tekniset ratkaisut. Teknologiaratkaisuun kuuluu olennaisena RFID -mikrosiru ja sille tallennettu biometrinen tunniste. Tutkimuksessa selvitetään yleisemmät biometriset tunnisteet ja niiden käsittelyvaiheet.

Työ on tieteellisiin artikkeleihin perustuva kirjoitelma. Yhdysvaltojen e-passiin toteutettiin RFID-tunniste ja se sai aikanaan arvostelua teknologiavalinnoista. Euroopan ja Suomen e-passien kehitykseen on vaikuttanut kokemukset Yhdysvaltojen e-passin käyttöönottoprojektista. Tutkielmassa pyritään löytämään eroja Yhdysvaltojen, Euroopan ja Suomen e-passien tietoturvan, yksityisyyden suojan kuin muidenkin tekijöiden osalta. E-passin tulevaisuus on kiinnostava, sillä matkailu ja siten tarve e-passeille on kasvava. E-passi on edellytys automaattiseen rajatarkastukseen. Miljoonien matkustajien mukana kulkeva tärkeä identiteetin todistava biometrinen tunniste e-passilla on sekä uhka että mahdollisuus sujuvampaan matkustamiseen.
Avainsanat: e-passi, biometriset tunnisteet, tietoturva, yksityisyyden suoja, RFID
Abstract: The purpose of the Master Thesis is to describe the development phases of a passport from a traditional travel document to an electronic passport. The thesis presents the technological solutions for e-passport system. One of the most essential parts of the e-passport's technological solution is the RFID microchip. This thesis focuses on e-passport system and the most commonly used biometric identification methods.

The approach of the thesis is based on scientific articles. It was found out that the e-passport implementation in the United States of America received a lot of criticism of its technological solutions. The adoption of e-passport was the first larger scale implementation in the world. It has had an impact on the other countries e-passport adoption. The e-passport implementation in Europe differs from USA's. Furthermore the study explains the differences between data security, privacy and

other actors.

The thesis concludes that the future of the e-passport is very interesting because it is estimated that travelling will be emerging thus the need of the e-passport is growing. In the conclusion of the thesis it can be discovered that the biometric identifier which is embedded in the e-passport may be both a threat and an opportunity for smoother travelling. E-passport is essential for automated border control. Millions of passengers benefit from secure e-passport which will authenticate their identity.
Keywords: E-passport, biometric identification, data security, privacy, RFID

Esipuhe

Minulta kysyttiin gradusta: ”mikä se sellainen ratu on?” ja ennenkuin vastausta ehdin sanoa myös jatkokysymyksiä esitettiin: ”mitä sillä tekee?” sekä ”onko minullakin e-passi?”

Hyviä kysymyksiä - siis mikä on tämän työn tarkoitus? Passi, e-passi ja biometrinen passi. Yritän kertoa, kuinka tavallisesta passista tuli e-passi ja miten biometriikka siihen liittyy.

Perheelleni, ystävilleni, kollegoilleni ja yliopistolle kiitokset kannustuksesta, kiinnostuksesta ja tuesta graduni tekemisessä.

Sanasto

AA	Active Authentication
ABC	Automated Border Control
BAC	Basic Access Control
CA	Chip Authentication
DEC	Dublicate Enrolment Check
DES	Data Encryption Standard
DNA	Deoxyribonucleic acid, Desoksiribonukleiinihappo
DOS	Denial of Service, U.S. Department of State
DPI	Dots per inch, Pixels per inch
EAB	European Association for Biometrics
EAC	Extended Access Control
ECC	Electronic Communications Committee, Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
EEPROM	Electronically Erasable Programmable Read-Only Memory
eID	Electronic Identity Card
eMRP	Electronic Machine Readable Passport
eMRTD	Electronic Machine Readable Travel Document
ERO	European Radiocommunication Office
ESTA	Electronic System for Travel Authorization
ETSI	European Telecommunications Standards Institute
FBI	Federal Bureau of Investigation
GPS	Global Positioning System
GPU	Graphical Processing Unit
IATA	International Air Transport Association
IC	Integrated Chip

ICAO	International Civil Aviation Organization
ID	Identity Card
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
JPEG	Joint Photographic Expert Group, JPEG2000
LDS	Logical Data Structure, LDS2
MCC	Minutia Cylinder Code
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
NFC	Near Field Communication
OCR	Optical recognition
OSEP	Online Secure e-Passport Protocol
PA	Passive Authentication
PACE	Password Authenticated Connection Establishment
PKD	Public Key Directory
PKI	Public Key Infrastructure
RF	Radio Frequency
RFID	Radio Frequency IDentification
RGB	Red Green Blue
RTP	Registered Traveller Program
SAC	Supplemental Access Control
TA	Terminal Authentication
TAG	Technical Advisory Group
UV	Ultraviolet
VRK	Väestörekisterikeskus
VWP	Visa Waiver Program

Sisältö

1 Johdanto

Passi on henkilökohtainen matkustusasiakirja. Passi, jossa on mikrosirulle tallennettuna passinhaltijan henkilötietoa on elektroninen passi, e-passi. E-passi on kehitetty matkustusturvallisuuden parantamiseksi. Teknologinen kehitys ja biometrisen tiedon sisällyttäminen passikirjaan on mahdollistanut sen, että e-passista on tullut tärkeä maailmanlaajuinen henkilötunnistamisen sovellus.

E-passin laajempi tarkastelu tietojärjestelmänä sisältää runsaasti matkustusasiakirjoihin liittyvää teknologiaa passinhaltijan henkilökohtaisten tietojen käsittelyssä. Tässä tutkimuksessa käsitellään e-passin tietoturvaa, yksityisyyden suojaa ja tietojen suojausta viranomaisten vastuualueella. Tutkimus käsittelee biometrisia tunnisteita, sillä biometrinen henkilötunnistaminen on yleistynyt laajalle. E-passi on tehokas identiteetin todentamisen väline.

Nopeat globaalit muutokset, liikkumisen vapaus ja sitä myötä kasvaneet matkustusmäärät ovat huomattavasti lisänneet tarvetta biometristen tunnisteiden käyttösovelluksille. Maapallolla liikkuu vuosittain 3,5 miljardia matkustajaa. Esimerkiksi Yhdysvalloissa tilastoitiin vuonna 2015 lentomatkustusmääräksi noin 798 miljoonaa. Euroopan unionin alueella lentomatkoja tilastoitiin reilut 653 miljoonaa. Suomessa tehtiin noin 10 miljoonaa lentomatkaa vuonna 2015. Ulkomaan matkoilla ihmisten identiteetin todistaa mukanakuljetettava passi. Kun eurooppalaisia ja suomalaisia e-passeja verrataan Yhdysvaltojen e-passin ratkaisuun, huomataan biometrian ja tietosuojan osalta eroja. Maailmanlaajuiset turvallisuutta uhkaavat ilmiöt aikaansaavat erilaisia henkilötunnistamisen oikeutuksia. Oikeutuksien ohella tarvitaan yhtälailla velvollisuuksia tietoturvasta ja henkilötietojen suojauksesta.

Tutkimuksen pääasiallinen tavoite on hahmottaa e-passin tekninen toteutus ja sovelluksen käyttötarkoitus. E-passi sovelluksen käsittelyketjuun liittyy etätunnistaminen. Tästä erityisesti e-passiin upotettu RFID-tunniste ja sen tietoturvanäkökulmat biometrian käsittelyssä kiinnostavat. RFID-teknologiaa on verrattu 2010 -luvulla merkittävyydeltään matkapuhelimiin 1990 -luvulla. RFID onkin suosittu tekniikka etätunnistamisessa. RFID toteutuksien osalta on huomattava, että sen kautta on mahdollisuus tuottaa ja saada todella runsaasti tietoa ja dataa esineistä, asioista, eläimistä ja ihmisistä. Tietoturvan lisäksi työssä arvioidaan yksityisyyden suojaa.

Biometriatiedot ja niiden keruu, säilytys sekä tarkastus ovat osa teknologiaratkaisua ja prosessia. Laajasti otten ihmiset liittävät edelleenkin sormenjälkitunnistamisen rikostutkintaan. Väestöstä suurin osa kokee, ettei mitään salattavaa ole. Useammat ihmiset suostuvat antamaan järjestelmiin sormenjälkitietojaan helposti, osa ihmisistä puolestaan kokee tilanteen kiusallisena ja yksityisyyttä loukkaavana. E-passia kehitetään turvallisuuden haasteisiin ja kiihtyvällä tahdilla kehittyvää teknologiaa vastaavaksi. Informaatioteknologian ja tietoverkkojen avulla järjestelmä tunnistaa identiteetin biometriatunnisteiden avulla hetkessä. E-passin tarkastaminen rajatarkastuksissa onkin kaikkein laajin nykyään käytössä oleva biometrian sovellus. Rajatarkastuksella on siis erittäin merkittävä rooli. Biometristen tunnistamisen metodeja ei ole tarpeeksi standardisoitu. Erittäin paljon käydään keskusteluja myös automaattisesta henkilötunnistamisesta.

Tutkimus herättää kysymyksen siitä, onko e-passi sovelluksessa biometrinen tunnistaminen tulevaisuuden mahdollisuus vai uhka? Tutkimus on tieteellisiin arkikkeleihin ja julkaisuihin pohjautuva kirjoitelma. Tavoitteena on antaa lukijalle kuva e-passin teknologiaratkaisun perusasioista ja sovelluksen käyttötarkoituksesta. Luvussa 2 on tietoturvan näkökulmia. Tietoturvallisuus johdetaan tietoturvan tavoitteista tarkemmin tietoturvallisuuden osa-alueisiin ja yksityisyyden suojaan. Koska e-passeissa käytetään julkisen avaimen järjestelmää, esitellään se ja sen tietosuoja. Luvussa 3 käsitellään biometriset tunnisteet. Luku 4 koostuu RFID-järjestelmästä. Siinä kuvataan etätunnistamisen sovellusalueita sekä ratkaisua matkustusasiakirjoissa. Luvussa 5 käydään läpi e-passi kokonaisuutena, sen kehitystarina tavallisesta passista e-passiksi, ICAO -standardi sekä esimerkkinä e-passi sovelluksesta Yhdysvaltojen, eurooppalaisen ja suomalaisen e-passin yksityiskohtia. Luvussa 6 on katsaus e-passin tulevaisuuden näkymiin. Lopuksi on tutkimuksen yhteenveto.

2 Tietoturvallisuus

Tietoturvallisuus on yleinen käsite kaikille niille järjestelyille, joilla pyritään varmistamaan tietoa. Käsite ymmärretään usein kovin teknisestä näkökulmasta, vaikka se on organisaatiossa hyvinkin hallinnollinen järjestely. Suomen standardisoimisliiton [64] julkaisussa tietoturvallisuus tarkoittaa tiedon luottamuksellisuuden, eheyden ja käytettävyyden säilyttämistä. Käytettävyys ja saatavuus esiintyvät tietoturvan määritelmissä toistensa synonyymeinä. Tietoturvallisuuteen voi sisältyä muitakin tiedon ominaisuuksia. Näitä ovat tietojen aitous, tiedon kiistämättömyys ja luotettavuus sekä vastuullisuus. Vastuullisuus merkitsee, että kaikki tahot ovat vastuussa tietoturvallisuudesta. Tietoturvallisuuden tavoite on varmistaa, että tietojärjestelmät tekevät aina sen mihin ne on tarkoitettu. Tietoturvallisuuden tehtävänä on suojata tietoja, palveluja, järjestelmiä ja tietoliikennettä odottamattomilta sekä odotetuilta tietoturvauhkilta ja -riskeiltä, kuten Peltomäki ja Norppa [53] määrittelevät. Sekä teknisillä että hallinnollisilla menetelmillä pyritään suojaamaan ja siten takaamaan tiedon luottamuksellisuus, eheys ja saatavuus.

Tietoturva on Järvisen [31] mukaan perusta tärkeiden ja luottamuksellisten tietojen käsittelemiselle. Ydinalueina voidaan pitää yksityisyyden suojan ja henkilötietojen käsittelyn periaatteita ja toimintatapoja. Tietoturvan tavoitteet ovat:

- Luottamuksellisuus
- Eheys
- Saatavuus

Tiedon luottamuksellisuus tarkoittaa sitä, että tietoja käsittelevät vain ne henkilöt, jotka ovat oikeutettuja siihen. Tietojen paljastaminen oikeudettomalle taholle merkitsee luottamuksen menetystä. Käytännössä tietojen luottamuksellisuutta toteutetaan fyysisillä turvajärjestelyillä, pääsynvalvonnalla, tietojen salauksella, todennuksella ja käyttövaltuuksilla.

Tietojen luottamuksellisuuden vaatimus perustuu siihen, että tieto on vain tietyn henkilön tai tiettyjen henkilöiden tietoon tarkoitettu. Järvisen [31] mukaan tietojen luottamuksellisuuden pyrkimys on siinä, ettei kukaan pääse oikeudettomasti katsomaan, selaamaan tai välittämään tai muutoin käyttämään tietoa, johon hänelle ei ole

etukäteen myönnetty oikeutta. Jotta tietoon voi luottaa, tulee tiedon olla autenttista, jolloin sen ominaisuuteen kuuluu kiistämättömyys.

Tietojen eheydellä tarkoitetaan sitä, että tieto pysyy muuttumattomana tai muutokset ovat hallittuja eikä mikään ulkopuolinen taho pysty luvatta muuttamaan tiedon sisältöä. Tieto ei myöskään tuhoudu hallitsemattomasti. Tietoaineistojen eheyttä voidaan varmistaa muun muassa varmuuskopioinnilla. Yksittäisten tietojen eheyttä voidaan varmistaa algoritmeihin perustuvilla tarkistussummilla tai muilla laskennallisilla tai tietoa korjaavilla koodeilla. Eheyden takaamiseksi käytetään tietojärjestelmissä ja tiedostoissa lokitiedostoja. Eheyttä voidaan varmistaa myös tiedonsiirtoprotokollien ja suojauksien avulla [31].

Tietojen saatavuudella tarkoitetaan myös palvelujen saatavuutta ja siten yleisestikin tietojärjestelmiin perustuvan toiminnan turvaamista [31]. Esimerkiksi tietoverkkoyhteydet muodostavat tärkeän osan saatavuudessa. Verkkoyhteydet pitää toimia, jotta tietojärjestelmän tietoja voidaan hyväksikäyttää aina kun käyttäjällä on siihen oikeus. Saatavuutta varmistetaan fyysisillä suojauksilla ja laitteistojen varajärjestelyillä. Saatavuuden ja käytettävyyden välillä on vain hiuksen hieno ero. Käytettävyys ilmentää sitä, miten tieto tai palvelu on sen ihmisen hyödynnettävissä, jolla on oikeus tiedon tai palvelun hyödyntämiseen haluttuna aikana ja vaaditulla tavalla. Järvisen [31] mukaan saatavuuden tärkeys mitataan ja arvioidaan yleensä sen mukaan kuinka kriittistä tietoaineisto on organisaation ydintoiminnalle.

Yksinkertainen tietoturvallisuuden uhka-analyysi auttaa arvioimaaan niitä vaikutuksia, mitä menetetään, jos tietojen saatavuus, luottamuksellisuus, eheys ja oikeellisuus murenee. Tietoturvallisuuden puutteiden vuoksi voi tietoja kadota osittain tai hävitä kokonaan, tiedot voivat muuttua tai tietoa voi vuotaa oikeudettomalle taholle. Hallinnollisilla ja teknisillä järjestelyillä pyritään suojaamaan tietopääomaa ja säilyttämään erityisesti käytettävyys, luottamuksellisuus ja tiedon eheys [73].

Tietoturvallisuuden tavoitteiden ja niiden osa-alueiden merkitys vaihtelee suojattavan tiedon mukaan. Esimerkiksi tiedon luottamuksellisuus, eheys ja saatavuus voi painottua uudemman sukupolven matkustusasiakirjojen käsittelyssä. E-passi tai eID sisältävät suojatulle mikrosirulle tallennettua arkaluontoista henkilötietoa sekä sensitiivisiä biometrisia henkilötunnisteita, jolloin tietojen alkuperäisyys ja kiistämättömyys nousevat tärkeään asemaan suojattavasta tiedosta. Tiedoista huolehtiminen kuuluu kansalaisten perusoikeuksiin.

Tietojen alkuperäisyys (autenttisuus) ja kiistämättömyys ovat luottamuksellisuuden vaatimuksia. Lisäksi pääsynvalvonta tietoihin luo perustaa luottamukselliselle

tietojenkäsittelylle. Yhteiset käyttösäännöt määräävät sen, miten tulisi toimia, jotta luottamuksellisuus syntyy ja säilyy. Käyttöoikeudet rajaavat sen, mitä tiedolle saa tehdä. Tiedon suojauksen toiminnallisuus takaa sen, että saatuja oikeuksia käytetään tarkoituksenmukaisesti eikä niitä rikota tai väärinkäytetä.

Autenttisuudella tarkoitetaan menetelmiä, joilla varmistetaan esimerkiksi se, että tietojen käyttöoikeudet ja -luvat tulevat oikeilta tahoilta. Tähän käsitteeseen liittyy tiiviisti kiistämättömyys. Kiistämättömyydellä tarkoitetaan, että määräyksen antaja ja tehtävän toimeksiantanut ei voi kiistää jälkeenpäin tehtäväksiantoa. Autenttisuus ja kiistämättömyys voidaan teknisesti aikaansaada julkisen avaimen salauksen avulla. Tietoturvan näkökulmasta autenttisuutta voidaan vahvistaa digitaalisella allekirjoituksella, johon tarvitaan julkisia avaimia.

Tietoturvan ydinaluetta ovat yksityisyyden suojan ja henkilötietojen käsittelyn periaatteet ja toimintatavat. Tietoturvan tulee olla korkempaa tasoa, jottei tietojen luottamuksellisuus, tiedon eheys tai tiedon saatavuus vaarannu. Suojattavan tiedon eheyteen liittyy tässä tapauksessa vaatimukset alkuperäisyydestä, koskemattomuudesta ja kiistämättömyydestä.

2.1 Yksityisyyden suoja

Yksityisyyden suojalla tarkoitetaan henkilön oikeutta yksityisyyteen, johon kuuluu muun muassa oikeus määrätä itseään koskevista asioista ja tiedoista. Tämä oikeus on sekä henkilötietolaissa [26] että perustuslaissa [63]. Yksityisyys on luonnollisen henkilön oikeus suojautua ulkopuoliselta puuttumiselta. Euroopan ihmisoikeussopimus [13] julistaa artiklassa 8 ihmisen oikeudesta yksityiselämään sekä perhe-elämän kunnioittamisesta siten, että jokaisella on oikeus nauttia kunnioitusta, joka kohdistuu yksityis- ja perhe-elämään, kotiin ja kirjeenvaihtoon. Ihmisoikeussopimuksessa ilmoitetaan myös, etteivät viranomaiset saa puuttua tuon oikeuden käyttämiseen muutoin kuin lain sallimissa rajoissa tai jos se on kansallisen ja yleisen turvallisuuden vuoksi välttämätöntä. Viranomaiset voivat puuttua ihmisoikeuteen myös siinä tapauksessa, jos maan taloudellisen hyvinvoinnin, terveyden tai moraalin suojaamiseksi tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi se on välttämätöntä [13].

Yksityisyys tarkoittaa myös sitä, että henkilöllä on oikeus tulla arvioiduksi oikeiden ja oleellisten henkilötietojen perusteella. Ihmisellä on siis oikeus omiin henkilötietoihinsa. Henkilötietolain [26] mukaan henkilötiedoilla tarkoitetaan henki-

löä tai hänen ominaisuuksiaan kuvaavia merkintöjä. Henkilötietolakia on sovellettava henkilötietojen automaattiseen käsittelyyn tai kun käsiteltävät henkilötiedot muodostavat tai niiden on tarkoitus muodostaa henkilörekisteri. Henkilörekisteriksi käsitetään ne yhteenkuuluvat merkinnät henkilöstä, jotka ovat käyttötarkoituksen vuoksi tallennettu tietojärjestelmään [26]. Nykyisin monet tietojärjestelmät muodostavat henkilörekisterin ja ovat siten osaltaan vaikuttamassa yksityisyyden suojaan.

Henkilötietojen osalta yksityisyyden suojan määrittely tarkoittaa myös henkilötietojen suojaamista oikeudettomalta tai henkilöä vahingoittavalta käytöltä. Henkilötietolain (523/1999)[26] mukaan yksilöllä on oikeus tarkastaa, mitä tietoja hänestä on tallennettu henkilörekisteriin. Järvisen [31] mielestä esimerkiksi henkilön nimi- ja osoitetiedot eivät ole salaisia, mutta niiden aiheeton rekisteröinti ja tietojen yhdistely voi aiheuttaa haittaa yksityisyydelle.

Suomen perustuslain 10§:n mukaan henkilötietojen suojausta säädetään tarkemmin lailla. Kansallisen lainsäädännön lisäksi henkilötietojen suojausta säädetään sekä EU-tasoisella että kansainvälisellä lainsäädännöllä. Yksityisyyden suojan ja yksilön kunnioittaminen noudattamalla huolellisuutta henkilötietojen käsittelyssä on niin ikään perustuslain keskeinen periaate. Tietoaineiston turvallisuuden uhkien tunnistamisessa tulee huomioida myös yksityisyyden suojaan liittyvät tietosuojan seikat.

Yksityisyyden kaventumiseen voi vaikuttaa lainsäädäntö, mutta esimerkiksi myös ihmisen oma digitaalinen käyttäytyminen. Internetissä lähes kaikki mitä sinne kirjoittaa tai jakaa, tulee näkyväksi kaikille hetkessä. Yksityisyyden suojan merkitystä ei aina käsitetä. Viattomalta tuntuvan valokuvan julkaisusta voi tulla yksityisyyden suojan asia, sillä digitaalinen kuva usein sisältää Global Positionin System (GPS) paikannustietoa. Kuvan metatiedoissa on GPS-koordinaatit, joista saa analysoitua tarkasti sen missä kuva on otettu. Muun kuvan sisältämän liitännäistiedon kanssa sekä kuvakäsittelytekniikalla voi saada selville samantyyppisestä kuvamateriaalista yhdistellen entistä enemmän yksityisyyttä koskevaa tietoa henkilöstä itsestään, hänen perheestään, työpaikastaan tai kodistaan. Vaikkei käyttäisi internettiä lainkaan, ei ihminen voi välttyä esimerkiksi kauppareissullaan joutumasta valvontakameraan. [50]

Tietoturvallisuutta, tietoturvaa sekä tietosuojaa että yksityisyydensuojaa voidaan tarkastella useista näkökulmista: yksityisen henkilön, yrityksen, yhteiskunnan tai kansainvälisen turvallisuuden kannalta, kuten Järvinen [31] jaottelee. Henkilötietojen suojaan, yksityisyyteen liittyvien tietojen, viestien ja muun aineiston käsittelys-

sä on noudatettava huolellisuutta. Henkilötietojen käsittely on perusteltava ja käsittelylle on oltava asiayhteys [58]. Tarkoitussidonnaisuus tarkoittaa sitä, että henkilö tietää henkilötietoihinsa suostumusta antaessaan sen mihin henkilötietoja tullaan käyttämään ja luovuttamaan. Salmisen [58] mukaan käyttötarkoitussidonnaisuudella rajataan henkilötietojen käsittely toiminnan perustehtäviin. Tästä päästään Järvisen [31] mainitsemaan yrityksen näkökulmaan. Liiketoiminnan näkökulmasta on keskeistä pitää huoli tietoturvasta yrityksen omien liikesalaisuuksien ja asiakkaiden luottamuksen säilyttämisen vuoksi, mutta myös tietotyötä tekevien työntekijöiden näkökulmasta.

Neuvonen [50] on kiinnittänyt huomiota tarpeellisuusvaatimukseen ja käyttötarkoitussidonnaisuuteen e-passeissa, joihin vaaditaan nykyisin biometrinen tunniste, kasvokuva ja sormenjälkitiedot. Sormenjälkitietoja on aiemmin kerätty rikostutkimusten yhteydessä. Neuvonen kertoo, että Ranskassa käytiin vuonna 2013 Euroopan ihmisoikeustuomioistuimessa (EIT) ratkaisu, jossa EIT totesi, että sormenjälkitietojen tarpeeton säilyttäminen loukkaa yksityiselämän suojaa sekä haittaa henkilön mahdollisuutta päättää itse toiminnastaan. Ratkaisusta keskusteltiin Suomen perustuslakivaliokunnassa. Suomen passilain perusteella päädyttiin tulkintaan, että passirekisterin sormenjälkitietoja saa käyttää vain passeihin ja tietoja on säilytettävä erillään rikoksesta epäiltyjen henkilötuntomerkeistä.

Suomen tietosuojavaltuutetun toimiston [69] näkemys on, että yksityisyyden suojan kannalta erityisen herkkiä biometrisiä tunnisteita, joiden avulla voidaan tehdä päätelmiä henkilön sairauksista tai perimästä on syytä välttää. Henkilötietolaki [26] velvoittaa rekisterinpitäjän toteuttamaan tarpeelliset tekniset ja hallinnolliset toimenpiteet henkilötietojen suojaamiseksi sekä huomioimaan erityisesti huolellisen käsittelyn merkitys myös yksityisyyden suojan kannalta.

Järvinen [31] vertailee eri maiden yksityisyydensuoja-asioita ja toteaa, että Pohjoismaissa on lakisääteinen tietoturva viety pitemmälle kuin muualla. Neuvosen [50] mukaan monissa maissa viranomaisten hallussa oleva tieto on salaista. Pohjoismaissa tieto on lähtökohtaisesti julkista. Julkisuusperiaate kuuluu hyvään hallintoon. Yhdysvalloissa on Neuvosen mukaan erilainen järjestely. EU:n kansalaisille on tietosuojalain mukaan tulossa oikeus kieltää heitä koskevien tietojen keruu. EU komission näkemys on, että Yhdysvaltojen henkilötiedoille tarjoama suoja on riittämätön. Järvinen [31] päätyy samaan. Yhdysvalloissa yksityisyyden suojaan ei ole erityisesti panostettu lainsäädännössä ja siksi henkilötietoja on helpommin saatavilla kaupallisten toimijoiden ja yksityisyrittäjyyden vuoksi.

Oikeudeton henkilötietojen käsittely voi vahingoittaa henkilön yksityisyyden suojaa, kuten Valtionhallinnon tietoturvasanasto [73] kuvaa oikeudetonta toimintaa yksityisyyden loukkaamisella. Yhdysvalloissa laaditut terrorismin vastaisen sodan perusteella luodut lait vaikuttavat Euroopan unionin yksityisyyden suojaan. Näin ollen Suomessakin on todennäköistä, että tulevaisuudessa yksityisyyden suoja kapenee, kun viestiliikennettä mahdollisesti aletaan tarkkailla. Se ei ole siis pelkästään teknologiasta johtuvaa yksityisyyden suojan muutosta. Tietojärjestelmissä tulisi kuitenkin pyrkiä noudattamaan tietoturvan ja yksityisyyden suojan periaatteita mahdollisimman aikaisessa vaiheessa, eli käytännössä jo suunnitteluvaiheessa, kuten Meingast et al. [45] toteavat.

2.2 Henkilötietojen käsittely

Henkilötiedoilla tarkoitetaan henkilöä tai hänen ominaisuuksiaan kuvaavia merkintöjä. Henkilötiedoiksi luetaan myös henkilön elinolosuhteita kuvaavia merkintöjä, joita voidaan hänen itsensä lisäksi hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi tiedoiksi [58]. Henkilötietoja kerätään, tallennetaan ja järjestellään tarpeen mukaan. Se on monipuolista sähköistä tietojen käsittelyä. Tietoja käytetään, siirretään ja luovutetaan eri tarkoituksissa. Muina henkilötietojen käsittelytoimenpiteinä henkilötietolaissa [26] luetellaan henkilötietojen säilyttäminen, muuttaminen, yhdistäminen, suojaaminen, poistaminen ja tuhoaminen. Henkilötietoja tulee käsitellä laillisesti, huolellisesti ja hyvää tietojenkäsittelytapaa noudattaen. Hyvä tietojenkäsittelytapa on laissa säädetty velvollisuus.

Henkilötietojen käsittelyä arvioidaan EU komissiossa tai rekisterinpitäjän toimesta. Rekisterinpitäjällä tarkoitetaan henkilöitä, yhteisöä, laitosta tai säätiötä, jonka käyttöä varten henkilörekisteri perustetaan esimerkiksi lain perusteella [58]. Henkilötietojen luovutuksesta antaa Neuvonen [50] esimerkin EU ja Euroopan talousalueen (ETA) ulkopuolelle. Henkilötietojen luovuttamisen edellytys on, että tietoja on käsitelty lähtömaassa asianmukaisesti henkilötietolain ja -direktiivin mukaisesti. Toinen vaatimus on, että myös siellä maassa, jonne henkilötietoja siirretään noudatetaan samoja periaatteita. Henkilötietojen siirrosta on ilmoitettava tietosuojavaltuutetulle.

Euroopan unionin tietosuojauudistus on hyväksytty vuonna 2015. Tietosuojauudistukseen kuuluu tietosuoja-asetus ja direktiivi, jota viranomaiset soveltavat vuodesta 2018 lähtien käsitellessään henkilötietoja. Tietosuojalla on tavoitteena paran-

taa yksilön tietosuojaa ja luottamusta sähköisiin palveluihin. Tarve henkilötietojen parempaan suojeluun on kasvanut tekniikan nopean kehityksen ja globaalien tietoverkkojen syntymisen vuoksi. Erilaiset henkilön tunnistamis- ja valvontajärjestelmät mukaan lukien biometrian käyttö on yleistynyt paikkoihin, joissa ihmiset liikkuvat paljon. Henkilötietoja kerätään yhä kehittyneimmin keinoin. Euroopan komission julkaisema Eurobarometri 2015 [15] kyselytutkimuksen mukaan henkilötietojen luovuttamista koskevaan kysymykseen vastattiin yli 70 %:sti, että henkilötietojen antaminen on jatkuvasti kasvava osa nykyelämää. Suurin luottamus barometrissa oli terveydenhuollon laitoksiin ja vähiten luottamusta verkossa toimiviin palveluihin. 67 %:a vastaajista epäilee sitä, että viranomaiset eivät pidä turvassa verkossa olevia henkilötietoja. Identiteettivarkauksista on huolissaan 68 %:a EU kansalaisista. Tietojen keräämistä on entistä vaikeampi havaita.

2.3 Julkisen avaimen järjestelmä

Tietoturvaan liittyy myös tunnistamisratkaisut. Public Key Infrastructure (PKI) on julkisen avaimen hallintajärjestelmä. Järjestelmä sisältää salausmenetelmän, joka käyttää avainpareja, joista toinen on julkinen ja toinen salausavain on yksityinen. International Civil Aviation Organization (ICAO) standardin [29] mukaan PKI muodostuu sovituista menettelytavoista, prosesseista ja teknologiasta. PKI-menetelmällä on standardi X.509, joka määrittelee varmenteiden todentamismenettelyjä [35]. Julkisen avaimen hallintajärjestelmällä varmennetaan tietojen oikeellisuus ja luottamuksellisuus. Mentelmää siis käytetään tietoturvan varmentamiseen ja tietoturvallisiin viestiyhteyksiin.

Tietojen salauksella tarkoitetaan varmennettuja menetelmiä ja työkaluja, joiden turvin tietoja voidaan suojata. Tähän kokonaisuuteen PKI-menetelmä on rakentunut. Se hyväksikäyttää julkisen avaimen salaustekniikkaa, jossa avain on salainen, algoritmi julkinen. Julkinen avain on asymmetrinen ja salakirjoituksella koodattu, jolloin salauksen avaamiseen tarvitaan vastaavaa yksityistä avainta [32]. Toisella avaimella salataan, toisella puretaan auki. Yksityinen avain on vain käyttäjän tiedossa [29].Salausavaimet liittyvät toisiinsa monimutkaisella matemaattisella tavalla. Avaimet ova pitkiä perustuen suuriin kokonaislukuihin. Julkisen avaimen salaustekniikka tarkoittaa epäsymmetrisen salauksen menetelmää, missä kaikki osapuolet omaavat avainparit, joita käytetään salaukseen ja sähköiseen allekirjoitukseen.

Varmenteella tarkoitetaan sähköistä todistusta eli sertifikaattia, joka siis sisältää julkisen avaimen, jolla varmenteen omistajan pystyy tunnistamaan. Sertifikaatti on toimivaltaisen viranomaisen antama turvallisuustodistus, varmenne siitä, että tietotekninen palvelu täyttää tietoturvallisuustasoa vastaavat vaatimukset. Sertifikaatti todentaa henkilöllisyyden ja liittää allekirjoituksen todentamistiedot allekirjoittajaan. Tätä turvallisuustodistusta voidaan käyttää vahvassa sähköisessä tunnistamisessa sekä sähköisessä allekirjoituksessa, joka on liitetty tai joka loogisesti liittyy muuhun sähköiseen tietoon. Varmenteita ja nimettyjä varmentajia julkisen avaimen infrastuktruuksi. PKI:n varmentajat tuottavat käyttäjille avainparit. Riippuen hieman sovellusalueesta, avainparien luominen voidaan hoitaa myös toisaalla. Avainparit varmennetaan sähköisella allekirjoituksella, jonka tarkoitus on suojata viestin eheyttä. Allekirjoituksen jälkeen avainparit jaetaan järjstelmän käyttäjille. Digitaalisen allekirjoituksen on katsottu kiistämättömyyden lisäksi takaavan paremmin myös tiedon eheyttä ja muuttumattomuutta sen lisäksi, että se varmentaa tietyn viestin sisällön ja lähettäjän henkilöllisyyden.

Suomessa laki väestötietojärjestelmästä ja Väestörekisterikeskuksen (VRK) varmennepalveluista (661/2009) sekä laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009) muodostavat varmennepolitiikan lainsäädännöllisen perustan. Laki [40] määrittelee varmenteen sekä digitaalisen allekirjoituksen ja niiden käyttötarkoituksen. VRK:n tehtävänä on tuottaa varmenteita kansalaisille ja organisaatioille. Varmenteita tarvitaan tietoverkoissa sähköisessä tunnistamisessa, salauksessa sekä sähköisessä allekirjoituksessa. VRK myöntää esimerkiksi e-passin biometriatietojen PKI-menetelmään perustuvat allekirjoitusvarmenteet.

PKI sisältää tietoturvaa lisääviä toimintaperiaatteita. Prosessit ja tekniikka on yhdistetty niin, että ratkaisua käyttämällä voidaan tietoturvaa vaativien sovellusten käyttäjät varmentaa ja todistaa oikeiksi. Sen jälkeen järjestelmä päästää käyttäjät kirjoittautumaan haluttuun tietojärjestelmään tai toiminnallisuuteen. Pääsynvalvontaa voidaan siten turvata salauksella. Tietojen kiistämättömyyden vaatimus on sähköisissä allekirjoituksissa oleellisin piirre. Vahvalla salaustekniikalla luotu järjestelmä takaa allekirjoituksen oikeellisuuden. Todennus kuuluu Järvisen [32] tietoturvaperiaatteista ongelmallisimpiin. Todentamisella varmistetaan ihmisten henkilöllisyys. Todentamisella varmistetaan aitous, kun on kysymys tietokoneohjelmista tai vaikkapa biometrisestä matkustusasiakirjasta, e-passista. Julkisen avaimen teknologia mahdollistaa luottamuksellisuuden ja pääsynvalvonnan [35].

3 Biometriset tunnisteet

Biometriset tunnisteet ovat ihmiskehon ainutlaatuisia piirteitä. Ei ole olemassa kahta ihmistä, joiden tunnuspiirteet olisivat täysin samanlaiset, ei edes identtisillä kaksosilla. Ihmisen geneettinen koodi ja yksilöllisyys muotoutuu jo hedelmöityksessä. Sikiöllä on viikosta kahdeksan lähtien yksilölliset kasvot ja sormenjälkitiedot [10]. Biometrisillä tunnistetiedoilla tarkoitetaan henkilön tunnistamisessa käytettäviä ja henkilön yksilöiviä tietoja, jotka perustuvat luonnollisen henkilön fysiologiseen ominaisuuteen tai käyttäytymiseen. Biometristen tunnisteiden avulla henkilö voidaan tunnistaa lähes varmasti [69]. Pavesic et al. julkaisukoosteessa [47] pitävät juuri erotettavuutta tärkeänä ominaisuutena. Lisäksi biometriseen tunnisteeseen liittyy muuttumattomuuden ominaisuus. Muuttumattomuus mahdollistaa vertailun ja tunnistamisen.

Biometriset tunnisteet ovat universaaleja ja yleismaailmallisia, siltikään ne eivät ole samanarvoisia, sillä jokaisessa yksilössä on omia tunnuspiirteitä, joita tulee hienovaraisesti kunnioittaa. Tietoturvallisuuden luottamuksellisuuden osa-alueella biometria toimii hyvin, sillä biometrisiä tietoja saavat käsitellä vain ne henkilöt, joilla siihen on lain mukaan oikeus. Tiedon eheys ja kiistämättömyys luovat perustan biometriseen tunnistamiseen.

Biometristen tunnisteiden kerääminen on maailmanlaajuinen ilmiö. Syitä löytyy lainsäädännöstä, jossa taustalla on turvallisuustekijöitä ja muita kansallisia operatiiviseen toimintaan liittyviä julkisia palveluja, mutta myös yksityissektorin tarpeita. Sähköisten palveluiden lisääntyminen, esimerkiksi digitalisoituminen, on luonut paineita kehittää varmoja ja luottamukselliseen tunnistamiseen tarkoitettuja biometrisiä ratkaisuja. Yleisimpiä perimään, ilmiasuun tai olemukseen perustuvia biometrisia tunnisteita ovat kasvokuva, sormenjäljet, silmän iiris ja ääni. Biometrisia tunnisteita käsitellään taulukon 3.1 mukaisessa järjestyksessä yksityiskohtaisemmin erityispiirtein sekä fysiologisten ja käyttäytymiseen perustuvien ominaisuuksien mukaan.

Taulukko 3.1: Biometriset tunnisteet jaoteltuna ominaisuuden mukaan.

Fysiologinen	Käytökseen perustuva
Kasvokuva	Ääni
Sormenjälki	Allekirjoitus
Silmän iiris	Kävelytyyli
Käden geometria	Näppäimistön käyttö
Korvan geometria	

3.1 Fysiologiset tunnisteet

Fysiologiseksi tunnisteiksi luokitellaan kasvokuva, sormenjälki, iiris, käden ja korvan muodot. Ailisto et al. [3] mukaan fysilologiset piirteet voivat muodostaa yksityisyyden suojan riskejä, sillä fysiologiset biometriset tunnisteet ovat pysyviä ja lähes muuttumattomia. Näitä ihmisen normaaliin kehoon ja elimistöön sekä toimintaan kuuluvia biometrisia tunnisteita käsitellään tarkemmin kasvotunnistuksen, silmän iiristunnistuksen, käden geometrian ja korvanlehden tunnistamisen tavoissa.

Fysiologisia biometrisia tunnisteita voidaan luokitella eri tavoin, vaikkapa tungettelevuusasteen mukaan, kuten Harel [25] on esittänyt. Vähiten häiritsevänä pidetään kasvotunnistamista. Kasvokuvan ottamisesta ja sen antamisesta ei juurikaan kieltäydytä herkkätunteisuuteen tai epämielyttävyyteen vedoten. Kasvotunnistus on luonnollista vuorovaikuttamista ihmisten välillä, mutta sitä on käytetty myös etätunnistuksessa koneellisesti. Kasvotunnistukseen perustuva teknologia on kehittynyt videokuvasta tunnistamiseen. Tunnistamismetodina kasvotunnistusta ei edes juurikaan vastusteta yleisellä tasolla. Siksi se on erittäin paljon käytetty operatiivisessa toiminnassa esimerkiksi identifioinnissa vastaamassa kysymykseen - kuka sinä olet?, verifioinnissa kysymykseen oletko se, joka väität olevasi? - kuin valvontasovellusten parissa.

3.1.1 Kasvokuva

Kasvokuva on visuaalinen esitystapa henkilön kasvoista. Kundra et al. [37] yksinkertaistavat kasvotunnistuksen perustuvan mittasuhteisiin, silmien asentoon ja paikkaan kasvoissa sekä nenään ja suuhun. Kasvokuvasta paikannetaan mallinteen avulla kasvot siten, että kuviot erotellaan ja luokitellaan kasvonpiirteittäin suun, silmien ja nenän muotojen, viivojen ja mittasuhteiden mukaan. Tietokannassa suorasuuntai-

sesti otetut kasvokuvat ovat tallennettuina Joint Photographic Expert Group (JPEG)-muodossa. ICAO 9303 standardin mukaan passin kasvokuvan koko tulee olla 45.0 mm x 35.0 mm mitoiltaan, mistä muodostuu riittävä resoluutio (300 dots per inch (DPI)) myös kasvotunnistuksen tarpeisiin [29]. JPEG-tekniikan avulla kompressoituna kuvasta saadaan 64 kilotavun kokoluokan tiedosto. Esimerkiksi Yhdistyneiden kuningaskuntien ja Amerikan yhdysvaltojen e-passeissa kasvokuvan resoluutio on 300 dpi verran.

3.1.2 Sormenjälki

Sormenjälki muodostuu ihmisen sormenpäähän erilaisista yksilöllisistä kohoumaja urakuvioista, joita voidaan havainnollisesti kuvailla harjanteiksi tai laaksoiksi, kuten Kundra et al. [37] selvittävät. Ihmisen sormenpäiden kohoumat, harjanteet ja kuviot kehittyvät sikiöaikana raskausviikolla 19, jolloin geenit määräävät sormenjälkikuvion yleispiirteet. Muut yksityiskohdat muodostuvat kehityksen aikana, kun sikiön sormet ovat kosketuksissa kohdussa lapsiveteen ja sen ympärillä olevaan. Sormenjälkimuoto säilyy ihmisen elämän ajan, vaikka sormenpää vaurioituisi, on uuden ihonmuodostuksen jälkeenkin sormenjälkikuvio samanlainen kuin aikaisempi. Tämä johtuu siitä, että ihon alla on näkymättömissä aivan sama sormenjälkikuvio. Pato ja Millet [49] esittävät, että sormenjälkiä voidaan ottaa joko yksityiskohtaisesti niin sanottujen minutiae -pisteiden tai rakenteellisen koostumuksen perusteella (texture). Minutiae tarkoittaa kohoumien ja jakaumien päätöskohtia sormenjäljissä. Minutiae voi olla muodoltaan niin sanottu päättyvä erikoiskohta (ridge ending), se voi olla muodoltaan haarautuma (bifurcation) tai piste (dot), kuten Accursio [2] on määritellyt.

Koska sormenjälkitieto on havainnollinen ja muuttumaton, sitä on paljon käytetty tunnistamisessa. Bromban [6] arvio on, että sormenjälkitunniste tulee säilymään vahvana. Sormenjälkitietojen keräämisen historiasta Coppock [9] kertoo, että sormenjälkitiedot otettiin rikolliselta kaikista kymmenestä sormesta ja tiedot olivat tallessa erityisillä korteilla. Musteella otettu sormenjälkikuva voitiin ottaa joko painamalla (plain impression) tai pyöräyttämällä (rolled impression). Federal Bureau of Investigation (FBI) pystyi tekemään vertailuja laajasta sormenjälkitietojen kokoelmasta, mutta se korvasi paperiset sormenjälkikortit digitaalisella kuvastolla käyttäen Wavelet Scalar Quantization (WSQ) algoritmiin perustuvaa -WSQ-tekniikkaa.

Sormenjälkitunnisteella voi tunnistaa henkilön yli miljoonan ihmisen joukosta, kun esimerkiksi kasvotunnistus rajoittuu noin tuhanteen ihmiseen. Sormenjäljen ot-

taminen on helppoa, mutta siihen tarvitaan erillinen lukijalaite (skanneri), jonka lasille sormi tai sormet painetaan. Coppock [9] käyttää tästä tavasta myös termiä livescan. Skannerin lasille heijastuu peilin kautta sormenjälkitiedot, josta kamera ottaa kuvan, jonka resoluutio 1000 dpi on riittävä sormenjälkitietojen keräämiseksi. Digitaalisessa kuvassa pikseleiden määrä muodostaa kuvan ja erottelutarkkuus on sen resoluutio. Mitä suurempi resoluutio kuvassa on, sitä tarkempi muodostettu kuva on, jolloin myös sen vertailutarkkuus on parempi. ICAO standardissa [29] suositellaan sormenjälkitiedon kooksi etäluettavalle sirulle 10 kilotavua per sormi. Tiedosto tulee pakata WSQ-tekniikalla, jota on tyypillisesti käytetty sormenjälkikuvien tiivistämisessä.

3.1.3 Iiris

Silmän rakenteessa on värikalvo eli iiris. Iiriksen keskellä on pupilli. Iiriksen kuva pysyy lähes muuttumattomana ja yksilöllisenä niin oikeassa kuin vasemmassakin silmässä. Lehpamerin [41] mukaan henkilön silmän iiriskuvio määräytyy jo ennen syntymää ja säilyy muuttumattomana koko elämän ajan, jollei silmä vaurioidu. Biometrisena tunnisteena iiristunnistusta ei pidetä liian tungettelevana, vaikkakin käytännön tasolla tunnisteen kerääminen vaatii silmän valottamista infrapunavalolla.

Iiristunnistamista käytetään enimmäkseen henkilön identifiointiin. Tunnistamistoimenpiteen aikana vaaditaan henkilön aktiivista osallistumista ja vapaata tahtoa. Iiristunnistuksen teknologia muodostuu Kundra et al. [37] mukaan selkeästi havaittavissa olevasta värillisestä ympyrästä silmän pupillin ympärillä. Iiriksessä on noin 266 erotettavaa piirrettä, kuten esimerkiksi renkaita, uurroksia ja valokehä. Lehpamerin [41] mukaan iiriksen kuvio on biometrisista tunnisteista kaikkein tarkin. ICAO standardissa [29] suositellaan biometrisen tunnisteen kooksi etäluettavalle sirulle 30 kilotavua per silmä.

3.1.4 Käden geometria

Uusin menetelmä esimerkiksi rikostutkinnan sovelluksissa tai henkilöllisyyden selvittämisessä on tutkia sormenjälkien lisäksi myös kokonaista kämmenen kuvaa. Käden geometria muodostaa samalla tavalla yksilöllisen tunnisteen kuin sormenjälkitiedon uniikit piirteet. Käden geometriaan perustuva biometrinen tunniste vastaa toimintamuodossaan verifiointia. Mittaaminen vaatii henkilön läsnäoloa ja yhteistyötä. Fyysinen kontakti lukijalaitteen kanssa sekä kädessä olevien muotojen valot-

taminen on välttämätöntä. Pato ja Millet [30] mukaan käden geometriatietojen saaminen on helppoa, koska siinä mitataan kämmenen leveys sekä sormien leveys ja pituus. Käden geometrian tunnistustekniikoita on ainakin kahden tyyppistä. Käden selkämys ja sivuprofiili voidaan kuvata tai käyttää tunnistamisessa kämmenen kuvan jälkeä. Riippumatta siitä kumpaako menetelmää käytetään, se ei välttämättä ole tarpeeksi erotteleva varsinkaan kun suuria ihmispopulaatioita käsitellään. Mittamisessa saatua tulosta verrataan vain yhteen mallinteeseen. Koska tunnistuslaitteen on oltava ihmisen kämmenen kokoinen, on tässä rajoitteita infrastruktuurissa sekä pienempiin laitteisiin integroinnissa.

Eglitis et al. [12] esittelevät bimodaalisen biometrian piirteitä kämmenen kuvasta. Kysymys on kahdesta kuviosta, mitkä voidaan saada yhdestä Red Green Blue (RGB) -kuvasta. Bimodaalisuus tarkoittaa tässä yhteydessä verisuonien ja ryppyjen kuvioita kämmenen geometriassa. Vaikka tutkijoiden prototyypin testitapauksessa oli mukana vain 64 ihmisen tiedot, tulokset olivat keskimääräisesti positiivisia. Tutkimustuloksissa verifiointi tuotti 70.6% verisuonihavainnoista oikein ja 64.7% kämmenen rypyistä tai kuvioista oikein. Tutkimuksessa on käytetty RGB-kuvan kanssa sensoria, mikä mahdollistaa näiden kahden erilaisen tunnisteen yhtäaikaisen suodattamisen.

3.1.5 Korvan geometria

Biometrisena tunnisteena voi olla myös ihmisen korvan lehti. Tunnistus tapahtuu kuvatun korvan muodon perusteella. Sana ja Gupta [59] ovat testanneet biometrista tunnistusratkaisua ja saaneet testituloksissa yli 90%:n tarkkuustason. Korva on helposti tunnistettavissa kasvokuvasta ja tunnistetiedon kerääminen on tutkijoiden näkemyksen mukaan vaivattomampaa kuin sormenjälkien tai iiristunnistuksen menetelmissä. Korvan lehdestä otetaan RGB-kuva, joka muunnetaan harmaasävykuvaksi. Kuvaa käsitellään siten, että korvan kuva skaalataan sopivan kokoiseksi, jotta sitä voidaan verrata muihin näytteisiin. Vertailussa käytetään mallinnetta (template) ja tietojärjestelmiä.

3.2 Käyttäytymiseen perustuvat tunnisteet

Ihmisen käyttäytymiseen perustuvat biometriset tunnisteet ovat puheääni, allekirjoitus, kävelytyyli ja tietokoneen näppäimistön käyttötapa. Käyttäytymiseen perus-

tuvat biometriset tunnisteet voivat muuttua eikä niiden osalta Ailisto et al. [3] pidä suurta riskiä yksityisyyden kannaltakaan. Käytösperusteisista tunnisteista voidaan käyttää myös yhteisesti termiä looginen biometrikka. Ihmiselle ominaisten toimintatapojen tunnistaminen on biometrian osalta käyttäytymiseen perustuvaa tunnistamista. Seuraavassa näitä ominaisuuksia käsitellään tarkemmin.

3.2.1 Ääni

Ihmisen puheääni on biometrinen tunniste, josta Ailisto et al. [3] ovat tehneet tutkimuksia. Äänitunnistamiseen tarvitaan menetelmiä, jossa tunnistetaan ääninäytteen perusteella henkilö tietokannassa oleviin puheen ääninäytteisiin (voice print) vertaamalla. Ääninäytteen ottaminen on helppoa, se ei vaadi kovinkaan erityisiä laitteita, kuten monet muut biometriset tunnisteet. Ääninäyte ei vie myöskään paljon aikaa, vaikkakin näytteen luotettavuuden vuoksi sitä tulee ottaa kahdesta kolmeen kertaan. Äänen tai puheen muodostus on yksilöllistä lähinnä ääntöelinten muuttumattomuuden vuoksi. Sen sijaan puhe voi olla erilaista ääninäytteen antamisen hetkellä, sillä ihmisen henkinen ja fyysinen tila vaikuttavat syntyvään ääneen. Ääninäyte voidaan antaa kommunikaatiovälineiden avulla, eikä siis vaadi henkilön fyysistä läsnäoloa. Automaattinen puheen tunnistaminen (speaker recognition) voidaan jakaa tekstiperusteiseen tai tekstiriippumattomaan tunnistustapaan. Äänitunnistamiseen perustuu myös esimerkiksi mobiilipuhelimiin integroitujen komponenttien hyväksikäyttö musiikintunnistamispalveluihin. Puhelimen mikrofonin avulla jo muutaman sekunnin soiton jälkeen, äänitietokanta palauttaa tiedot tunnistetusta musiikkikappaleesta.

3.2.2 Allekirjoitus

Allekirjoitusta voidaan verrata staattisella tai dynaamisella tavalla ja saada yksilöllisiä eroja tulokseksi. Visuaalisesti samanlaiset allekirjoitukset ovat staattisia. Dynaamiseen vertailuun tarvitaan laajempaa kirjoitusprosessin vertaamista, jossa tutkitaan kirjoitusnopeutta ja rytmiä. Tämä vaatisi tarkempaa ohjelmallista analyysia siitä, mikä on yksilön ominainen tapa kirjoittaa. Pato ja Millet [30] toteavat, että allekirjoitusta on kautta aikojen käytetty tunnistamismenetelmänä. Allekirjoitus vaaditaan passinhaltijalta e-passiin sen tietosivulle hakemusvaiheessa, sillä nimikirjoitus on henkilötunnistuksen vanha käytäntö. Valtioneuvoston asetuksen 362/2015 [72] mukaan erityistilanteessa hakijan nimikirjoituksen tilalle voidaan passiin merkitä

viiva. Allekirjoitustapa voi vaihdella henkilön tunnetilojen mukaan. Allekirjoitustapahtumaan voi vaikuttaa yksinkertaisesti fyysiset olosuhteet ja tilanne, jossa allekirjoitus annetaan.

3.2.3 Kävelytyyli

Kävelytyyli on yksilöllinen, mutta siihen vaikuttaa jalkineet, vaatteet sekä pinta, jossa ihminen kävelee. Kävelytyylin tunnistamiseen käytetään kuvaustekniikkaa ja tunnistamiseen liittyy paljon erilaisia parametreja, jonka Pato ja Millet [30] toteavat. Esimerkiksi henkilön hahmo ja ääriviivat, askelluksen tahti ja järjestys ovat muuttuvia tekijöitä. Menetelmää tutkitaan ja kehitetään edelleen.

3.2.4 Tietokoneen näppäilyrytmi

Tietokoneen näppäimistön käyttö ja siitä muodostuva näpyttelyrytmi on jonkun hypoteesin mukaan yksilöllisesti erotettavissa muista. Väitettä on vaikea todentaa täysin varmaksi. Pato ja Millet [30] epäilevät, että näppäimistön dynamiikka on kuitenkin hyvin pitkälle olosuhderiippuvainen. Henkilön tunnetila voi vaikuttaa siihen, missä tahdissa hän näppäilee. Lisäksi henkilön ryhti ja se missä asennossa näppäily tapahtuu vaikuttavat näppäimistön käyttöön. Tietokoneen näppäimistön tyypillä on myös merkitystä. Tietokoneen käytössä myös hiiren napautus voi olla yksilöllistä ja tunnistettavaa.

3.3 Muut tunnisteet

Muitakin kuin fysiologisen tai käyttäytymisen perusteella luokiteltavia biometrisia tunnisteita on Ailisto et al. [3] mukaan hyödynnettävissä. Solun perintötekijöitä sisältävä kemiallinen yhdiste, desoksiribonukleiinihappo (DNA) on tulevaisuuden biometrinen tunniste. Yksityisyyden suojan näkökulmasta DNA on herkkä tunnistetapa. Harelin [25] mukaan DNA teknologia toimii identifioinnin välineenä, mutta vaatii kuitenkin asiantuntevan ihmisen varmistamaan tuloksen ja päätöksen tekemisen. DNA näytteen etuna on, että se on iätön. DNA:ssa säilyy mitä enenemässä määrin yksilöön liitettävää dataa, jota voidaan myöhemmin yhdistää perheenjäseneen, etniseen taustaan tai muuhun tulevaan käyttötarkoitukseen.

Sormenjälkitietojen lisäksi on kehitetty sormien verisuonistoon perustuva tunnistamistapa. Kauba et al. [34] esittelee sormen verisuoni tunnistusmenetelmän. Sor-

men verisuonet voi erottaa infrapunavalolla. Sormen verisuonitunnistamisen etuna verrattuna sormenjälkiin on, että kuva saadaan, vaikka sormenpäät olisivat hankautuneet tai kuluneet. Sormenjälkitunnistaminen voi olla vaikeaa silloin kun sormenpää on kuiva, likainen, viilletty tai muutoin vaurioitunut.

Silmän rakenteeseen kuuluva verkkokalvo eli retina on niin ikään tutkimuskohteena biometriseksi tunnisteeksi. Verkkokalvon kuvausmenetelmä on vaativa, sillä henkilön tulee keskittää katseensa kameraan ja olla liikkumatta kuvaushetken ajan, jotta verkkokalvon rakenne saadaan tarkasti kuvattua. Ailisto et al. [3] tutkimuksessa mainitaan, että kahden silmiin perustuvan menetelmän yhdistelmä - iiris ja retina - on erittäin tarkka ja luotettava.

3.4 Käsittelyvaiheet

Biometristen tunnisteiden käsittelyssä voidaan erottaa kolme eri vaihetta: tietojen kerääminen, kerättyjen tietojen vertailu olemassaoleviin tunnisteisiin sekä tunnistamisen prosessi. Biometristen tunnisteiden käsittelyvaiheissa on tyypillistä ihmisen aktiivinen osallistuminen tietojen saamiseksi. Tietojärjestelmiin on rakennettu biometristen tietojen käsittelysääntöjä. Biometristen tietojen käsittelyyn tarvitaan erityisiä laitteita kuten sormenjälkitunnistuslaitteita ja silmänpohjantunnistuslaitteita. Seuraavassa näitä vaiheita tarkastellaan lähemmin.

Kerääminen

Biometrisen tiedon keräämisestä voidaan käyttää termiä enrollaus, kuten Ailisto et al. [3] määrittelevät. Enrollauksessa biometriset tiedot kerätään tietojärjestelmään ja samalla henkilöstä rekisteröidään myös muita henkilötietoja. Suomessa biometrisia tunnisteita voidaan kerätä ja tallentaa tietojärjestelmiin huomioiden henkilötietolain [26] sekä muiden lakien asettamat vaatimukset tietojen keräämisestä, käytöstä ja säilyttämisestä.

Sormenjälkien keräämisen tarvittavia laitteita on olemassa yhden sormen lukijoista monisormilukijoihin sekä hipaisuun perustuvia sormenjälkilukijalaitteita että kosketusvapaita malleja. Yhteydettömästi toimivat lukijat (contactless fingerprint scanner) eivät vaadi lukutapahtumassa kosketusta laitteeseen. Lukijalaite pystyy ottamaan liikkuvasta kädestä neljä sormenjälkitietoa ja muodostamaan niistä sovelluksen avulla sormenjälkitiedot. Sellaisiin kohteisiin, joissa on paljon jatkuvaa eri

ihmisten sormenjälkitietojen keräämistä, kuten kulunvalvonnassa tai rajatarkastuksissa sopisi kosketusvapaata teknologiaa soveltava sormenjälkilukijalaite, sillä se on hygieenisempi kuin kosketuspintaan perustuva skanneri.

Vertailu

Biometrista vertailua voidaan suorittaa erilaisten biometristen tunnisteiden avulla. Yleisesti voidaan todeta, että biometriset uniikit tunnisteet ovat tuoneet kaivattua parannusta tekniseen vertailuun ja tunnistamiseen. Uusia menetelmiä käytetään laajasti ainakin sormenjäljillä ja kasvotunnistuksessa. Käden ja sormen muodoilla, äänentunnistuksella ja silmän iiriksen skannauksella on myös käyttöä, josta Rebne tutkimuksessaan [56] kirjoittavat. Teknisesti ottaen biometrinen tieto ei eroa esimerkiksi aakkosnumeerisesta henkilönumerosta, kun vertailussa olevaa dataa sovelletaan tietojärjestelmän tietokannassa. Vertailuun tarvitaan menetelmiä, sääntöjä ja luokittelutapoja. Biometrinen tieto voi toimia vertailuavaimena, jos avaimeen liittyy henkilö ja avaimella sallitaan pääsy jonnekin fyysiseen tilaan tai palveluun.

Biometristen tunnisteiden keräämiseen tarkoitetuilla laitteilla poimittu biometrinen informaatio muunnetaan sopivan mallipohjan kautta biometrisen järjestelmän ymmärtämään tiedostoformaattiin. Vertailutulos voi perustua numeerisiin ja matemaattiseen malliin. Tuloksena voi olla matemaattinen indikaattori, esimerkiksi prosenttiluku, joka ilmaisee kuinka samanlainen mitattava biometrinen tunniste on verrattavan tunnisteen kanssa.

Yksinkertaistettuna henkilöön liittyvässä vertailussa on kysymys ihmisen fyysisestä ulkonäöstä ja siitä, kuinka ihminen tulee tunnistetuksi sekä siitä, kuinka ihminen pystyy tunnistamaan toisen ihmisen. Vertailua voidaan tehdä silmämääräisesti tai automatisoidusti. Kasvotunniste on yksi käytetyimmistä biometrisista tunnisteista passeissa, mutta se ei ole paras mahdollinen. Kasvokuvasta tunnistamiseen perustuvissa järjestelmissä sovelletaan esimerkiksi kolmiulotteista (3D) tekniikkaa ja infrapunavalokuviin perustuvaa tunnistamistekniikkaa [37]. Ihmiset muuttavat hiustyyliään, parta tai sen puuttuminen muuttaa kasvokuvaa ja vaikeuttaa tunnistamista. Kasvotunnistamisen automatiikan algoritmi perustuu jälkimmäisen kuvan täsmäämiseen aikaisemman kuvan kanssa, jolloin toiseen henkilöön tehty vastaavuus tuottaa virheellisen hyväksynnän (false acceptance). Jos hakutoiminto hylkää tietokannassa olevan henkilön, muodostuu tästä käsite virheellinen hylkäys (false rejection). Van der Ploeg [74] kuvailee, että kohdatessamme tuntemattoman hen-

kilön käytämme eräänlaisia ruumillisia johtolankoja luokitellaksemme ihmisen johonkin kategoriaan. Tunnistaminen ja todentaminen voi kuulostaa teknisesti hankalalta, mutta on ihmisten kesken hyvin arkipäiväinen ilmiö.

Tunnistaminen

Biometrisella henkilötunnistamisella tarkoitetaan yleisesti automaattista tapaa tunnistaa henkilö fysiologisten ominaisuuksien tai käyttäytymisen perusteella, kuten Pavesic et al. julkaisusarjassa [47] määrittelee. Biometrian käyttöönottoa ja tunnistamisen etua puolletaankin seuraavista syistä:

1. tunnistettava henkilö vaaditaan olemaan fyysisesti läsnä tunnistamispisteessä
2. henkilön tunnistaminen perustuu biometriseen ominaispiirteeseen eikä mukana tarvita erillisiä salasanoja tai muita henkilötodisteita
3. biometrisia tunnisteita ei voi kovin helposti siirtää, unohtaa, kadottaa tai kopioida

Biometrista henkilötunnistamista käytetään henkilön yksilöimiseen, sillä se tuo vakautta tunnistamiseen, koska biometrisiä tunnisteita on vaikea vaihtaa [69]. Biometriset tunnisteet ovat mitattavissa olevia tietoja; niitä on ensin kerätty, tallennettu ja sitten vasta niitä voidaan verrata olemassaoleviin tunnisteisiin. Vertailutilastot osoittavat, etteivät kahdet eri henkilön sormenjäljet ole riittävän samanlaiset tullakseen tulkituksi identtisiksi. Biometrisistä henkilötunnisteista varmimpana pidetään edelleen sormenjälkitunnisteita [9].

3.5 Biometrisia sovellusalueita

Biometriaan perustuvia sovelluksia käytetään sekä julkisella että yksityisellä sektorilla. Valtionhallinto, armeija ja kaupalliset toimijat hyödyntävät biometriaa. Yhteiskunnalle välttämättömät infrastruktuurin edellytykset ovat lisänneet turvallisuusalalla biometrian käyttöä. Kulunvalvonta ja laitteiden käytön esto tai pääsy biometriikka-avusteisesti on lisääntynyt. Sähköisiä palveluita ja sovelluksia liittyen virkakortteihin, henkilökorttiin (eID), e-passeihin, viisumeihin tai e-pankin ratkaisuihin on tullut lisää. Biometrisia sovelluksia on kehitetty investointihankkeisiin

ja rahaliikenteeseen, vähittäiskaupan alalle sekä rikostutkintaan. Myös terveydenhuolto sekä sosiaaliala ovat biometrian vaikutusalueena. Biometrian mitattavuus on vaikuttanut siihen, että sovelluksia on kehitetty runsaasti eri toimialoille [10].

Käyttökohteet ja perusteet biometristen tunnisteiden hyväksikäyttöön vaihtelevat laajasti. Peruslähtökohtana on nopea ja varma tunnistaminen. Järvinen [31] jaottelee todennusmenetelmiä keinotekoisiin ja biometriaan perustuviin. Keinotekoisia tunnistusmenetelmiä ovat esimerkiksi käyttäjän salasanat. Oikea salasana ei takaa, että käyttäjä on oikea, mutta järjestelmät suorittavat käyttäjätietoihin perustuvan tunnistuksen ja antavat sen perusteella valtuutuksen. Laitteiden välinen todentaminen perustuu yleensä salaukseen tai sovittuun protokollaan. Automatisoinnilla pyritään tehokkuuteen ja kustannussäästöihin [30]. Liikenne- ja viestintäministeriön tutkimuksessa [3] on esimerkkejä biometristen tunnisteiden käyttämisessä. Yhteistä kaikille on biometrisen tunnistamisen tarkkuus, virheettömyys ja tietosuoja. Koska järjestelmät laajenevat, tulee tietojen jatkuva käytettävyys, tietojen eheys ja luottamuksellisuus sekä fyysinen tietoturvataso nousta vastaavasti korkealle tasolle.

Biometriset järjestelmät voidaan luokitella unimodaalisiin ja multimodaalisiin järjestelmiin. Tutkimuksen [47] mukaan unimodaalisessa, yhden tunnisteen järjestelmässä virheiden määrää pidettiin korkeana, eikä näitä tunnisteita suositeltu laajamittaisiin tietojärjestelmiin, kuten esimerkiksi biometrisiin matkustusasiakirjoihin.

Biometrinen tunnistaminen ei ole koskaan täydellisen varmaa, koska kyse on ihmisistä ja ihmisen ainutlaatuisista ominaispiirteistä. 100 %:n varmuustasolle tuskin koskaan päästään millään yksittäisellä biometrisellä tunnisteella. Hyvä algoritmi tuottaa mahdollisimman vähän virheellisiä tunnistuksia [1]. Mutta yhdistelemällä erilaisia biometrisia tunnisteita voidaan päästä parempiin ja tarkempiin tuloksiin.

Multimodaaliset järjestelmät sisältävät useamman biometrisen tunnisteen yksilöstä. Tämän vuoksi järjestelmää pidetään turvallisuustasoltaan muita korkeampana. Väärennyksien tai huijauksen estämisen kannalta järjestelmä on varmempi, sillä huijarin täytyisi pystyä kehittämään useampia tunnisteita pystyäkseen hyödyntämään oikeudettomasti saamiaan biometrisia tunnisteita. Eglitis et al. [12] mukaan lisääntyneet turvallisuusvaatimukset ovat syynä multimodaalisien biometriajärjestelmien käyttöön. Esimerkiksi kämmenen verisuoniston rakenne ja kämmenen kuvioiden analysointi näkyvällä kuvalla sekä infrapunavalolla muodostaa jo modaalisen biometrisen järjestelmän.

Biometrian yhdistäminen muihin tietoihin tehostaa toimintaa. Harel [25] esittää miten useampaakin erityyppistä biometrista tietoa voidaan nykyisillä automaatti-

sen tietojenkäsittelyn välineillä hankkia, varastoida, hakea ja yhdistellä. Yleisesti ottaen, tietojärjestelmien laskentateho on kasvanut. Älykkäitä algoritmejä on keksitty. Siksi on luonnollista, että myös biometrisia hakutuloksia voidaan jatkokäsitellä helposti ristiintarkastuksilla, tiedon louhintatyökaluilla, analysoimalla ja tunnistamista tukevilla tavoilla. Mitä monipuolisemmin tietoa on käytettävissä, sitä useampi toimija tietoa hyödyntää.

3.5.1 Biometrinen todentaminen

Biometrinen todentaminen perustuu ihmisen tunnistamiseen jonkin fysiologisen tai käyttäytymiseen kuuluvan piirteen perusteella. Verifiointi on yksi osa biometrista todentamista ja siihen kuuluu biometrinen tunniste. Toisinaan todentamisesta käytetään autentikointi-termiä. Järvisen [31] mukaan autentikoinnin tarkoitus on varmistua oikeellisuudesta. Biometrisen todentamisen tavoite on niin ikään varmistua siitä, että todennettava henkilö on se, joka hän väittää olevansa.

Todentamisen voi suorittaa henkilö, mutta se voi olla myös laite tai muu tekninen ohjelmisto. Todentamisen osalta henkilön aitoutta varmistetaan luottamustasolla. Luottamustason katsotaan perustuvan ominaisuuksiin, jota tunnistettava henkilö tietää tai joita tunnistettavalla henkilöllä on tai joka henkilö on. Järvisen [32] mukaan henkilön todennus pohjautuu johonkin, mitä henkilöllä on hallussaan, mitä henkilö tietää ja johonkin henkilön yksilölliseen ominaisuuteen. Biometrisen todentamiseen käytettävän piirteen tulee olla helposti mitattavissa ja sellainen, joka lähes kaikilla ihmisillä on olemassa. Piirteen pitäisi olla riittävän erottuva ja yksilöllinen, kuitenkin tarpeeksi pysyvä ja muuttumaton samalla ihmisellä. Tunnistamistilanteessa henkilö voi tietää henkilökohtaisen koodin tai salasanan, henkilöllä voi olla hänelle myönnetty passi tai muu henkilökortti. Se fyysinen seikka, jotain mitä henkilö itse siis on, kuuluu Järvisen [31] mukaan tekniseen todentamiseen silloin kun ihmisen ominaisuuksia käytetään todentamisessa. Tällöin on kyseessä biometrinen tunnistaminen.

Todentaminen biometrisen tunnisteen avulla pohjautuu edellämainittuun henkilön yksilölliseen ominaisuuteen. Kun tunniste kerätään, käynnistyy verifioinnin prosessi. Verifioinnilla tarkoitetaan yhden suhde yhteen (1:1) tunnistamista [3]. Tästä biometrisen näytteen vertaamisesta yksittäiseen vertailunäytteeseen on käytetty myös termiä yksittäisvertailu. ICAO standardin [29] mukaan verifiointi tarkoittaa biometrista vertailua siihen tunnisteeseen, jonka sähköisen matkustusasiakirjanhaltija antaa nyt verrattuna siihen, mitä hänestä on aikaisemmin järjestelmään kerätty.

Saatu tulos vastaa kyselyn suorittajalle yksiselitteisesti siihen, onko tunnistettava henkilö se, joka hän väittää olevansa.

3.5.2 Biometrinen identifiointi

Toinen henkilön tunnistamistapa tarkoittaa identifiointia eli yhden suhde moneen (1:n) tunnistamista [29]. Tämä käsite voidaan mieltää myös moneenvertailuksi. Identifiointi määrittää henkilön persoonan tunnistamisen ja siinä toimenpiteessä etsitään esimerkiksi useita identiteettejä tietokannasta. Identifiointimenettelyllä henkilö tunnistetaan kaikista muista henkilöistä yksiselitteisen ominaisuuden perusteella, muttei sen perusteella mitä henkilö tietää. Identifiointitilanteessa henkilöllä ei tarvitse olla todistetta henkilöllisyydestään.

Ailisto et al. [3] mukaan identifioinnissa on suurempi yksityisyyden suojan riski, koska biometrisia tunnisteita verrataan suureen joukkoon samantapaisia mallinteita. Pato ja Millet [30] esittävät ajatuksen, että tunnistamisprosessissa tosiasiallisesti tutkitaankin ihmisen samankaltaisuuksia. Tunnnistamisalgoritmit on rakennettu sen mukaan mitä biometrista tunnistetta käytetään tunnistamisvälineenä. Identifiointiprosessin tulos vastaa ilman alkuoletustietoja tehtyyn kyselyyn sitä suorittavalle mahdollisesti tunnistettavan henkilön oikealla identiteetillä kysymykseen - kuka sinä olet? Luonnollisesti on mahdollista, ettei henkilöä pystytä tunnistamaan biometristen tunnisteidenkaan avulla.

3.6 Biometrian tietoturva

Biometrian tietoturvaa voidaan tarkastella henkilöstöturvallisuuden ja tietoaineistoturvallisuuden osa-alueilla. Erilaisia rooleihin ja vastuisiin, tietoturvaohjeisiin sekä sähköisen tietoaineiston käsittelyyn ja säilyttämiseen liittyviä tietoturvahaavoittuvuuksia on pyrittävä ennakoimaan. Tietosuojavaltuutetun toimiston julkaisu [69] ohjeistaa, että tunnistamista varten kerätty biometrinen tieto on aina suojattava. Tämä vaatimus tulee myös Euroopan unionin passiasetuksen [11] teknisistä lisäeritelmistä. Biometrinen tunniste on suojattava myös tunnistautumisen käsittelyn aikana, esimerkiksi silloin kun matkustusasiakirjan tietoja tarkistetaan. Suojatuksi tallennusvälineeksi, jolle biometriikkaa e-passille tallennetaan, on valittu RFID-siru. Viranomaiskäytössä olevissa sovelluksissa lainsäädännöllä on pyritty varmistamaan tietosuojaa, mutta näin ei välttämättä ole yksityisen sektorin biometriaa soveltavissa

järjestelmissä.

Biometriikan käytöstä seuraa, että tietoturvavaatimukset kasvavat ja riski tietosuojasta nousee. Esimerkkinä potentiaalisista henkilösuojaan liittyvistä haavoittuvuuksista Harel [25] mainitsee joukon tahoja, joista voi löytyä henkilöitä, joiden käsityskyky tai ymmärrys on heikolla tasolla. Näitä toimijoita voi löytyä biometristen tietojen käsittelyketjusta julkisen hallinnon ja rikostutkinnan virkamiehistä. Vallan keskittyminen voi olla tietoturvauhka. Se ei ole pelkästään viranomaisiin liitettävä uhka. Myös muut toimijat, jotka käsittelevät biometrisia tietoja muodostavat potentiaalisen haavoittuvuuden. Sidosryhmät, kaupalliset toimijat, insinöörit ja järjestelmän kehittäjät, väärinkohdellut tai muutoin huolimattomat, ahneet tai korruptoituneet henkilöt, joilla on pääsy biometrisiin tietoihin muodostavat erityyppisiä uhkia, jotka tulee tunnistaa ja joihin tulee varautua.

Swaminatha ja Elden [68] lähestyvät tietoturvaa I-ADD -prosessilla. I-ADD tulee englannin kielen sanoista Identify, Analyse, Define, Design. Tunnistaminen (Identify) tarkoittaa tietoturvan näkökulmasta sitä, että biometristen tietojen käsittelyn yhteydessä tulisi tunnistaa potentiaaliset roolit, joissa tietoturvauhka piilee. Pahansuopa käyttäjä voi kuulua organisoituun rikollisryhmään, jonka motiivina on raha. Hakkereilla vaikuttimena ei ole taloudellinen hyöty, vaan maine tai kunnia. Ilkeämielinen ohjelmoija voi toimia taloudellisen edun tavoittelemiseksi tai vaikkapa tuotemerkin vahingoittamistarkoituksessa. Akateemista tutkijaryhmää tai tietoturvatutkijoita ei luokitella suoranaisesti mitenkään häijyksi, mutta heidän vilpitön ja syvällinen tutkimustapansa ja tulosjulkaistut voivat hyödyttää niitä, joilla on motiivi tietoturvan vaarantamiselle. Lopuksi Swaminatha ja Elden mainitsevat kokemattomat langattoman verkon ohjelmoijat, suunnittelijat ja ylläpitäjät, joilla ei ole tarvittavaa osaamista, mutta jotka voivat silkkaa tietämättömyyttään muodostaa tietoturvauhkia tietojärjestelmiin ja näin ollen myös biometrisiin järjestelmiin. Bogari et al. [4] ovat tutkineet e-passin tietoturvaa ja ovat saaneet selville, että toisen sukupolven e-passin tietosuojaa hyökkääjät koettelevat muilla kuin teknisillä keinoilla; näitä ovat viranomaisiin kohdistuneina lahjonta, uhkailu ja kiristys.

3.7 Biometrian yksityisyyden suoja

Biometriset tunnisteet ovat riippuvaisia toisistaan, koska niitä verrataan joko henkilön omiin aikaisempiin tunnistetietoihin tai kaikkiin niihin tunnisteisiin, joita tietojärjestelmässä on. Tähän liittyy biometrinen yksityisyyden suoja sekä verrannol-

lisuuskäsite. Biometrian verrannollisuus tarkoittaa teknistä tilannetta, jossa kysely tietokantaan suoritetaan, mutta samalla siitä ei saisi tuottaa mitään sellaista tietoa, jota voidaan verrata tietokannassa oleviin muihin tietoihin. Biometrinen haku tulisi olla mahdollisimman yksiselitteinen. Teknisten ratkaisujen tulisi Bringer ja Chapanne [5] mukaan vastata biometrisen tunnistamisen verifioinnin (1:1) sekä biometrisin tiedon identifoinnin (1:n) vastaavuuksiin yksityisyyden suojan näkökulmasta.

Van der Ploeg [74] pitää biometriaa osana valvontaverkostoja. Ihmisistä kerätty biometrinen tieto tallennetaan järjestelmiin, joissa näitä tietoja haetaan, tarkastetaan sekä verrataan. Kysymys on kontrollista. Esimerkkisovelluksena valvontakameroiden keräämää kasvokuva-aineistoa verrataan tietojärjestelmässä oleviin mallinne tietoihin ja tulokset näytetään valvontamonitoreissa. Multimodaalisissa järjestelmissä kontrolloitava biometrinen tieto voidaan kerätä useammalla sensorilla, useammalla näytteellä tai useammalla biometrisellä tunnisteella.

Biometrisen tunnistamisen osalta yksityisyyden suojan kysymys nousee siitä, kun biometrisellä tunnisteella tehdään tietokantaan haku, mitä tietokanta antaa vastaukseksi? Jos on kyseessä henkilö, jonka tiedot löytyvät tietokannasta, saako tuloksen mukana nousta esiin muuta tietoa henkilöstä? Yksityisyyden suojan näkökulmasta vastauksen mukana ei saisi esittää muita tietoja kuin tismalleen sen, mitä hakutulokseen on tarkoitusperäisesti vaadittu. Toinen seikka, jos osumaa ei löydy ja biometrista tunnistetta tarjoaa kyselyyn toiseksi henkilöksi tekeytynyt huijari, mitä tietoja tietokannan tulisi siinä tapauksessa antaa vastaukseksi? Biometrisen tietokannan olisi tarkoitus antaa vain niitä vastauksia ja palveluja, joihin se on alunperinkin tarkoitettu. Järjestelmää ei saa käyttää mihinkään muuhun tarkoitukseen kuin tunnistamiseen. Tietojen urkkijan ei pitäisi saada missään vaiheessa tietoonsa niitä tekijöitä, mistä kysely tai sen vastaus koostuu. Tietokannan sisältö ei saa paljastua. Esimerkiksi vastaukseksi ei saisi tulla useita mahdollisia identiteettejä. Identiteetin suoja tarkoittaa tutkimuksen [5] mukaan myös sitä, ettei tietojärjestelmän pitäisi mitenkään oppia sitä, mitä identiteettejä tietokannassa on.

Pääasiallinen viesti teknisen tunnistamisen osalta on siinä, että vaikka kuinka hyvin pystyttäisiin salaamaan biometrinen tieto rekisteröintivaiheessa tai tietokannassa itsessään, ei se ole riittävää. Biometrisella tunnisteella tietokannasta saadut vastaukset kun eivät välttämättä ole kryptattuja. Korkeaa tietoturvaa vaativissa biometrisissa sovelluksissa näin kuuluisi varmasti olla.

4 RFID

Radio Frequency Identification, RFID on radiotaajuustunnistustekniikkaa. RFID-tunniste kuuluu objektiin, josta RFID:n mikrosirulla olevia yksilöllisiä tietoja voidaan langattomasti lukea [42]. Tekesin tutkimuksessa Seppä ja Uusikylä [62] määrittelevät tekniikkaa etätunnistamiseksi, jossa tietoa etäluetaan ja -tallennetaan radiotaajuuksilla toimivien tunnisteiden avulla.

RFID edustaa sähkömagneettista radioaaltotekniikkaa, jonka avulla esineitä, eläimiä ja ihmisiä voidaan etälukea ja tunnistaa. Tunnistamisen mahdollistaa mikrosirulla oleva yksilöivä tunniste, joka on yhdistetty tai kiinnitetty esineeseen, eläimeen tai henkilöön. Yleisesti käsittäen tunniste sisältää yksilölliset tiedot, joiden avulla objektin identiteetti on tunnistettavissa ja todennettavissa. Tunnistaminen tapahtuu ilmarajapinnan kautta etälukuna, ilman manuaalista käsittelyä langattomasti. Siksi RFID tunnetaan myös etätunnisteena, jonka kokonaisjärjestelmään kuuluvat tunnisteet, lukijat ja tietojärjestelmä.

RFID-ratkaisuja kehittivät 1970 -luvulla aktiivisesti yliopistot, yritykset ja julkishallinto. Tuloksena syntyi käytännön sovelluksia esimerkiksi eläinten merkitsemisessä, autojen avaimisissa, tehdasautomaatiossa sekä sairaaloissa ja muissa julkishallinnon kohteissa. 1990 -luvulla teknologiakehitys oli muutoinkin kiivasta ja tästä RFID-teknologia hyötyi vanavedessä, kun mikroelektroniikkaan integroitiin RFID ja langattomien järjestelmien sovellukset omaksuivat RFID-tekniikkaa. RFID-järjestelmiä pilotoidaan maksamiseen ja lippujärjestelmiin liittyvissä hankkeissa ja erilaisissa maksukorteissa. Järjestelmiä testataan ja on otettu käyttöön esimerkiksi lentoliikenteeseen liittyvissä osajärjestelmissä, rakennusalalla erilaisiin antureihin kytkettynä esimerkiksi betonivalun kosteuden mittamisessa, sillan rakenteiden valvonnassa, liikenteen seurannassa, autoverojen tai tietullimaksujen keräämisessä, vaarallisten aineiden kuljetuksissa, lääkepakkauksissa ja kyselylomakkeissa. Terveys- ja hyvinvointipalvelut tulevat lisäämään RFID-tunnisteen käyttöä vanhusten hoidossa. [41]

2000 -luvun RFID-teknologian innovaatiot ja ratkaisut otettiin laajamittaisesti käyttöön, sillä radiotaajuuksia ja standardeja saatiin tuolloin sovittua. RFID-teknologia valittiin mukanakuljetettaviin henkilöllisyyttä osoittaviin asiakirjoihin - passeihin

ja henkilökortteihin. Esimerkiksi 2010 -luvulla RFID integroitiin matkapuhelimiin, vaikkakin innovaatio oli saanut alkunsa jo 1990 - luvulla [65].

4.1 RFID-standardit ja toimijat

RFID-tekniikan alan standardeilla on suuri merkitys, sillä vaikka lisenssejä ei tarvittaisi, on tarpeen hallita radiotaajuudet ja niiden toimijat. Lehpamer [41] on koostanut melko kattavasti standardoimistyötä tekevät toimijat, jotka esitellään seuraavassa tarkemmin.

RFID:n kokonaisratkaisun osalta standardointi on käynnistynyt oikeastaan vasta 2000 -luvun alkupuolella [76]. Kansainvälinen yhteisö, EPCglobal ratifioi vuonna 2004 RFID-standardin ja on edelleenkin kehittämässä radiotaajuuksiin perustuvia etätunnistuksen teknologiaratkaisuja. EPCglobal on voittoa tuottamaton standardointiorganisaatio ja sen pääasiallinen tahtotila on tuottaa yleinen, universaali sähköiseen tuotekoodiin perustuva globaali tietoverkko, jossa automaattinen tavaroiden tunnistaminen toimitusketjussa on mahdollista.

Euroopan tasolla toimii lyhytaaltojen ja taajuuksien jakamiseen liittyvissä asioissa standardisoinnissa European Radiocommunication Office (ERO). ERO toimii yhdessä Electronic Communications Committee (ECC) kanssa, mikä puolestaan vaikuttaa tietoliikennealan säätelykomiteassa, joka on siis European Conference of Postal and Telecommunications Administrations (CEPT). Muita aktiivisia standardointiin liittyviä toimijoita RFID:n alalla on The European Telecommunications Standards Institute (ETSI). Sen tekninen ryhmä on ETSI TG34, jonka työn tuloksena syntyi EPCglobalin kanssa yhteistyössä standardi ETSI EN 302 208-2, joka Lehpamerin [41] mukaan sisältää merkittäviä parannuksia ja teknistä kehittämistä RFID-teollisuudelle. Lentoliikenne on alunpitäenkin ollut RFID:n kehityksen alkuajoista mukana, joten on luonnollista, että The International Air Transport Association (IATA) tutkii ja kehittää RFID-teknologiaa mm. lentomatkustajien matkatavaroiden hallinnassa.

Matkustusasiakirjojen viitekehyksessä toimii International Civil Aviation Organization (ICAO) ja sen alatyöryhmä Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD). TAG/MRTD työllä on ollut tärkeä paikka passien ja viisumien määrittelytyössä kehittäessään sekä ihmissilmin luettavia että koneluettavia matkustusasiakirjastandardeja. Standardit kuuluvat ICAO Doc 9303 -sarjaan, johon liittyy tiiviisti yhteydettömän integroidun mikrosirun, Integra-

ted Chip (IC) määrittely ja ISO/IEC 14443 - standardi [30].

International Organization for Standardization (ISO) ja International Electrotechnical Commission (IEC) ovat sitoutuneet tekemään valtavia standardointitoimenpiteitä useilla RFID-teknologian aloilla. Tuloksia on tullut ISO/IEC Joint Technical Committee 1 (JTC1) alaryhmässä 17, joka koskee ID-kortteja ja henkilötunnistamista sekä alaryhmässä 31, joka koskee automaattista tunnistamista ja tietojen keruuta. The International Telecommunication Union (ITU) on Yhdistyneiden Kansakuntien (YK) alainen toimisto tietoliikennealalla, joten näissäkin järjestöissä on toimialoja, joissa RFID-teknologiaan liittyviä kysymyksiä ratkaistaan. ITU-R on radioviestinnän alalla toimiva taho ja ITU-T toimii televiestinnän sektorilla maailmanlaajuisesti. [41]

4.2 RFID-tunniste ja peruselementit

RFID-teknologia rakentuu kolmesta elementistä Mohamed et al. [46] mukaan seuraavasti:

1. RFID-tunnisteesta (tag, transponder), johon kuuluu antenni ja mikrosiru
2. RFID-lukijalaitteesta (reader, transceiver), johon kuuluu antenni
3. Sovellusjärjestelmästä (data processing subsystem), johon kuuluu tietojärjestelmät

Elementeille on olennaista saumaton yhteentoimivuus. Tyypillinen RFID-järjestelmä koostuu siis pienestä RFID-tunnisteesta, jolla on yksilöivä tunniste ja tuotekuvaus sekä RFID-lukijalaittesta, jolla on tietoteknistä kyvykkyyttä ottaa selville tunnisteen tiedot ja välittää niitä eteenpäin tietojärjestelmälle ja sen tietokantaan [36].

RFID-tunnisteesta käytetään useita englanninkielisiä nimityksiä kuten tag, transponder, integrated chip, RFID-chip. Suomeksi RFID-tunnisteesta on erilaisia nimityksiä kuten esimerkiksi: tagi, älytarra, RFID-tarra, etätunniste.

RFID-tunnisteen koko sekä muoto vaihtelee riippuen sovelluksesta ja objektista, johon tunniste on kiinnitetty. Alkujaan HF-tekniikkaan perustuvan tunnisteen koko oli noin 2,5 cm x 2,5 cm. Lukuetäisyys kasvoi 50 cm:iin, mikä on nykyään myös LF-taajudella toimivan etätunnisteen lukuetäisyys. Tunnisteen koko voi olla vaikkapa pulverityyppisessä tunnisteessa todella pieni hiukkanen (kooltaan 0,05 mm x

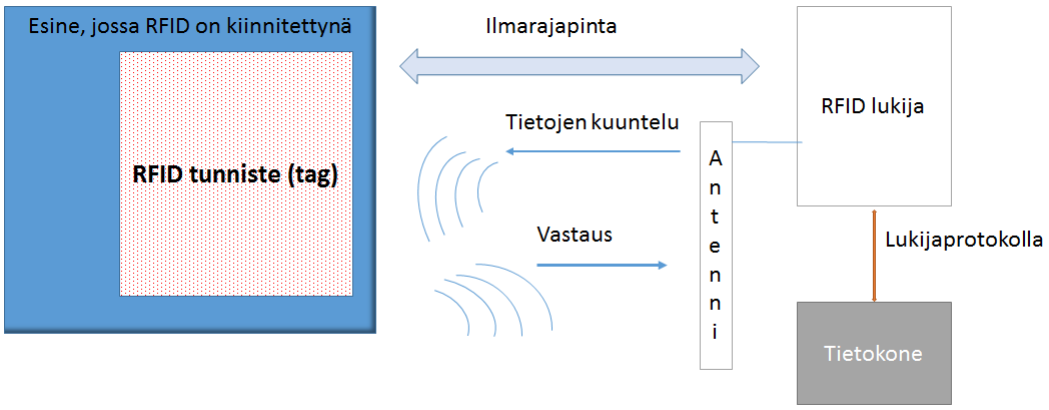
0,05 mm x 5 μm). Kun toisaalta tunnisteen mitat voivat olla suurikokoisissa tunnisteissa esimerkiksi 140 mm x 25 mm x 8 mm. Mohamed et al. [46] mukaan ISO 7810 -standardi määrittelee e-passin RFID-sirun fyysisiä piirteitä. E-passissa RFID-tunniste on kooltaan 125 mm x 88 mm. E-passiin integroiduissa tunnisteissa tulee olla sisäänrakennettu antenni [46]. Antenni ja sen materiaali määrittelee enemmänkin tunnisteen kokoa kuin siinä oleva mikrosiru.

RFID-tunnisteessa on muistipiiri, jossa on vaihteleva määrä tallennuskapasiteettia biteistä kilotavuihin. Esimerkiksi e-passin etätunnisteelle voi Vaudenayn [75] mukaan tallentaa 512 kilotavua dataa ICAO:n matkustusasiakirjoja koskevan standardin määrittelemän loogisen tietorakenteen, Logical Data Structure (LDS) vaatimalla tavalla. ICAO standardin [29] etäluettavan sirun tiedon tallennuskapasiteettia koskeva määritys asettaa minimiksi 32 kilotavua, jotta sirulle mahtuu pakolliseksi määriteltyä tietoa (esimerkiksi kasvokuva, jonka koko on 15 - 20 kilotavua). ICAO ei määritä maksimikapasiteettia sirulle.

Tunnisteessa olevan tiedon määrä voi vaihdella sen muistin mukaan [65]. RFID-tunnisteen mikrosiruun tallennettavan tiedon koko voi olla identifiointiin perustuvissa siruissa 64:stä bitistä kerran kirjoitettavaan passiivisen tunnisteen vaatimaan 96:een bittiin. Glover ja Bhatt [20] laskevat, että 96 bittiä riittää nykyisin yksilöimään objektin, johon tunniste laitetaan. Hypoteettisessa esimerkkilaskelmassa maapallon kaikille ihmisille (noin 7.4 miljardia) varattaisiin 33 bittiä tunnisteessa, jolloin se riittäisi nykyiseen väestömäärään ($2^{33} = 8.589,934,592$).

EPC-standardin [22] mukaan RFID-tunnisteen tiedot jaetaan kolmeen osaan: liiketoiminta (business data), kontrolli (control information) ja valmistajatiedot (tag manufacture information). Ensimmäiseen osaan kuvataan se fyysinen objekti, johon tunniste kiinnitetään. Toinen osa on tiedon keräämiseen liittyvälle datalle varattua tilaa. Kolmanteen osaan tulee valmistajatieto, jossa tunniste yksilöityy. ISO/IEC 18000-1:2008(E) määrittää tunnisteen yksilöiviä tietoja sarjanumeron tarkkuudella [66]. Sirun valmistajan antama tunnisteen yksilöllinen koodi voi olla 48-bittinen ISO/IEC 7816-6 mukainen tai uniikki tunnistenumero voi perustua ANSI INCITS 256 -määrittelyyn, jolloin valmistajan sarjanumerolle on käytettävissä 64 bittiä. Valmistajilta vaaditaan yksilöllisten tunnisteiden rekisteröintiä, jotta tunnisteiden ainutlaatuisuus ja yksilöllisyys säilyy.

Etätunniste voi olla tyypiltään passiivinen, semi-passiivinen (puoli-passiivinen) tai aktiivinen [65]. Passiivinen RFID toimii lähettämällä signaalia, johon tunniste vastaa heijastamalla takaisin signaalia. Passiivisessa tunnisteessa ei ole virtalähdet-



Kuva 4.1: RFID-järjestelmän peruskomponentit.

tä [36]. Identifiointiin tarkoitetut tunnisteet ovat passiivisia kerran kirjoitettavia tunnisteita. RFID:n älytarra saa energiansa lukutapahtumassa syntyvässä sähkömagneettisesta kentästä. Tästä seuraa, että sirun muistissa oleva data moduloi tunnisteen käämin virtaa. Semi-passiivisessa ja aktiivisessa RFID-tunnisteessa voi olla akku tai paristo virtalähteenä. Aktiivisessa RFID-järjestelmässä se voi sisäisen virtalähteensä vuoksi lähettää signaalia lukijalaitteelle, kun semi-passivinen ei tätä tee [36]. Glover ja Bhatt [20] luokittelevat tunnisteita tarkemmin vielä sen mukaan onko tunniste vain lukumuodossa vai luku- ja kirjoitusmuodossa ja vaatiiko se esimerkiksi salausta ja onko tunniste uudelleen kirjoitettava.

4.2.1 RFID-lukijalaite

RFID-lukijalaite (reader, transceiver) pystyy langattomasti ilmarajapintaa käyttäen lukemaan RFID-tagilta tiedot. RFID:n etuna on se, ettei suoraa näköyhteyttä vaadita RFID-tunnisteen ja lukijalaitteen välille. RFID-lukijalaite lähettää kantoaaltoa samaan aikaan kun se vastaanottaa kohteen etätunnisteesta heijastunutta moduloitua kantoaaltoa [62].

Ilmarajapinnan parametrit ja taajuudet on määritelty ISO/IEC 18000-7:2009(E) [67] standardissa. Lukijalaite voi yhden sekunnin aikana lukea useita tunnisteita, mutta se pystyy tunnistamaan keskimäärin vähintään kaksi tunnistetta sekunnissa. Nopeus toki vaihtelee tunnistetyypeittäin. Esimerkiksi e-passiin on integroitu niin sanottu varmennettu turvasiru, jota lukijalaitteella luetaan julkisen avaimen hallintamenetelmän mukaisesti. Lukijalaite saa konelukuriviltä avaimen datan lukuta-

pahtumaan sirulle [44]. Avaintenvaihtomenetelmä estää Choi et al. [8] mukaan tietoliikenteen salakuuntelun luomalla Data Encryption Standard (DES) -salausalgoritmilla kooditetun kanavan luettavan kohteen ja lukijalaitteen välille. Abid et al. [1] mukaan RFID-tunnisteissa toimii salaustekniikka. Yksi vaihtoehto on käyttää Elliptic Curve Cryptography (ECC) -salaustekniikkaa.

Useamman tunnisteen lukemisen ja vastaanottamisen yhtäaikaisuus voi aiheuttaa lukijalaitteella yhteentörmäyksiä. Törmäyksenestoalgoritmit ovat tunnistetyyppikohtaisia ja ne määritellään standardeissa, esimerkiksi ISO/IEC 18000-2 [66] mukaan. Lukijalaite pystyy myös mahdollisesti kirjoittamaan tunnisteelle tietoa, mutta tämä toiminallisuus on harvinaista eikä vielä täysin standardoitu. Lukijalaitteelta saatua tietoa puolestaan hyödyntää tietojenkäsittelyjärjestelmä.

RFID-signaalien kulkemista voidaan suhteellisen helposti estää tai heikentää materiaalivalinnoilla. Esimerkiksi metalli toimii signaalin heikentäjänä. Pidemmän toimintasäteen ratkaisussa signaali voidaan torjua vaikkapa ihmiskeholla. Tutkijat pyrkivät suunnittelemaan uudenlaisia antenneja yhä pienempiin ja monimuotoisempiin tunnisteisiin samalla kun lukijalaitteiden valikoima ja tarkkuustaso kasvaa. [41]

4.3 RF-taajuudet

Radio Frequency (RF) on alle 300 MHz:n taajuisten radioaaltojen yleinen ilmaisu radiotekniikassa. Taulukossa 4.1 luetellut radioaaltojen taajuusalueet perustuvat Räisäsen ja Lehdon [55] radiotekniikan lähteeseen. Taulukkoon on sisällytetty passivisille tunnisteille olevia enimmäislukuetäisyyksiä Glover ja Bhattin [20] mukaan.

RF-aaltoihin luokitellaan taulukosta 4.1 kirjainlyhenteillä VHF, HF, MF, LF ja VLF merkittyjä taajuusalueilla toimivia radioaaltoja [55]. Lehpamerin [41] mukaan tyypilliset taajuudet tämän päivän RFID-sovelluksissa sijoittuvat välille 125 kHz - 245 GHz. RFID toimii lisenssivapaasti, mutta esimerkiksi lukijalaitteelle on asetettu maakohtaisia rajoituksia [65]. Suomen Standardisoimisliiton [65] mukaan ensimmäiset passiiviset RFID-tunnisteet perustuivat magneettikenttään ja toimivat LF-taajuusalueella, jossa lukuetäisyys oli noin 10 cm.

Taajuuksien ja kaistojen valvonta sekä standardointi on tärkeää radiotekniikan alalla. Suomen Standardisoimisliiton [65] mukaan RFID-tunnisteiden ja lukijalaitteiden toteutukset ovat keskittyneet neljälle taajuuskaistalle käyttökohteiden soveltuvuuden mukaan. RFID-tunnisteita käytetään LF-taajuudella alle 135 kHz, HF-taajuudella 13,56 MHz, UHF-taajuudella 869 MHz - 928 MHz ja 433 MHz sekä mik-

Taulukko 4.1: Radioaaltojen taajuusalueet (Radio Frequencies) Hertseinä (Hz) ja maksimi lukuetäisyys (cm). [55]

Lyhenne	Taajuuskaista	Taajuusalue (Hz)	Lukuetäisyys
VLF	Very Low	3-30 kHz	
LF	Low	30-300 kHz	lukuetäisyys 50 cm
MF	Medium	300-3000 kHz	
HF	High	3-30 MHz	lukuetäisyys 3 m
VHF	Very High	30-300 MHz	
UHF	Ultra High	300-3000 MHz	lukuetäisyys 9 m
SHF	Super High	3-30 GHz	
EHF	Extremely High	30-300 GHz	

roaaltoalueella 2,45 GHz tai 5,8 GHz. Mohamed et al. [46] mukaan lyhyt lukuetäisyys tarkoittaa myös sitä, ettei välitettävä tietomääräkään ole kovin iso. Yleensä yksilöivä tunnistekoodi välittyy, mikä on monessa RFID-sovelluksen tapauksessa riittävää. E-passien RFID-tunnisteet toimivat etälukuun perustuen 13,56 MHz radiotaajuudella. E-passeille sopii matala taajuus, sillä lukuetäisyys on lyhyt. Morshed et al. [48] mukaan e-passin lukuetäisyys on 10 cm perustuen ISO/IEC 14443 -standardiin. Radioaaltojen kantomatka tulee säilymään pienenä, jotta tietoturvaa on myös riittävästi.

Ensimmäiset HF-taajuuden ja RFID-teknologian lyhyen lukuetäisyyden Near Field Communication (NFC)-teknologiaa [62] sisältävät matkapuhelimet ilmestyivät vuonna 2004. Suomalainen Nokia oli tässä valmistajana. Käytännössä NFC-puhelin tarkoittaa sitä, että matkapuhelimessa on integroituna RFID-lukija, jonka lukuetäisyys ylettyy noin 4 cm päähän. Suomen Standardisoimisliiton [65] mukaan NFC-tekniikka eroaa RFID-tekniikasta juuri tästä sisäänrakennetusta toiminnasta, jossa tunniste pystyy toimimaan sekä lukijalaitteena että tunnisteena peer-to-peer (P2P) moodissa, luku- ja kirjoitustilassa sekä passiivisena tunnisteena. Tällä hetkellä tärkeimpinä RFID-tekniikan kehittämisen kannalta voidaan pitää juuri NFC-teknologiaa sekä lisäksi HF- ja UHF-tekniikoita.

4.4 RFID matkustusasiakirjoissa

Lehpamer [41] kirjoittaa, että RFID-teknologian etu on siinä, että valmistajat, vähittäiskaupat ja muut toimijat sekä viranomaiset voivat tehokkaasti kerätä, hallita, jakaa ja tallettaa tietoa varastoista, liiketoimintaprosessista ja turvatarkastuksista. RFID on monen sovellusalueen ratkaisu. RFID-tunnisteen käyttö näkyy lopputuotteena erilaisissa muovikorteissa tai muissa objekteissa (ranneke, avaimenperä, tarra) sisäänrakennettuina. RFID-tunnisteen sisältämistä korteista käytetään muun muassa seuraavia nimityksiä: sirukortti, älykortti, toimikortti, RFID-kortti. Englanninkielisiä termejä ovat esimerkiksi smart card ja chip card.

Integrointi RFID-tagin ja fyysisen passikirjan välillä on yksi tunnetuimmista koneluettavista sovelluksista [43]. RFID-tunnisteita käytetään henkilötunnistamiseen e-passeissa ja henkilökorteissa (ID). RFID:n ja biometrisen henkilötiedon yhdistäminen pitäisi parantaa tietosuojaa ja toimia identiteettivarkauksia vastaan. E-passinhaltijan kasvokuvan, sormenjälkien tai silmän iiriksen tietojen tallennus passiin upotetulle mikrosirulle mahdollistaa tietojen luettavuuden ohjelmallisesti erillisillä lukulaitteilla, jolloin passinhaltijan tunnistaminen helpottuu. Sirua ei pääse koskemaan eikä se ole näkyvissä, kuten esimerkiksi maksukorteissa, vaan se on passin kannen tai tietosivun sisällä. Peruskomponentit RFID-sirullisessa matkustusasiakirjasovelluksessa ovatkin dokumentti itsessään, erillinen lukijalaite, joka vaatii valvonta- ja salausyksikön sekä sovelluksen tietojärjestelmä [43].

Riippuen hieman kerätystä biometriatunnisteesta, kansallisesta toteutuksesta ja itse objektista, johon RFID on integroitu, on sirun tietojen salaamisessa eroja. Matkustusasiakirjoissa oleva RFID-siru on tietosuojatasoltaan vahvempi kuin tavalliset RFID-sirut. RFID-tunniste tulee olla digitaalisesti allekirjoitettuna ICAO Doc 9303 -standardin mukaan. Morshed et al. [48] toteavat, että RFID-tunnisteen koko- tai muistirajoitteen (32 - 64 kilotavua) vuoksi perinteisiä salausmenetelmiä ei voida käyttää. Tietoliikenteellisesti kommunikaatio passin ja lukijalaitteen välillä on kryptattu.

Tiedonsiirron lisäksi sirun tietosisältö tulee olla suojattu, sillä muun muassa e-passin RFID-sirulla on sensitiivistä tietoa: passin numero, myöntämispäivämäärä sekä viimeinen voimassaolopäivämäärä, myöntäjävaltio, passinhaltijan koko nimi, sukupuoli, kansalaisuus, syntymäaika, dokumentin tyyppi, passinhaltijan kasvokuva digitaalisessa muodossa, sormenjäljet tai silmän iiris skannattuna [4]. E-passeissa RFID-siru on määritelty sijoitettavaksi passin tekniseen osaan. Loogiseen tietorakenteeseen määritellyt ja tallennettavat tiedot tulee ICAO 9303 -standardin [29] mu-

kaan koodata niin sanotulla Random Access -hajasaantimetodilla. ICAO suosittelee käytettäväksi RF-modulaation vaihtoehtoja ISO/IEC 14443 A- tai B-tyypin -standardia ja ISO/IEC 7816-4 teknisiä määrityksiä tunnisteiden käyttämiseen. RFID on matkustusasiakirjoissa tyypiltään passiivinen. Se aktivoituu tiedonsiirtoon vain silloin, kun RFID-lukijalaite on lukuetäisyydellä - ICAO:n mukaan maksimissaan 10 cm - antamassa sirulle virtaa [36].

Poliisin [54] mukaan kaikki yli vuodeksi myönnetyt voimassaolevat Suomen passit ovat koneluettavia, mutta kaikissa ei ole sirua. Hätäpassi ei ole koneluettava, eikä siinä ole sirua. Kaikki RFID-sirulliset passit ovat myös koneluettavia. ICAO määrityksen mukaan koneluettava matkustusasiakirja (MRTD) on voimassa, vaikka siihen sisällytetty mikrosiru vahingoittuisi eikä olisi enää luettavissa. RFID:n tarjoama yhteydetön siruteknologia katsottiin toimivaksi jopa kymmenen vuotta voimassa olevalla passilla [36]. Kaikissa koneluettavissa matkustusasiakirjoissa ei ole RFID-teknologiaa [43]. ICAO [29] määrittää, että vuoteen 2015 mennessä ei-koneluettavien matkustusasiakirjojen voimassaolo lakkaa.

Etäluettavan sirun tunnisteen symboli tulee olla näkyvissä etukannessa kaikissa koneluettavissa matkustusasiakirjoissa. ICAO määrittää ”siru sisällä ” -symbolin paikan e-passikirjan etukannen ylä- tai ala-reunaan ja korteissa etupuolelle. E-passeissa RFID:n komponentit voivat olla sijoitettuna muovitettuun tai kangaspäällysteiseen kanteen upotettuina. Siru ja antenni voivat olla myös upotettuna kestomuoviseen polykarbonaatista valmistetulle tietosivulle. Integroitu mikrosiru joko kansisivulla tai tietosivulla muodostaa kirjasen, e-passin.

5 E-Passi

Passi on virallinen matkustusasiakirja. Perinteinen passi muuttui e-passiksi, kun siihen liitettiin elektroniikkaa. E-passi on siten passin kehittyneempi ilmentymä. Siitä on tullut maailmanlaajuisesti tärkeä sähköinen henkilötodistus, joka sisältää passinhaltijasta biograafista ja biometrista tietoa [36]. ICAO [29] käyttää e-passista englanninkielisiä termejä electronic passport tai ePassport. Ranskankielinen sana ”passe ports” viittaa portin läpikulkemiseen. Koneluettavuus ilmenee termistä Electronic Machine Readable Passport (eMRP). E-passi on siis myös biometrinen passi (biometric passport), jonka suojatulle mikrosirulle, Integrated Chip (IC) on tallennettu passinhaltijan kasvokuva ja/tai sormenjälkitiedot sekä passinhaltijan henkilötiedot.

Passikirja sisältää paljon visuaalisesti nähtävissä olevia pakollisia tietoja. Tapahtuuhan henkilön tunnistaminen asiakirjasta myös perinteisin keinoin silmämääräisesti lukemalla, vertailemalla ja tutkimalla. Passin pakollisina henkilötietoina ovat passinhaltijan nimitiedot, kansalaisuus, syntymäaika ja sukupuoli sekä kasvokuva ja omakätinen allekirjoitus [29]. Ajan mittaan passeihin on lisätty näkyviä turvatekijöitä vesileimoista laminointiin. Tietosuojatun mikrosirun vuoksi e-passiin on lisätty tärkeitä teknisiä turvatekijöitä, joita pystyy tutkimaan vain tietojärjestelmillä. Koneluettaviksi matkustusasiakirjoiksi käsitetään e-passit, viisumit ja erityistarkoitukseen olevat ID-kortit sekä rajanylityskortit [43].

Turvallisuustilanteella ja etenkin maailmansodilla on ollut suuri merkitys matkustusasiakirjojen historiassa. Mordinin [47] mukaan Ranska pani täytäntöön ensimmäisen länsimaisen lain, jossa yhdistettiin henkilön identiteettiin syntymätodistus ja kansalaisuus. Kansalaisuus- ja viisumiasioihin erikoistunut Henley & Partners [27] on laatinut IATA:n kanssa yhteistyössä maiden välisen viisumivapautta koskevan tilaston. Se kertoo, kuinka moneen eri maahan biometrinen passi riittää matkustusasiakirjaksi ilman etukäteen hankittavaa maahantulolupaa. Vuonna 2016 kärkisijoilla olivat Saksa (177) ja Ruotsi (176). Suomi, Ranska, Italia, Espanja ja Yhdistyneet kuningaskunnat (175) sijoittuivat kolmanneksi passien tilastossa. Suomen e-passilla voi siis matkustaa 175 eri maahan ilman passiin haettavaa viisumia. Amerikan yhdysvallat on tilastossa sijalla neljä. Tilaston häntäpäähän sijoittuvat Syyria (32), Somalia (31), Irak (30), Pakistan (29) ja Afganistan (25). Indeksiin on otettu mu-

kaan YK:n yhteistyöjärjestön ICAO:n Doc 9303 -standardin yhteensopivat passit. Näitä kertyy kaikkiaan 199 kansalaisuutta, joista 193 kuuluu YK:n alaisuuteen.

Matkustaminen ja ulkorajojen ylitys vaatii pääsääntöisesti matkustajalta voimassa olevaa passia ja/tai muuta matkustusasiakirjaa. Passin lisäksi matkustusasiakirjana voidaan käyttää uuden mallista biometriaa sisältävää henkilökorttia tai rajanylityskorttia. Varsinkin USA:n ja Meksikon välisen rajan tuntumassa rajanylityskortit ovat vilkkaassa käytössä. Meksikon lisäksi rajanylityskortilla voi matkustaa Kanadaan, Karibialle ja Bermudaan muutoin kuin lentämällä. Passin ja henkilökortin ero on siinä, että henkilökortin tarkoitus on osoittaa haltijansa henkilöllisyys ja kansalaisuus rajojen sisällä. Passi puolestaan oikeuttaa myös matkustamiseen rajojen ulkopuolelle.

Pohjoismaiden kesken on passivapaus siten, että Pohjoismaiden (Islanti, Norja, Ruotsi, Suomi ja Tanska) kansalaiset voivat liikkua Pohjoismaissa ilman matkustusasiakirjaa. Henkilöllisyyden todistamiseen hyväksytään esimerkiksi ajokortti. Suomen passilain mukaan ulkomaalaisella henkilöllä tulee Suomeen saapuessa olla passi ja lisäksi viisumi, mikäli viisumia edellytetään Schengen-alueelle.

Viisumi on maahantulolupa-asiakirja. Ulkoasiainministeriön mukaan se myönnetään matkustustarkoituksessa lyhytaikaista ja tilapäistä, enintään 90 päivää kestävää vierailua varten. Viranomainen myöntää viisumin ja kiinnittää ICAO Doc 9303 -standardin mukaisen viisumitarran voimassaolevaan passikirjaan. Myönnetty viisumi ei siis kuitenkaan takaa maahan pääsyä, vaan maahantulon edellytykset tarkistetaan erikseen passintarkastuksessa. Rajatarkastuksissa passikirjan sivuja leimataan asianmukaisin maahan saapumisen tai maasta lähtemisen osoittavin leimoin ja viranomaismerkinnöin.

Viisumivapaus on maiden välinen sopimus. Esimerkiksi Suomen ja Venäjän välillä ei ole viisumivapaussopimusta, mutta helpotuksia on tehty muun muassa monikertaviisumien myöntämisestä. Venäjän ja EU:n väliseen viisumivapausneuvotteluihin on kuulunut biometristen e-passien käyttöönottovaatimuksia. Amerikan yhdysvaltain Visa Waiver Program - (VWP) on mittava viisumivapausohjelma, johon Suomikin kuuluu. VWP kuuluvan maan kansalainen voi matkustaa Yhdysvaltoihin ilman viisumia, mutta vaatimuksena on e-passi.

Laite- ja ohjelmistotekniikan käyttöönotto passintarkastuksessa on johtanut siihen, että e-passista on tullut teknologiaratkaisultaan maailmanlaajuisesti käytetty sovellusohjelmisto. Choi et al. [8] jakaa e-passin kahteen komponenttiin; laite- ja ohjelmistotekniikkaan. Laitetekniikkaa kuvastaa se, että vaikka e-passi on ulkoasul-

taan pieni kirjanen, paperisten sivujen lisäksi siihen on muoviselle tietosivulle integroitu mikrosiru (IC), jolle on sisällytetty biometrista tietoa. Kundra et al. [37] mukaan e-passi on onnistunut toteutus biometrian ja RFID-teknologian kanssa. Tietojen lukemiseen tarvitaan sekä optista lukijalaitetta että RFID-lukijalaitetta. E-passi on tietotekninen sähköisen identiteetin sovellusinnovaatio. E-passin tarkoitus on hyödyttää passinhaltijaa ja viranomaisia.

Tilastollisesti tarkastellen e-passista on tullut tärkein kansainvälinen henkilöllisyyttä todentava asiakirja. Choi et al. [8] mukaan väärennettyjen passien lukumäärä maailmanlaajuisesti on kasvanut. Tästä syystä syystä kansallista turvallisuutta vahvistaakseen terrorismia ja rikollisuutta vastaan kehittyneitä turvatekijöitä sisältäville e-passeille on useissa maissa paljon kysyntää. Gemalto [19] kertoo passitilastoista, että vuonna 2013 oli 25 % passeista tyypiltään e-passeja. Arvio vuodelle 2017 on, että niitä on yli puolet. Secunetin [61] mukaan vuonna 2010 yli 100 valtiota oli lisännyt biometrisia piirteitä passeihinsa. ICAO MRTD report -lehden [21] 2015 vuoden tilastojen mukaan yli 120 valtiota myöntää e-passeja. Esimerkiksi PRADO tietokannan [17]mukaan Venäjän federaation viisi vuotta voimassa olevia e-passeja on otettu käyttöön vuonna 2006 ja uudempia kymmenen vuoden e-passeja on ollut käytössä vuodesta 2010 saakka. Väkirikkaimmista maista Kiina on ottanut käyttöön vuonna 2013 sirupassin. E-passinhaltijoita on noin puoli miljardia ihmistä koko maailmassa ja määrä on lisääntymässä.

5.1 Roolit

Matkustusasiakirjoihin liittyy useita rooleja. Näitä ovat passinhaltija, passin myöntäjä, passin valmistaja ja passin tarkastaja. Lainsäätäjällä on oma roolinsa asetusten ja lakien valmistelussa. Ennen kuin yksilöllinen passi on konkreettisesti valmis, on sille asetettu määrittelyillä tietyt vaatimukset. Standardoimistyöryhmät vastaavat määrittelystä eri toimijoiden sekä teknologian näkökulmista. E-passin määrittelijöiden tulee tuntea passin käyttötarkoitus, teknologia ja passin käyttäjän että viranomaisten vaatimukset.

Passinhaltija on henkilö, jolla on vastuu oman matkustusasiakirjan oikeasta ja huolellisesta säilyttämisestä aina passin elinkaaren ajan ja myös osittain passin hävittämisestä. Suomen passilain [51] mukaan passinhaltijan on säilytettävä passiaan huolellisesti. E-passinhaltija hyötyy siitä, että e-passissa on paljon turvatekijöitä ja biometriaa. Oman identiteetin osoittaminen on helppoa koneluvun ominaisuuksil-

la. Väärissä käsissä e-passia on vaikeampi hyödyntää identiteettivarkauksissakaan.

Passin myöntäjä on viranomainen. Suomessa poliisi on se, jolta passia haetaan ja joka passin myöntää [54]. Diplomaattipassin ja virkapassin myöntää ulkoasiainministeriö. Muukalaispassin ja pakolaisen matkustusasiakirjan voi poliisilaitoksen lisäksi myöntää maahanmuuttovirasto. Poliisin uusissa passin toimitusohjeissa [54] muun muassa kerrotaan passinhaltijan velvollisuudesta tarkistaa passin tiedot. Passinhaltijalla on myös oikeus tarkistuttaa passin sirulle tallennetut tiedot viranomaisen kautta. Passia uusittaessa poliisi ei kerää vanhoja passeja pois, vaan se antaa ohjeet siitä, kuinka passi tulee mitätöidä ja hävittää. Passin hävittämisen taustalla on henkilötietojen turvallisuus sekä se, että vanhat passit eivät pääse mahdollisesti väärinkäyttäjille identiteetin varastamis- tai passin väärennöstarkoituksiin.

Passin valmistaja on yleensä kaupallinen toimittaja, jonka viranomainen on valinnut hankintamenettelynsä mukaisesti. Passin käsittelyyn kytkeytyy passin valmistaja, josta muun muassa Euroopan unionin passiasetus [11] määrää siten, että kunkin jäsenmaan on nimettävä yksi vastuullinen laitos, jolla on oikeus passien tulostamiseen. Valittu passinvalmistaja tulee ilmoittaa muille jäsenmaille ja EU komissiolle. Esimerkiksi Suomessa passin kansallinen valmistus keskitetään yhdelle toimittajalle julkisella hankintakilpailutuksella. Passinvalmistusprosessiin tuo omat haasteensa viranomaisten vaatimukset biometriikasta, sillä e-passin turvatekijöitä on paljon ja sen mukaan myös tietoturvavaatimukset ovat korkeat. Passinvalmistuksessa voi olla mukana useita toimittajia riippuen tilaajan vaatimuksesta ja toimittajan tuotantomenetelmistä. Valmistajalla on vastuu passien personoinnista ja tietojen suojauksesta. E-passin valmistajan tulee huolehtia sirun tietojen suojaaminen, mutta tietojen aitouden ja eheyden varmistaa viranomainen. E-passien osalta on olemassa vaatimus, että passien yksilöinti tulee tehdä Suomessa eikä yksilöintitietoja saa siirtää Suomen rajojen ulkopuolelle. Valmistusvaiheessa on siis monen toimijan ketju, jossa suoritetaan useita työvaiheita sekä tarkkaa laadunvalvontaa.

Passin tarkastaja on viranomainen. Schengenin rajasäännöstön [60] mukaan rajatarkastus on rajavartioiden tehtävä. Tehtäviään hoitaessaan viranomaisen on kunnioitettava ihmisarvoa kaikilta osin. Ketään ei saa syrjiä sukupuolen, rodun, etnisen alkuperän, uskonnon, vakaumuksen, vammaisuuden, iän tai seksuaalisen suuntautumisen perusteella. Passin tarkastus on osa rajatarkastusta ja rooli on haasteellinen. Matkustusasiakirjojen fyysisiä, optisia ja sähköisiä turvallisuustekijöitä kehitetään jatkuvasti, jolloin niiden tarkastus vaatii osaamista. Maailmalla olevien matkustusasiakirjojen valikoima on runsas. Optisesti koneluettavan passin tietosivun tarkas-

tuksen lisäksi rajatarkastukseen on tullut biometriatietojen käsittely tunnistustilanteissa.

Passin tarkastaja voi olla myös automaatti. Euroopan unionissa on otettu käyttöön rajatarkastuksiin itsepalveluperiaatteella toimivia automaatteja, joita tunnetaan Automated Border Control Gates (ABC) -rajatarkastusportteina. Näissä automaattisissa rajatarkastusporteissa on vaatimuksena, että matkustajalla on hallussaan biometrinen e-passi. Matkustussujuvuus toki lisää tyytyväisyyttä kansan parissa, mutta on eri asia arvioida automaattien toimivuutta tunnistustilanteissa. Kun kansalaisen tietoisuus biometriasta on alhaisella tasolla, johtaa tämä seikka Tiits et al. [70] näkemyksen mukaan siihen, että kansalaiset uskovat hyväntahtoisuuteen ja viranomaisten toimivan kansalaisten parhaaksi. Hoepman et al. [28] toteaa, ettei ABC-rajatarkastusporttien käyttäminen ole täysimääräisesti mahdollista, koska läheskään kaikilla matkustajilla ei ole vielä biometrista matkustusasiakirjaa, jonka mikrosirulta automaatti voisi tarkastaa tiedot samalla kun se vertaa reaaliaikaista kasvokuvaa matkustajasta.

Passin hakemiseen ja valmistukseen liittyy olennaisesti viranomaistehtävänä myös hakijan identiteetin varmistaminen [54]. Butt et al. [7] mukaan ratkaisuna hakijan identiteetin varmistamiseen passin hakuvaiheessa olisi käyttää kansalaisten passien tietokantaa, josta käytetään nimitystä Dublicate enrolment check (DEC). Tämä tulevaisuuteen tähtäävä ratkaisu edellyttäisi Euroopan unionin jäsenmaissa keskitettyä kansalaisten tietokantaa, joka sisältäisi passitiedot biometrioineen. Passihakemuksien yhteydessä saataisiin selville identiteettien väärinkäyttö. DEC-järjestelmä toimii identifiointiperiaatteella. Jokaisella jäsenmaalla tulisi olla oikeus käyttää tietoja e-passien hakuprosessissa. Projekti on työn alla.

Lainsäädäntötyötä tekevät viranomaiset ja asiantuntijat pyrkivät pitämään lait ja asetukset ajan tasalla. Suomessa yhteisen passitietokannan asiasta on käyty keskustelua passilain muutoksien yhteydessä. Luotettavan todentamisen vuoksi ainoastaan passin sirulla olevalla sormenjälkitiedolla ei voida saada varmuutta henkilöstä. Sormenjälkitietojen rekisteri mahdollistaisi vertailuja passinhakijan sormenjälkitietojen ja tietokannassa olevien sormenjälkitietojen välillä. Harel [25] varoittaa siitä, kuinka vaikutusvaltaista tietoa biometrinen tietokanta voi pitää sisällään. Mitä suurempi tietokanta, sitä korkeammaksi nousee riski ja houkutus tietojen väärinkäytölle.

E-passiin liittyvät roolit muodostavat siis kokonaisuuden, jota voidaan pitää turvallisen matkustusasiakirjan perustana. Kokonaisuuteen kuuluu luotettavasti haet-

tu ja myönnetty e-passi. Passinhaltijan ja tässä tapauksessa siis loppukäyttäjän pitää myös pystyä muodostamaan itselleen käsitys koko järjestelmästä ja prosessista. Ihmisillä on luonnostaan henkilökohtainen tarve kontrolloida yksityisyyttään. Tästä syystä ihmisille tulisi pystyä viestimään ymmärrettävästi e-passin prosessi, elinkaari ja sen tavoitteet. Yksityisyyden hahmottamista helpottaisi, jos ihmisille kerrottaisiin selkeästi henkilötietojen keräämisen, tietojen säilytyksen ja tietojen käytön periaatteet. Valvontaa voidaan mitata sillä, miten käyttäjät itse pystyvät hallitsemaan omien tietojensa käytön sekä, mitä apukeinoja käyttäjällä itsellään on suojata tietojaan väärinkäytöltä.

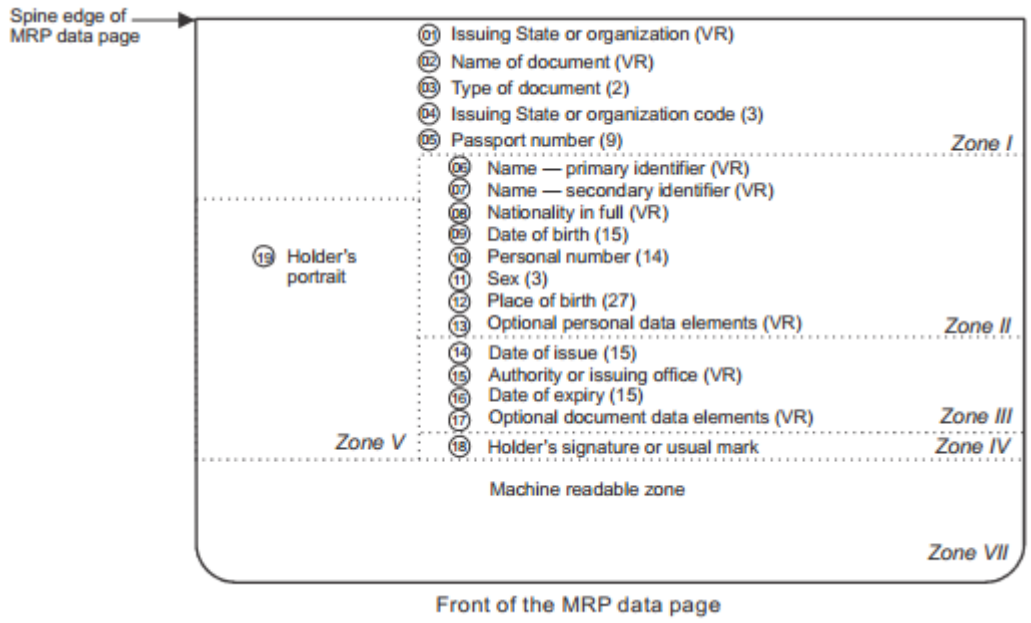
5.2 ICAO Doc 9303 -standardi

Matkustusasiakirjojen standardointityö on alkanut 1920 -luvulla. Työn tuloksena matkustusasiakirjojen tietosisältöjä yhtenäistettiin, passin ulkoasua harmonisoitiin, passin voimassaoloaikoja sekä viranomaisten passin myöntämiseen liittyviä maksuja selkeytettiin ja sovittiin. International Civil Aviation Organization (ICAO) on kansainvälinen siviili-ilmailujärjestö, joka on perustettu vuonna 1944. Se on ollut merkittävässä roolissa passien kehitysvaiheissa ja vaikuttanut kauan matkustusasiakirjojen standardoimistyössä. Vuodesta 1946 lähtien ICAO on kuulunut Yhdistyneiden kansakuntien (YK) alaisuuteen. YK yhteistyö velvoittaa sopimusvaltiota henkilöllisyystodistuksissa ja matkustusasiakirjoissa noudattamaan yleissopimusta. ICAO työskentelee konventiossa 191 jäsenmaan kanssa. [29]

Biometrisia tunnisteita ryhdyttiin suunnittelemaan matkustusasiakirjoihin vuonna 1998, kun standardoimisryhmään muodostettiin uusien teknologioiden työryhmä (TAG/MRTD). E-passien määrittelytyön kehityskulussa vuosi 2004 oli tärkeä, sillä tuolloin ICAO Doc 9303 -dokumenttisarjan standardi [29] virallisesti julkaistiin. Standardissa käsitellään myös koneluettavat matkustusasiakirjat eli Machine Readable Travel documents (MRTD), jolla määritellään ID-kortteja ja muita MRTD-asiakirjoja, kuten taulukossa A.1 ja B.1. ICAO:n standardointityössä kysymyksessä oli merkittävä passiuudistus. E-passien määrittelykuvauksista ICAO Doc 9303 -standardista on käytössä vuoden 2006 sekä vuoden 2008 dokumentit, joiden mukaan uusia e-passeja valmistetaan, mutta koko Doc 9303 -sarja on saanut päivityksen vuonna 2015. [29]

5.2.1 E-passin tietoelementit

ICAO Doc 9303 -standardin [29] mukaan e-passin visuaaliset tietoelementit muodostuvat kahta optionaalista tietoa lukuunottamatta pakollisista tiedoista. E-passi sisältää ainakin seuraavat tiedot: myöntäjävaltio, sana passi (asiakirjan tyyppi), iso kirjain P (asiakirjan tyypin lyhenne), myöntäjämaa (kolmikirjaimisena kooditettuna), passin numero, passinhaltijan koko nimi (ensijainen ja toissijainen nimitieto), kansalaisuus, syntymäaika, henkilönumero, sukupuoli, syntymäpaikka (optionaalinen), henkilötunnistetieto tai sormenjälkikuva (optionaalinen), myöntämispäivämäärä, myöntäjäviranomainen, viimeinen voimassaolopäivä, passinhaltijan omakätinen allekirjoitus ja passinhaltijan kasvokuva. Tietoelementit tulee sijoittaa määrämuotoisesti niille varatuille osa-alueille (Zone I - Zone VII) passin tietosivulla, kuten kuvassa 5.1 [29].



Kuva 5.1: ICAO Doc 9303 -standardin koneluettavan passin (MRP) tietosivun alueet [29].

Ensimmäinen alue (Zone I) on pakollinen otsikko-osa. Alueelle kaksi (Zone II) sijoitetaan pakolliset henkilötiedot sekä vapaavalintaiset henkilötiedot. Alueelle kolme (Zone III) tulee sijoittaa pakolliset ja vapaavalintaiset asiakirjaa koskevat tietoelementit. Alueelle neljä (Zone IV) on varattu tilaa passinhaltijan allekirjoitukselle. Viides alue (Zone V) on pakollinen tunnistetiedoille ja siihen sijoitetaan passinhalti-

jan kasvokuva. Seitsemäs alue (Zone VII) on pakollinen koneluettavalle osiolle. Nämä alueet kuuluvat passin tietosivun etusivulle. Tietosivun takapuolelle voidaan sijoittaa kuudennen alueen (Zone VI) ei-pakolliset tietoelementit. Alueet on eroteltu myös selvästi lukemista ajatellen niin, että alueet yhdestä viiteen ovat nähtävissä ja visuaalisesti luettavissa, kun esimerkiksi konelukurivin alue (MRZ) on tarkoitettu optisesti luettavaksi. [29]

Moniosainen määrittelykuvaus kertoo tarkasti myös sen millaista painopaperia, kirjasinlajia ja painatustekniikkaa passikirjan valmistuksessa tulisi käyttää. Materiaalivalinnoissa standardi kiinnittää huomiota kestävyyteen. E-passien yhteentoimivuuden kannalta ovat olennaista määritykset etenkin siitä, missä muodossa biometriatiedot tulee kerätä ja kuinka ne tallennetaan passille. Dokumenttisarjassa on myös viisumeihin ja henkilökortteihin liittyviä määrityksiä. [29]

5.2.2 MRZ-rivi

ICAO Doc 9303 -standardin [29] mukaan e-passin koneluettava osa, pakollinen MRZ-rivi on tarkoitettu optista tunnistusmenetelmää varten. MRZ on kaksirivinen ja se sisältää keskeiset tiedot kirjaimin, numeroin ja erikoismerkein. Pääosin MRZ sisältää samat tiedot kuin mitä passin tietosivun visuaalinen osa. ICAO Doc 9303 -standardin määrittelemässä koneluettavassa osassa on lisäksi teknisiä tietoja. Kuva MRZ-rakenteesta C.1 havainnollistaa optisesti luettavaa rivitietoa, ja osoittaa missä kohdissa löytyy numeerisia tarkistussummia.

Optinen tunnistusmenetelmä, Optical recognition (OCR), pystyy tunnistamaan dokumentille painettuja merkkejä [43]. ICAO Doc 9303 -standardi [29] määrittelee muun muassa optiseen lukemiseen vaadittavan kirjaimiston fonttityypin (OCR-B), jossa koko on 1, merkkien väli vakiona 2,54 mm ja kirjaimisto aakkosten isoilla kirjaimilla. Vaatimukset ovat optisen lukemisen yhteentoimivuuden kannalta olennaisia.

Ensimmäinen MRZ-rivi sisältää positiosta 1 alkaen dokumenttikoodin. Tyypillisesti se on passeissa P-kirjain. Positiosta 3 alkaen myöntäjämaa tai myöntäjä organisaatio kooditettuna. Esimerkiksi Suomen passeissa on FIN, josta esimerkki kuvassa 5.3, saksalaisessa passissa D, sveitsiläisessä passissa CHE ja yhdysvaltalaisessa passissa USA [17]. Positiosta 6 positioon 44 on varattu tilaa passinhaltijan nimelle. Määrittelyssä on runsaasti sääntöjä pitkistä nimistä ja erikoismerkkien käytöstä. Esimerkiksi, jos passinhaltijan etunimi on MARIE-ELISE, on tämä tieto koneluettavalla rivillä muodossa MARIE<ELISE, missä <-merkki korvaa erikoismerkin -. To-

della pitkän nimen osalta joudutaan koneluettavalle riville tekemään erikoiskäsittelyä verrattuna visuaalisesti nähtävillä olevaan passinhaltijan nimeen. Vaihtoehtoja on kolme, joista esimerkkejä liitteessä C.1.

Toinen MRZ-rivi sisältää positiosta 1 positioon 9 passin numeron, positiossa 10 on tekninen tarkistusnumero, positiossa 11 - 13 on kolmemerkkinen kansallisuustunnus kooditettuna ICAO Doc 9303 -standardin mukaan. Positiossa 14 - 19 on passinhaltijan syntymäaika. Päivämäärien esitysmuodoissa on kansallisia esitystapoja, mutta ICAO Doc 9303 -standardi määrittelee päiväyksistä MRZ-rivin tietosisällön tarkasti. Päiväyksen rakenne on kuusimerkkinen (YYMMDD). Esimerkiksi 12 heinäkuuta 1942 esitetään 420712. Tätä seuraa jälleen tekninen tarkistusnumero. Positiossa 20 on sukupuoli kooditettuna siten, että M tarkoittaa miestä, F naista ja <- merkki tarkoittaa määrittelemätöntä sukupuolta. Positiossa 22 - 27 on passin viimeinen voimassaolopäivä. Positiossa 28 on tarkistusnumero. Positiossa 29 - 42 on henkilötunniste. MRZ-rivin lopussa on kaksi erillistä teknistä tarkistusnumeroa. [29].

Vaikka joissakin tapauksissa koneluettava rivi näyttää erikoiselta, on standardoitu MRZ-rivin malli osoittautunut käyttökelpoiseksi koneluettavissa matkustusasiakirjoissa. E-passin suurimpana etuna pidetään koneluettavuutta, mutta perusedellytyksenä sirun tietojen lukemiselle on, että lukijalaite pystyy lukemaan MRZ-rivin tiedot ensin. Sen lisäksi, että koneluettavat tiedot on standardoitu, e-passeissa ovat niin MRZ-rivin kuin sen mikrosirun tiedot maailmanlaajuisesti yhteensopivia ja -toimivia.

5.2.3 Mikrosirun biometriatiedot

ICAO:n [29] määritelmän mukaan biometrialla tarkoitetaan mitattavissa olevaa yksilöllistä ominaisuutta tai henkilön käyttäytymiseen liittyvien omaisuuksien tunnistamista ja väitetyn identiteetin vertailua. Biometrinen tieto kerätään ja tallennetaan e-passin mikrosirulle. Tämän hetkisen voimassaolevan määrittelykuvauksen mukaan vain kolmentyyppisiä biometrisia tunnisteita voidaan e-passin mikrosirulle sisällyttää. Näitä ovat taulukossa 5.1 mainitut kasvokuva, sormenjälkitiedot tai silmän iiris. Kunkin tunnisteen tekniset yksityiskohdat mikrosirutallennukselle määritellään ISO/IEC standardeissa erikseen. Sormenjälkiin perustuva biometrinen tunnistaminen on edelleen eniten käytetty muoto. Suuret sormenjälkitietoja sisältävät tietokannat, esimerkiksi sellaiset, joissa minutiae-pisteet muodostavat vertailun algoritmin, vaativat tehoa. Gutierrez et al. [23] mukaan Minutia Cylinder Code (MCC) -algoritmi on osoittautunut erittäin tarkaksi. Koska MCC -algoritmi vaatii kuitenkin

paljon laskentatehoa, käytetään sormenjälkivertailuun Graphical Processing Unit (GPU):ta. ISO/IEC 19794 -tekninen standardi määrittelee sormenjälkitunnistamista ja MCC:ta tarkemmin.

Hoepman et al. [28] mukaan ICAO on valinnut kasvokuvan ja sormenjälkitedot ensisijaisiksi biometrisiksi tunnisteiksi. Kasvokuvat ovat helppokäyttöisiä, koska valokuvan voi ottaa välimatkan päästä. Kasvokuvat eivät aiheuta kulttuurillisesti esteitä. Sormenjälkitietojen keräämisessä on selkeästi kulttuurisia jarruja, sillä niitä pidetään sensitiivisinä eikä niitä voida kerätä ilman henkilön suostumusta. ICAO Doc 9303 -standardissa vain kasvokuva on pakollinen biometrisena tunnisteena e-passissa. Gemalton [19] mukaan vuoteen 2015 mennessä silmän iiris-tunnistetta ei ole missään maassa valittu passeihin biometriseksi tunnisteeksi.

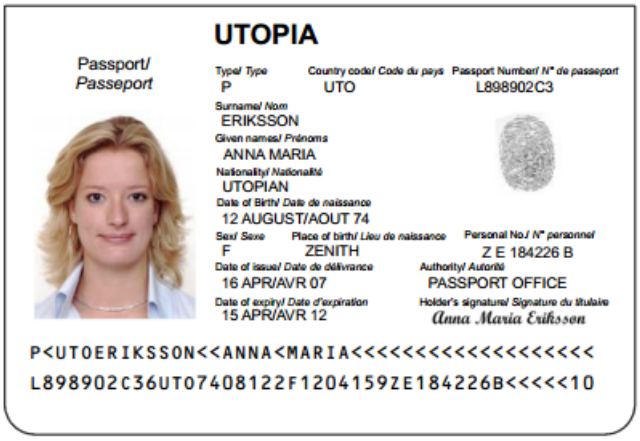
Taulukko 5.1: Biometriset tunnisteet koneluettaviin matkustusasiakirjoihin ICAO 9303 -standardin mukaan. [29]

Biometriatyyppi	Pakollisuus	Tekninen standardi
kasvokuva (facial recognition)	pakollinen	ISO/IEC 19794-5
sormenjälki (fingerprint recognition)	valinnainen	ISO/IEC 19794-4
silmän iiris (iris recognition)	valinnainen	ISO/IEC 19794-6

E-passin mikrosiru on tyypiltään passiivinen. Bogari et al. [4] mukaan ISO/IEC 14443 -standardi määrittää kahta vaihtoehtoista integroitua sirua (IC); passiivisia tai aktiivisia. Tästä seuraa, että mikrosirun lukijalaitekin on kykenevä lukemaan joko passiivisia tai aktiivisia tunnisteita. Mohamed et al. [46] mukaan e-passin sirulla olevassa RFID-tunnisteessa on sisäänrakennettuna Electronically Erasable Programmable Read-Only Memory (EEPROM) puolijohdemuistia, jonka koko on 32:sta kilotavusta 144:ään kilotavuun. Muistiin tallennetaan ICAO Doc 9303 -standardin loogisen tietorakenteen mukaisesti muun muassa biometrisen tunnisteen tiedot sekä tietoturvaan liittyvät tekniset tiedot. Esimerkiksi henkilön kasvokuva JPEG-muodossa vie tästä kapasiteetista 15 - 20 kilotavua. ICAO jatkokehittää standardia, joten tulevaisuuden e-passeissa voi olla useita biometrisia tunnisteita, mikä puolestaan merkitsisi uusia vaatimuksia mikrosirulle.

E-passin tekninen osa on tarkoitettu yhteydettömään RFID-teknologiaan perustuvan mikrosirun upottamiseen passin rakenteeseen. Mikrosirun sisältöä voidaan koneellisesti lukea muutaman senttimetrin päästä lukijalaitteesta. ICAO Doc 9303

-standardin [29] mukaan Data Group 2 (DG2) on varattu kasvokuvalle, Data Group 3 (DG3) on sormenjälkitiedoille ja Data Group 4 (DG4) silmän iirikselle. Data Groupit 2 - 4 ovat koodattuja tietoja ja kuuluvat loogiseen tietorakenteeseen (LDS). Erityisesti mikrosirulle suunniteltu tietosuojauksen salausmenetelmä Password Authenticated Connection Establishment (PACE) on protokolla, jonka tarkoituksena on estää tietojen pihistäminen ja väärinkäyttö. PACE estää sähköisen matkustusasiakirjan ja sen tarkastukseen tarkoitetun lukijalaitteen välisen tietoliikenteen salakuuntelun. PACE on Diffie-Helllman avaintenvaihtoprotokollaan perustuva tietoturvallinen viestintämenetelmä, jolla voi autentikoida e-passin sirun ja lukijalaitteen välisen kommunikoinnin. Diffie-Hellman -algoritmi perustuu julkisen avaimen kryptografiaan, salakirjoitustekniikkaan [35]. ICAO Doc 9303 -standardin [29] mukaan PACE-menetelmä ei kuitenkaan estä tietojen tai sirun kopiointia.



Kuva 5.2: ICAO Doc 9303 -standardin mallipassin tietosivu sormenjälkitiedolla [29].

ICAO Doc 9303 -standardi [29] määrittelee PKI-hallintamenetelmään liittyvää varmenteisiin pohjautuvaa suojausta muun muassa hallinnoimalla ja ylläpitämällä julkisen avaimen hakemistopalvelua, Public Key Directory (PKD):tä. ICAO:n PKD-menetelmä palvelee maailmanlaajuisesti järjestelmään kuuluvia osapuolia, joita on vuoteen 2015 mennessä 45 eri valtiota [21]. Vuonna 2016 tämä lukumäärä on noussut 54:ään. Hakemistopalvelun salaustekniikka helpottaa koneluettavien matkustusasiakirjojen tarkastuksen yhteydessä tarvittavien varmennetietojen laillisuuden ja oikeellisuuden tarkistusta. PKD-palvelu on tärkeä mikrosirun biometriatietojen lukemiseen.

5.3 Kehittyminen sukupolviksi

E-passiksi voidaan määritellä sellaiset koneluettavat matkustusasiakirjat, joissa on ICAO standardin mukainen yhteydetön mikrosiru sisältäen passinhaltijan tietoja. RFID Journal -lehden artikkeli [76] kertoo RFID-teknologian ja e-passien kehittämisestä. ICAO:n dokumentaatiossa [29] on jo 1960 -luvun lopulta alkaen määritelty matkustusasiakirjoihin teknisiä ratkaisuja. Ratkaisussa on edetty koneluettavista passeista e-passeihin ja biometrisiin passeihin. Migraatioprosessi tavallisesta passista koneluettavaksi ja edelleen e-passiksi on kestänyt useita vuosia. Koneluettavuus oli aluksi optiseen riviin perustuvaa passin tietojen lukemista. Mikrosirun sisältävä passi luokitellaan e-passiksi. Biometriseksi passiksi kutsutaan e-passia, jonka mikrosirulla on biometrisia tunnisteita. Teknologiakehitys määrittelee e-passien sukupolvia, mutta sukupolviin vaikuttaa myöskin passien muut ominaisuudet ulkoasussa ja turvatekijöissä. Passin liittyvät prosessit ja passin elinkaari määrittelevät sukupolvia. Passien voimassaoloajat vaihtelevat kansallisissa toteutuksissa kahdesta vuodesta kymmeneen vuoteen, jolloin on mahdollista, että samaan aikaan maailmalla on eri sukupolviin kuuluvia e-passeja liikkeellä.

E-passin esiaste saatiin aikaan Malesiassa vuonna 1998. Mohamed et al. [46] mukaan tuolloinen ensimmäisen e-passin toteutus noudatti ICAO:n ohjeistusta ja vietiin käytäntöön ennen kuin ICAO oli virallisesti julkaissut standardinsa. Malesian e-passi sijoittuu 12:ksi Henley & Partners [27] passien paremmuutta vertailevassa vuoden 2016 tilastossa, sillä sen ICAO Doc 9303 -standardin mukaisesti valmistetulla e-passilla pääsee 164:ään maahan ilman viisumia.

E-passit voidaan jaotella sukupolviin niiden teknisen ratkaisun perusteella, kuten Abid et al. [1] on tehnyt. Valmistusvuosien mukaan sukupolviin jakaminen on vaikeaa, sillä eri maissa on otettu käyttöön e-passin teknologiset muutokset vaiheittain sekä siihen tahtiin, milloin passinhaltijan passien voimassaoloaika päättyy. Teknologinen kehitys on vaikuttanut paljon myös biometriikan keräyksen prosesseihin ja erityisesti e-passin tietojen tietoturvallisempiin lukutapahtumiin. Tästä puolestaan on seurannut muun muassa automatisointia passien tarkastuksissa. 2000-luvun e-passin evoluutio on kuitenkin erotettavissa neljään eri sukupolveen. Aikajanalla e-passin sukupolvet sijoittuvat vuodesta 2004 vuoteen 2030.

Ensimmäisen sukupolven e-passi perustui teknisesti toteutettuna ICAO:n julkisen avaimen PKI-menetelmään ja Basic Access Control (BAC)-peruspääsynvalvontaan passin mikrosirulla. E-passin mikrosiru sisälsi biometrisena tunnisteena vain kasvokuvan. E-passin tarkastusta varten täytyi luoda prosesseja myös mikrosirun tietojen

lukemista varten. Choi et al. [8] mukaan BAC-menetelmä päästää mikrosirulle vain sellaisen lukijan, joka tietää e-passin MRZ-rivin kaikki 88:n position tiedot. Lukijalaite saa MRZ-riviltä avaimen datan lukutapahtumaan sirulle [44]. Avaimella lukijalaite todistaa mikrosirulle, että se on pystynyt optisesti lukemaan MRZ-rivin. Tällä menettelyllä varmistuu istuntoavainten välityksellä tietoturvallinen lukutapahtuma. Menetelmä estää lukutapahtuman tilanteessa, jossa e-passi ei ole vastaanottanut signaalia. Lisäksi, kun lukija on osoitettu oikeaksi, menetelmä estää tietoliikenteen salakuuntelun luomalla kooditetun kanavan käyttäen Data Encryption Standard (DES) -salausalgoritmia e-passin ja lukijalaitteen välillä. Huolimatta teknisistä ratkaisuista, ensimmäisen sukupolven e-passissa raportoitiin olevan useita tietoturvan puutteita, joista Mohamed et al. [46] mukaan nimenomaan MRZ-rivin lukemiseen perustuvissa pääsynhallintaprotokollissa ilmeni yleisiä haavoittuvuuksia. Esimerkiksi Man-in-the-Middle -tapauksia, salakuuntelu, pihistys, kloonaus, jäljitys, huijaus ja radiohäirintää. ICAO kehitti edelleen teknisiä vaatimuksia e-passeihin huomioiden tietoturvan näkökulmia. Kehitystyön tuloksena syntyi toisen sukupolven e-passi.

Toisen sukupolven e-passeista on paljon käytetty termiä biometrinen passi. Tämä johtuu sensitiivisen sormenjälkitiedon keräämisestä passinhakijalta e-passin mikrosirulle, mistä Euroopan unioni sääti vuonna 2006 asetuksella. Biometrian turvaamiseksi toisen sukupolven e-passiin lisättiin pääsynhallintaan Extended Access Control (EAC)-protokolla. EU:n vaatimuksesta EAC -menetelmää kehitettiin entistä tietoturvallisemmaksi. Teknisenä lisänä EAC-protokollan todentamismenetelmän aktiivisesta autentikoinnista (AA) tuli pakollinen. AA:lla todennetaan sitä, ettei sirua ole vaihdettu. Mohamed et al. [46] mukaan toisen sukupolven e-passin tietoturvataso on parempi kuin mitä sen tiedettiin olevan ensimmäisessä e-passin sovelluksessa. Mikroprosessoriin perustuva ratkaisu estää väärinkäytöksiä ja vilppiä henkilötunnistuksessa. Toisen sukupolven passin tyypillisin käyttöönotto ajoittuu vuosille 2009 - 2010. E-passit levisivät nopeasti maailmanlaajuiseen käyttöön [4].

Kolmannen sukupolven e-passi eroaa edeltävästä passista siinä, että sen lukemisessa käytetään suoraa reaaliaikaista autentikointi- ja turvallisuusmekanismia [1]. Tämä tunnetaan Online Secure e-Passport (OSEP) protokollana, jonka salaustekniikka perustuu Elliptic Curve Diffie-Hellman (ECDH) -avaimiin. Kundra et al. [37] mukaan OSEP-protokolla syrjäyttää sertifikaattien hierarkkisen järjestyksen eli sertifikaattiketjun, koska vain päätason varmennetietoa käytetään tässä protokollassa. Etuna on vähemmän muistitarvetta mikrosirulla. Lisäksi OSEP-protokolla estää

luvattoman lukutapahtuman. OSEP-protokolla pyrkii torjumaan Denial of Service (DOS) palvelunestohyökkäyksen. Kolmannen sukupolven passi on siis myös biometrinen passi ja sen mikrosirulla olevaa biometriaa on turvattu Password Authenticated Connection Establishment (PACE) -protokollalla [52]. Poliisin passihankinnan tiedotteen [54] mukaan uusin suomalainen e-passi kuuluu kolmanteen sukupolveen, jonka ensimmäiset toteutukset maailmalla ovat alkaneeet vuonna 2015.

Neljännen sukupolven e-passi sisältää rajatarkastuksiin liittyviä ominaisuuksia kuten esimerkiksi e-viisumin ja sähköisen leimauksen. Gemalton [19] mukaan ICAO valmistelee standardia Logical Data Structure 2 (LDS2):sta, jossa siruratkaisuun liitetään myös viisumitietoja sekä erilaista lisäbiometriikkaa. ICAO:n [29] mukaan LDS2 tarkoittaa optionaalista ja takautuvasti yhteensopivaa sirun laajennusta. Dynaaminen tietosisällön päivitys e-passin mikrosirulle tuo paljon uusia mahdollisuuksia, mutta myös uhkia. Nykyisen LDS:n A.1 tavoitteena on taata kansainvälinen yhteentoimivuus kaikissa e-passeihin tallennettavissa tiedoissa. LDS ratkaisu on staattinen, sillä sirulle tallennetaan passin valmistuksen yhteydessä passinhaltijan biograafiset tiedot eikä tietoja ole mahdollisuus muuttaa säädetyin tietosuojajärjestelyin. Tästä syystä dynaamisemmaksi tavoiteltu LDS2 on ICAO:n TAG-työryhmässä kehitteillä. Neljännen sukupolven e-passin ratkaisu valmistunee vuoteen 2020 mennessä.

5.4 Yhdysvaltalainen e-passi

Amerikan yhdysvalloissa on matkustusasiakirjoina passeja, e-passeja ja rajanylityskortteja, joita myönnetään USA:n kansalaisille. Meingast et al. [45] mukaan Yhdysvaltain ulkoministeriö, U.S. Department of State (DOS) teki ehdotuksen passiuudistuksesta elektroniseksi passiksi 2000 -luvun alussa. Valtionhallinnossa päätettiin biometriikan ja yhteydettömän sirun teknologiavalinnoista [45]. Vaudenayn [75] mukaan painetta passiuudistukselle loi Yhdysvaltain viisumivapausohjelma (Visa Waiver Program, VWP), jonka piirissä ilman etukäteen haettavaa viisumia pääsee maahan yli 40 eri valtion kansalaiset. VWP:n vaatimuksena on, että ulkomaalaisen passi on koneluettava ja että maahan saapuvalla on myös biometriaa sisältävä sirullinen e-passi. Matkustajan on läpäistävä Yhdysvaltain turvallisuusministeriön matkustuslupajärjestelmä Electronic System for Travel Authorization (ESTA) hakemuksen vaatimukset. Paineet saada Yhdysvaltojen omien passien ominaisuudet vastaavalle tasolle muiden kanssa syntyivät siis osittain VWP -viisumivapausohjelman

kautta.

USA:n passitilastojen [71] mukaan ennen 2000 -lukua passien määrät vuositasolla liikkuivat 6 - 7 miljoonassa kappaleessa. Uudistuksella oli siis vaikutusta kansallisestikin suurelle ihmisjoukolle. E-passin käyttöönottoon tähtäävät toimenpiteet käynnistettiin nopeasti Amerikan yhdysvalloissa 9/11 terrorismitapahtuman jälkeen. Yhdysvaltojen e-passien käyttöönotto näkyy tilastoissa varsinaisesti vuonna 2007, jolloin ennätyksellinen määrä, yli 18 miljoonaa Yhdysvaltalaisia passia myönnettiin. Sen jälkeen myönnettyjen matkustusasiakirjojen vuosittaiset lukumäärät ovat olleet keskimäärin 14 miljoonaa e-passia, sisältäen noin 1,5 miljoonaa rajanylityskorttia.

Pääpaino passiuudistuksen läpiviennissä oli tuolloin sisäisessä turvallisuudessa, maahantuloasioissa ja sitä kautta erityisesti rajatarkastuksien tehostamisessa. Liu et al. [44] kertovat, kuinka Yhdysvallat ja muut maat sitoutuivat biometriseen henkilötunnistautumiseen ja RFID-teknologian käyttöönottoon rajatarkastuksissa, joissa e-passi-sovelluksen täytäntöönpano ICAO määrityksen mukaan koneluettavaksi passiksi oli ehdoton edellytys. Rajatarkastuksiin luvattiin matkustusasiakirjojen koneluettavuuden myötä sujuvuutta sekä lisäetuna tietojen keruumahdollisuuksia, jolloin esimerkiksi sellaisten ihmisten tunnistettavuus helpottuisi, jotka matkustavat varastetuilla matkustusasiakirjoilla.

Teknisenä ratkaisuna vuonna 2002 päätettiin Yhdysvalloissa hyödyntää RFID-teknologiaan perustuvaa yhteydetöntä (contacless) älykorttiteknologiaa e-passeissa. Perusteluina RFID-teknologian valintoihin pidettiin tuolloin globaalia yhteensopivuutta, luotettavuutta, kestävyyttä sekä käytännöllisyyttä, kuten Meingast et al. [45] tutkimus Yhdysvaltojen e-passeista toteaa. Tuolloin käytössä oleva teknologia perustui ISO/IEC 14443 -standardin [30] määrittelemään yhteensopivaan RFID-tunnisteeseen, jossa oli muistia 64 kilotavua. Mikrosiru oli passiivinen, eikä siinä siis ollut virtalähdettä vaan se sai energiaa lukijalaitteen kautta. Lukuetäisyys oli noin 10 cm lukijan ja sirun välillä, mutta Meingast et al. [45] mukaan kyseinen standardi ei tuolloin eksplisiittisesti määritellyt lukuetäisyyttä, jota ISO/IEC 14443 -standardi [30] ja ICAO Doc 9303 [29] nyt yhdessä määrittää. Teknisen ratkaisun perusteella Yhdysvaltalainen e-passi kuuluu ensimmäiseen e-passin sukupolveen.

Ensimmäisen sukupolven e-passeihin luokiteltavalla yhdysvaltalaisella e-passilla on älykorttisirulla samat tiedot, mitä on visuaalisesti nähtävissä passin tietosivulla [45]. Kansallisesti voidaan päättää vapaavalintaisten tietojen käyttämisestä, vaikka e-passeissa noudatetaan ICAO standardin dokumenttisarjaa Doc 9303 [29]. RFID-

tunnisteelta löytyy passinhaltijan nimi, syntymäaika ja muut henkilön biografiset tiedot. Yhdysvaltojen e-passissa biometrisena tunnisteena on passinhaltijan kasvokuva JPEG-tiedostomuodossa RFID-mikrosirulle tallennettuna. Yhteydetön siru toimii lähetin-vastaanotin periaatteella, ja se on sijoitettuna passikirjan kanteen [45]. Koska passin tietojen asiatonta urkintaa pelätään, varustetaan passit metallisella kuorella (ns. Faradayn häkki). Suojaustoimenpiteellä pyritään estämään tietojen kalastelu. Teknisenä tietoturvatoimenpiteenä ensimmäisen sukupolven e-passi käyttää BAC-protokollaan perustuvaa sirun lukemista suojaava pääsynvalvontamenetelmää. BAC-menetelmä sallii pääsyn tietoihin ja toimintoihin vain valtuutetuille käyttäjille.

Yhdysvalloissa e-passin passiivisen autentikoinnin (PA) vaatimuksena on, että etäluettava siru on myöntäjävaltion digitaalisesti allekirjoittama, ja että allekirjoitus on tarkastettu ennen käyttöä [33]. Tämä johtuu tietojen eheysvaatimuksesta. Päätös käyttää RFID-teknologiaa e-passeissa Yhdysvalloissa, aiheutti runsaasti kritiikkiä vuonna 2002. E-passin suunnitteluvaiheessa ei tarpeeksi osattu huomioida mahdollisia yksityisyyden suojaan kohdistuvia näkökulmia eikä myöskään tietoturvanäkökulmia. Yhdysvaltain e-passin käyttöönotto viivästyi noin vuodella ja tapahtui varsinaisesti joulukuussa vuonna 2005 vaiheittain. Passien voimassaoloajasta johtuen viimeisimmätkin passit on uusittu vuoteen 2015 mennessä. Samanaikaisesti e-passien tarkastukseen tarkoitetut lukijalaitteet olivat kriittisen tarkastelun alla nimenomaisesti tietojen urkintamahdollisuuksien tai salakuuntelun vuoksi [44].

Vuodesta 2007 lähtien Yhdysvallat on myöntänyt kansalaisilleen vain e-passeja. Tietoturvanäkökulmia on huomioitu, sillä biograafiset tiedot ja henkilön kasvokuva ovat suojattuja. Digitaalinen allekirjoitusteknologia varmentaa sirun tietojen aitouden. Erona Amerikan yhdysvaltojen ja Euroopan e-passien välillä on biometriatiedoissa sormenjälkitiedot sirulla. Niitä ei Yhdysvallat käytä e-passissa. Aitojen matkustusasiakirjojen mallitietokannassa, PRADO:ssa [17] on malleja USA - Yhdysvallat kansalaisten passeista. Esimerkiksi vuonna 2006 käyttöönotettu tavallinen e-passi sisältää 28 sivua, sen materiaali on muovia ja kannet siniset. Diplomaattipassin oikeudellinen merkitys on osoittaa, että passin haltija (USA kansalainen) nauttii diplomaattista koskemattomuutta. Passin kannet ovat mustat. Sivulla 52 on huomautus, että dokumentti sisältää sensitiivistä elektroniikkaa. Ohje neuvoo lisäksi e-passin säilytyksestä yksityiskohtaisesti: dokumenttia ei pidä taittaa, lävistää tai altistaa äärimmäisiin lämpötiloihin. Virkapassi on Yhdysvaltain kansalaiselle myönnettävä passi virkamatkalle ja siinä on 28 sivua, kannet ovat ruskeat. Vuonna 2015

Yhdysvaltojen passitilastossa [71] komeilee luku 15 556 215 myönnettyä matkustusasiakirjaa, joista 1,6 miljoonaa kappaletta on tyypiltään rajanylityskortteja.

5.5 Eurooppalainen e-passi

Euroopan unioni on vuodesta 1980 lähtien pyrkinyt harmonisoimaan tavallisen passin suunnittelua. EU:lla ei ole kuitenkaan itsellään passien valmistusoikeutta. Vuoden 2004 aikana Euroopan neuvoston asetus (EY) N:o 2252/2004 [11] antoi määräyksen biometriikan käytöstä passeissa ja matkustusasiakirjoissa. EU:n jäsenmaita velvoittavan asetuksen tarkoituksena oli lisätä passien turvallisuutta käyttöönottamalla yhdenmukaisia turvatekijöitä Euroopan alueella. Matkustusasiakirjoihin lisätyillä turvatekijöillä ja erityisesti biometriikalla Euroopassa haluttiin torjua terrorismia, laitonta maahanmuuttoa ja lapsikauppaa. Uudistettu eurooppalainen e-passi on tekniikaltaan toisen tai kolmannen sukupolven passikirja.

Eurooppalaisia henkilö- tai muita tietoja sisältävissä passin tai matkustusasiakirjan osissa käytettävälle paperille on asetuksessa vähimmäisvaatimuksia. Esimerkiksi passin paperissa ei sallita optisia kirkasteita, vesileimat tulee olla kaksisävyiset, värillisiä kuituja (osittain näkyviä ja osittain UV-valossa nähtäviä) tulee käyttää ja erityistä turvalankaa suositellaan sisällytettävän paperiin [11]. Jäljentämisen estämiseksi henkilötietosivulla on käytettävä optisesti muuttuvaa tekijää, joka vastaa viisumin kaavaa tunnistus- ja turvatasoltaan. Passin tietojen väärentämisyrityksiltä henkilötietoja pyritään suojaamaan lasertulostus- tai lämpösiirtomenetelmällä passikirjojen valmistusvaiheessa käyttäen erityistä kuumasaumausta tai vastaavaa laminointia. [11].

Euroopan neuvoston jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijöistä ja biometriikkaa koskevista vaatimuksista oleva asetus (EY) - N:o 2252/2004 [11] velvoittaa kaikkia EU:n jäsenmaita ottamaan e-passeihin biometriset tunnisteet ja ne on tallennettava yhteentoimivassa muodossa e-passin mikrosirulle. Biometristen tunnisteiden katsottiin muodostavan matkustusasiakirjan ja passinhaltijan välille luotettavan yhteyden. Lisäksi asetuksessa vaaditaan, että tallennusvälineen on oltava kapasiteetiltaan riittävä ja kyettävä takaamaan tietojen eheys, aitous ja luottamuksellisuus. Asetuksen valmistelun yhteydessä käsiteltiin yhteistä biometrista tietokantaa. Euroopan parlamentti vaati, ettei sellaista Euroopan unionin passien ja matkustusasiakirjojen keskustietokantaa, jossa olisi tallennettuna EU:n passinhaltijoiden biometriset tunnisteet, perusteta lainkaan. Asetuk-

sen valmistuttua havaittiin tarve täsmentää mm. biometriikan keräämistä siten, että sormenjälkien antamisesta vapautetaan alle 12-vuotiaat lapset ja henkilöt, jotka eivät fyysisten rajoitteiden vuoksi pysty antamaan sormenjälkiä. E-passiin kerätään ensisijaisesti hakijan molemman käden etusormista sormenjäljet. Turvatoimena sovelletaan periaatetta, että yhdellä henkilöllä on yksi passi. Tämä muutos tarkoittaa käytännössä sitä, että lapsella tulee olla oma henkilökohtainen passi.

Euroopan laajuinen e-passien käyttöönottovaihe kesti useita vuosia. Hoepman et al. [28] mukaan ensimmäiset eurooppalaiset biometriaa sisältävät e-passit RFID-teknologiaan perustuvalla mikrosirulla varustettuina painettiin vuonna 2006. Yhteinen käyttöönotto tapahtui kesäkuussa 2009, johon EU:n asetus vuodelta 2004 velvoitti [11]. Biometrisen tunnisteen sisältävän e-passin kannessa on tätä osoittava tunnuskuva, sirun symboli (kuvassa 5.3), johon Suomenkin passilaissa [51] viitataan, ja jonka ICAO Doc 9303 -standardi vaatii. Vuonna 2014 Euroopassa 49 maalla oli sirullinen e-passi. Rebne [56] toteaa, että EU:n laajuinen e-passin sovellus vaikuttaa huomioineen käyttäjäystävällisyyden, sillä useissa EU maissa e-passi on toteutettu tilaustyönä kansallisten tarpeiden mukaiseksi. EU jäsenmaiden passeissa on yhteistä se, että sana ”EUROPEAN UNION” on nähtävissä yhdellä tai useammalla kielellä passin etusivulla. Kansallisten toteutuksien eriaikaisuudesta johtuen eurooppalaisia e-passeja ei oikein voida jakaa yhteneväisesti ajallisesti sukupolviin, mutta useimmat passinhaltijoilla voimassaolevat e-passit ovat toisen tai kolmannen sukupolven e-passeja.

Vaikka ICAO Doc 9303 -standardi määrittelee maailmanlaajuisesti e-passien ulkoasua, yhteentoimivuutta, turvatekijöitä ja teknisiä yksityiskohtia, on mahdollista teknisten eritelmien pohjalta muodostaa kansallisesti omia erityispiirteitä omaavia ratkaisuja. Eurooppalaisen e-passin kehityksessä saavutuksena voidaan pitää EU jäsenmaiden välistä yhteistä asetusta, jonka velvoittamana jäsenmaat ja muut Euroopan maat ovat yhtenäistäneet e-passien sovellusta. Eurooppa-neuvosto on julkaissut PRADO-tietokannan, jossa on aitojen matkustusasiakirjojen julkista tietoa. PRADO [17] tiedoista voi havaita yhteneväisyyksiä sekä eroja EU-maiden passien painotekniikassa, turvaominaisuuksissa, kansissa, kuvioissa, vesileimoissa tai sivujen lukumäärässä, kuten esimerkiksi Itävallan passissa sivuja on 36, kun Alankomaiden e-passissa sivuja on 66. Passien voimassaoloaika vaihtelee maittain viidestä kymmeneen vuoteen.

E-passin koneluettavan alueen MRZ-rivin lukemiseen EU otti käyttöön laajennetun peruspääsynvalvontaan liittyvän teknisen ratkaisun, Extended Access Control

(EAC) -menetelmän, jonka se oli itse standardoinut [28]. EAC -menetelmä on kaksivaiheinen. Ensinnäkin se kattaa sirun autentikoinnin, Chip Authentication (CA) ja päätelaitteen autentikoinnin, Terminal Authentication (TA). Teknisesti tarkastellen tietojärjestelmissä pääsynvalvontaohjelmiston tehtävänä on valvoa tietoihin pääsyä ja tarkistaa käyttäjävaltuudet [73]. Hoepman et al. [28] mukaan EAC-menetelmä vaatii suorituskykyä e-passissa olevalta RFID-sirulta. Mohamed et al. [46] mukaan TA pyrkii siihen, että lukijalaite tunnistaa luettavan passin ja käyttää lukutapahtumassa sekä BAC- että CA-menetelmiä ja estää siten valtuuttamattoman lukemisen. Autentikointitapahtumien etuna on luvattoman pääsyn esto e-passin biometrisiin tietoihin. Gutman et al. [24] toteaa, että EAC-pääsynhallinta vaatii julkisten avainten hallintaa ja lisää siten monimutkaisuutta, mutta samalla se vahvistaa tietoturvaa.

Eurooppalaista e-passien turvallisuustasoa pidetään luotettavampana kuin muiden maiden, minkä Jeng ja Chen [33] ovat tutkimuksessaan havainneet esimerkiksi Saksan e-passitoteutuksesta. Euroopan maista lähes kaikki ovat liittyneet Public Key Directory (PKD) -palveluun. Saksa on ollut ensimmäisenä eurooppalaisena maana PKD:ssa mukana vuodesta 2007 saakka. Ranska on liittynyt vuonna 2008, Sveitsi vuonna 2009. Latvia, Tšekki, Slovakia, Hollanti ja Itävalta vuodesta 2010, kun esimerkiksi Suomi on liittynyt PKD:hen vuonna 2016. ICAO:n PKD-palvelu on maailmanlaajuinen keskitetty tietovaranto sisältäen salaustekniikkaa, jota tarvitaan e-passien turvatekijöiden tarkistukseen. Erityisesti e-passien hyöty tulee rajatarkastuksissa silloin, kun mikrosirulta luetaan tietoja PKD-ratkaisun avulla. Siruilla pitäisi olla ajantasainen tieto siitä, mitkä maat ovat PKD-järjestelmän sekä siten myös PKI-järjestelmän piirissä ja kenellä on voimassa oleva sopimus siitä, että sensitiivistä tietoa pääsee lukemaan. Euroopan unionin jäsenmaiden osalta jokainen maa vastaa itse PKI-menettelystä ja avaimen hallinnoimisesta. Tästä on maininta Suomen passilaissa [51].

E-passien tietosuojakysymykset ovat edelleen tutkimuksen alaisina nimenomaan mikrosirun sisältämien arkaluontoisten tietojen vuoksi. Euroopan alueella toisen sukupolven e-passeissa toteutetaan Bogari et al. [4] mukaan ICAO:n standardissa määriteltyä aktiivista autentikointia (AA). BAC -pääsynvalvontaan perustuva tekniikka todennäköisesti korvautuu vuoteen 2018 mennessä Supplemental Access Control (SAC)-protokollalla, joka puolestaan pohjautuu ICAO:n standardissa määriteltyyn PACE-menetelmään [52]. Tekniikan näkökulmasta e-passi kuuluu silloin kolmanteen sukupolveen. Peeters et al. [52] ovat esittäneet vaihtoehtoista IBIHOP+ -

autentikointiprotokollaa eurooppalaisessa FIDELITY-tutkimusprojektissa. FIDELITY-lyhenne tulee sanoista Fast and trustworthy Identity Delivery and check with ePassports leveraging Traveller privacy. Projekti on käynnissä ja sen tavoitteena on mm. tulevaisuuden e-passin arkkitehtuuriin vaikuttaminen.

5.6 Suomalainen e-passi

Suomen passi on Suomen kansalaiselle myönnettävä matkustusasiakirja, jolla toteutetaan perustuslaillista liikkumisvapautta, mutta passi toimii myös virallisena todistuksena haltijansa henkilöllisyydestä [54]. Suomalainen e-passi noudattaa Euroopan unionin yhteistä linjaa ja säännöstöä e-passeista passilaissa [51] mainitulla tavalla. Passilakiin vuodelta 2006 perustui myös Suomessa ensimmäisen biometrisen tunnisteen käyttö passissa. Tämä tunniste oli kasvokuva. Euroopan parlamentin ja neuvoston asetus [57] (EY) N:0 444/2009 määrittää, että passeissa on oltava erittäin turvallinen tallennusväline, jossa on kasvokuva ja kaksi sormenjälkeä yhteentoimivassa muodossa. Vuonna 2009 lisättiin Suomen passeihin toinen biometrinen tunniste, sormenjälkitiedot RFID-teknologiaan perustuvalle mikrosirulle.

Asetuksen [57] mukaan sormenjälkitiedot on otettava alaspainetuista sormista. Ensisijaisesti e-passiin otetaan hakijan molempien käsien etusormien sormenjälkitiedot. Mikäli etusormien luku ei onnistu, kerätään sormenjälkitieto keskisormesta, nimettömästä tai peukalosta. Tiedot on suojattava ja tallennusvälineen on oltava kapasiteetiltaan riittävä, jotta se kykenee takaamaan tietoturvaa eheyden, aitouden ja luottamuksellisuuden vaatimuksista. Suomessa Poliisihallituksen [54] vastuulla on, että tiedot suojataan EU:n passiasetuksen [11] ja sen soveltamiseksi annettujen säännösten [57] mukaisesti. Passin teknisessä osassa olevat tiedot suojataan luvatonta käsittelyä vastaan ja samalla pyritään estämään tietojen luvaton lukeminen ja muuttaminen. Koska passin mikrosiru sisältää arkaluontoista henkilötietoa, on viranomaisen myös pyrittävä tehokkaasti löytämään keinot tietoihin tunkeutumista ja muuta luvatonta käyttöä vastaan. Suomen uudet passit täyttävät ICAO 9303 -standardin mukaiset turvavaatimukset sekä omaavat vapaavalintaiset lisäturvaominaisuudet. Tietosuoja koskee myös RFID-sirua, johon on liitetty Suomen valtion sähköinen allekirjoitus takaamaan aitoutta.

Vuonna 2012 on esitetty passilain muuttamista erityisesti niiltä osin, jossa on selvennetty tietosuojan näkökulmia passin sirun osalta. Esityksessä mainitaan, että Suomen passin sirun tiedot on suojattu digitaalisella allekirjoituksella. Suomen

valtion allekirjoituksen tarkistamalla passisirua lukeva viranomainen voi varmistua siitä, että passin tiedot ovat alkuperäiset ja muuttumattomat. Digitaalisella allekirjoituksella pystytään varmistamaan myös se, ettei sirulle ole jälkikäteen lisätty mitään tietoa. Sormenjälkitietoja suojataan erikseen siten, että niitä voi lukea sirulta vain Suomen viranomaisten myöntämän varmenteen avulla.

Poliisin [54] mukaan e-passin tietosivulla oleva kasvokuva on tarkoitettu passinhaltijan silmämääräiseen tunnistamiseen. Kasvokuvan tulee olla frontaalinen, edestä päin kuvattu. ISO/IEC 19794-5 -standardi määrittelee kasvokuvan tarkemmin. Tietotekniikkaa hyväksikäyttävä koneellinen kasvotunnistusmenetelmä vaatii mahdollisimman tuoreen kasvokuvan passinhaltijasta. Sama kuva on tallennettu sirulle koneellista kasvotunnistusta varten. Mitä vanhempi kuva on, sitä epäluotettavampaa on sekä silmämääräinen että koneellinen kasvotunnistus, joka rajatarkastusautomaatteilla tapahtuu reaaliaikaisen kasvokuvan vertaamisena passin mikrosirulle tallennettuun kasvokuvaan.

Rajavartiolaitoksella on henkilötietojen käsittelyyn liittyvän lain [38] perusteella oikeus vastaanottaa henkilön fyysisiin ominaisuuksiin perustuva sähköinen tunniste, joka on liitetty matkustusasiakirjaan. Tunnisteita käsitellessään viranomaisen tulee erityisesti huolehtia tietoturvasta. Koska Suomi kuuluu Schengen-alueeseen, on rajatarkastajan noudatettava Schengenin rajasäännöstön [60] ohjeita asianmukaisen koulutuksen antamisesta rajavartioille.

Kuva 5.3: Esimerkki Suomen passista ja koneluettavasta rivistä [54].

Suomen passilaki [51] määrittelee tarkemmin sen, mitkä tiedot merkitään passiin. Näitä tietoja ovat henkilöstä: sukunimi, etunimet, sukupuoli, henkilötunnus, kansalaisuus ja syntymäkotikunta. Passin tietoja ovat: passin myöntämispäivä, pas-

sin viimeinen voimassaolopäivä, passin myöntänyt viranomainen ja passin numero. Lisäksi vaaditaan passinhaltijan kasvokuva ja nimikirjoitus. Passin tekniseen osaan tallennetaan edellämainittujen tietojen lisäksi kasvokuva ja sormenjäljet. ICAO Doc 9303 -standardin [29] mukaan JPEG- tai JPEG2000-standardeja voidaan käyttää tiedon kompressointiin erityisesti kasvokuvassa. Optimaalinen kompressoitu koko on 15 - 20 kilotavun verran. Suomen passissa kasvokuvan digitaalinen formaatti on JPEG2000 sisältäen metadataa. JPEG2000-kompressointi voi tiivistää kuvan kokoa. Kompressointiin vaikuttaa kuvassa olevat tekijät, kuten henkilön vaatetus tai hiustyyli.

Teknisen osan tietojen aitouden ja eheyden varmistaminen kuuluu viranomaisille. Suomessa julkisen avaimen hallinnoinnista vastaa Väestörekisterikeskus (VRK), joka siis luo varmenteen tähän toiminnallisuuteen. Laki Väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista [39] on säätänyt VRK:n tehtäväksi tuottaa, tarjota ja hallinnoida varmennetussa sähköisessä asioinnissa käytettäväksi tarkoitetut varmenteet sekä sen käyttöön liittyvät varmennehakemisto- ja sulkulistapalvelut. Passinhaltijan oikeudesta tarkastaa passin tekniseen osaan hänestä talletetut tiedot säädetään puolestaan EU:n passiasetuksessa [11].

Biometrisia tunnisteita saa käyttää ainoastaan asiakirjan aitouden tunnistamiseksi tai asiakirjan haltijan henkilöllisyyden varmistamiseksi vertaamalla biometrisia tunnisteita tilanteessa, jossa passi on lain mukaan esitettävä [51]. Passinhaltijan tunnistaminen ei perustu pelkkään sormenjälkitietoon, vaan on kokonaisvaltaista. Tunnistaminen voi perustua tunnistautumiseen tai se voi olla passivista tunnistamista, joka ei edellytä tunnistettavalta henkilöltä omaa toimintaa ja jossa tunnistettava ei välttämättä edes tiedä tulevansa tunnistetuksi. Joka tapauksessa tarkistustilanteessa henkilön fyysisiin ominaisuuksiin perustuvia tunnistetietoja käsiteltäessä tulee lain mukaan erityisesti huolehtia niiden tietoturvasta.

Koska viranomainen myöntää virallisen matkustusasiakirjan, on sen tehtävä myös varmistaa matkustusasiakirjan käsittelyketjussa tarvittava tietojen luokittelu, jolla asetettu vaatimustaso tietosuojan ja tietoturvan osalta voidaan täyttää. Varsinkin arkaluonteisia henkilötietoja käsiteltäessä on viranomaisten ja muiden osapuolien tunnettava periaatteet tietojen eheydestä, luottamuksellisuudesta ja käytettävyydestä asiakirjojen suojauksessa. Esimerkiksi Suomen passilaissa viitataan käsittelyketjuun ja vastuisiin tilanteessa, jossa on tehtävä passin laadun ja sisällön suhteen toimenpiteitä. Käytännössä viranomainen vastaa laadullisen tarkastamisen järjestämisestä, mutta se voi antaa tehtävän palvelun tuottajalle. Laatuvaatimuksista ja

turvallisuusjärjestelyistä on sovittava ja huomioitava tietoturvan säännökset. [51]

Poliisihallitus voi siirtää yksityiselle palveluntuottajalle passin laadun ja oikeasisältöisyyden tarkastamista sekä passin toimittamisen. Palveluntuottajan kanssa sovitaan passin toimitukseen liittyvän tehtävän sisältö ja laatuvaatimukset. Edelleen on aiheellista sopia turvallisuusjärjestelyistä ja muista passin toimittamiseen liittyvistä asianmukaisen hoitamisen kannalta tarpeellisista seikoista, jolloin huomioidaan viranomaisia velvoittavat tietoturvallisuutta koskevat säännökset. Käytännössä se merkitsee, että vastuuviranomaisen on luokiteltava tietoturvatarpeiltaan eroavat asiat erikseen. Tietoturvaa erityisesti vaativat tietoaineistot, sähköinen tiedonkäsittely ja prosessit voivat muodostaa oman luokittelukriteerien mukaisen ryhmän. Kriteereissä on tärkeää huomioida tietojen elinkaari.[51]

Suomessa on käytössä seuraavat passilaissa [51] luetellut passityypit: tavallinen passi, väliaikainen passi, hätäpassi, tilapäinen passi, diplomaattipassi, virkapassi ja merimiespassi. Tavallinen suomalainen e-passi on voimassa viisi vuotta ja siinä on siis biometriset tunnisteet. Sormenjälkitietoja ei tarvitse antaa uudelleen passia uusittaessa, mikäli sormenjälkitiedot ja nimikirjoitusnäyte on otettu enintään kuusi vuotta sitten eikä haltijan nimi ole muuttunut. Voimassaoloajan rajoituksella pyritään siihen, että sirulla olevat tiedot täyttävät tietoturvallisuuden vaatimukset. Passilaissa mainittujen passityyppien lisäksi Suomessa on käytössä myös Ahvenanmaan passi, väliaikainen Ahvenanmaan passi, muukalaispassi, väliaikainen muukalaispassi ja pakolaisen matkustusasiakirja.

Poliisin vuosikertomuksissa [54] kerrotaan passiuudistuksista sekä ilmoitetaan numeeriset tilastotiedot, joita on koottu taulukkoon 5.2. Uuden biometrisen tunnisteen (kasvokuva) sisältävän e-passin käyttöönotto Suomessa tapahtui elokuussa 2006. Myönnettyjen passien lukumäärä oli tuolloin reilut 515 000 kappaletta. 10 vuoden ajan tilastohavainnoissa suurin pudotus on tapahtunut vuonna 2007. Toinen miinusmerkkinen kasvuvuosi on ollut vuonna 2009, jolloin myönnettiin noin 427 600 passia. Tuolloin biometristen tunnisteiden käyttö passissa laajeni. Kesäkuusta 2009 lähtien Suomen e-passeihin on ollut sirulle talletettuna biometrisina tunnisteina kasvokuva ja hakijan kaksi sormenjälkeä. Suomen passeja myönnetään myös ulkomailla. Esimerkiksi vuonna 2014 Suomen passeja myönnettiin yli 18 000 kappaletta Suomen ulkomaanedustustoissa kautta maailman.

Passien lukumäärä on kasvanut hieman. E-passi sovelluksen teknologiaratkaisu ei ole vähentänyt suomalaisten passien hakemista. Passin hakeminen on mahdollista sähköisessä asiointipalvelussa tai lupapalvelupistessä.

Taulukko 5.2: Suomen passitilasto 2006 - 2015 (mukaeltu) [54].

Vuosi	Lukumäärä	Kasvu %
2006	515 778	+-
2007	374 375	-27
2008	433 522	+16
2009	427 580	-1
2010	459 416	+7
2011	507 220	+10
2012	643 595	+27
2013	692 688	+8
2014	721 794	+4
2015	774 570	+7

Suomen uusin passimalli on julkaistu marraskuussa 2016. Uusi passimalli D.1 tulee voimaan vuoden 2017 alusta. Turvatekijöitä on lisätty ja näkyviä ulkoasumuutoksia on mm. Suomi 100 vuotta teemaan liittyen passikirjan kannen kuvioissa. Passin muotoilu on suunniteltu kokonaan uudelleen, mutta silti perinteisiäkin elementtejä on Poliisin mukaan haluttu pitää mukana. Esimerkiksi joutsen löytyy perinteisesti passista ja henkilökortista. Uuden passin viisumisivuja nopeasti selaamalla voi nähdä joutsenen lentävän. Lapin luonto näyttäytyy passin muotoilussa. Revontuliin perustuu monet erilaiset turvatekijät. Passinhaltijan kasvokuva on e-passilla kaikkiaan viidessä paikassa vaikeuttamassa sen väärentämistä. Yksi kuva on mikrosirulla ja muut kasvokuvat löytyvät passista tulostettuna neljällä erilaisella teknisellä ratkaisulla.

5.7 EU:n ja Schengenin yhteistyö

Euroopan unionin kansalaisena matkustaessa Schengen-alueeseen kuuluvasta EU-maasta toiseen ei tarvitse esittää henkilötodistusta tai passia. Käytännössä kuitenkin esimerkiksi lentokoneeseen pääsy edellyttää henkilöllisyyden osoittamista passilla. Joissakin EU-maissa on kansallisia säädöksiä, joiden vuoksi passia voidaan pyytää esitettäväksi. Sisärajattomaan Schengen-alueeseen, joka perustuu vuonna 1985 tehtyyn Schengenin sopimukseen kuuluvia maita ovat nykyään Alankomaat, Belgia,

Espanja, Islanti, Italia, Itävalta, Kreikka, Latvia, Liechtenstein, Liettua, Luxemburg, Malta, Norja, Portugali, Puola, Ranska, Ruotsi, Saksa, Slovakia, Slovenia, Suomi, Sveitsi, Tanska, Tšekki, Unkari ja Viro. Kroatia on parhaillaan liittymässä Schengeniin. Suomi ja Ruotsi allekirjoittivat Schengen sopimuksen 1996. Nämä maat muodostavat alueen, johon kuuluvien maiden välillä ei ole matkustusrajoituksia eikä rajatarkastuksia. Schengenin säännöstön mukaisesti tilanne voi tosin muuttua, mikäli jäsenmaat kokevat yleisen järjestyksen tai sisäisen turvallisuuden olevan vaarassa. EU-maista Bulgaria, Kroatia, Kypros, Irlanti, Romania ja Yhdistyneet kuningaskunnat vaativat passia tai henkilötodistusta. Muun kuin EU-kansalaisen matkustamiseen koskee passivelvoite ja lisäksi joissakin tapauksissa tarvitaan viisumi. [14]

Euroopassa rajatarkastuksien yhtenä tavoitteena on passien sisältämän biometrian avulla pystyä tarkistamaan (1:1 verifioinnilla) ja tunnistamaan, että tietty passi kuuluu tietylle henkilölle. Tästä on olemassa Suomessa laki henkilötietojen käsittelystä rajavartiolaitoksessa 579/2005 [38]. Biometriset tiedot ovat erittäin arkaluonteisia, joten vain toimivaltaisilla viranomaisilla on mahdollisuus päästä RFID-tunnisteen tietoihin. Euroopan komission mukaan 1,2 miljardia ihmistä on tunnistettu biometrisen tunnistamisen kautta. Tämä tieto on peräisin vuodelta 2015 European Association for Biometrics (EAB) konferenssista, jossa Euroopan komission edustaja Paolo Salieri EC DG Home -toimistosta luennoi. Henkilötunnistamistavasta ei ole tarkempaa tietoa, mutta nykyisin on käytössä enimmäkseen kasvotunnistus ja sormenjälkitunnistus. Iiristunnistaminen on harvinaisempaa. On todettu, että kahden tai useamman biometrisen tunnisteen käyttö toisi varmuutta henkilötunnistamisen sovelluksissa. ISO/IEC 27001 standardin [64] mukaan pääsyoikeuksien valvontaan liittyy sovelluksen pääsynvalvonta. Sovelluksissa, joissa on arkaluontoista henkilötietoa tulee järjestää eristetty tietojärjestelmäympäristö ja rajoittaa pääsynvalvontaperiaatteiden mukaisesti tietojen käyttöä ja pääsyä tietoihin [64].

Euroopan parlamentin ja neuvoston asetus (EY) N:o 562/2006 koskee Schengenin rajasäännöstöä. Se [60] määrittelee muun muassa sen, että ulkorajat voidaan ylittää ainoastaan rajanylityspaikoista. Ulkorajoja ylittäville tehdään vähimmäistarkastus henkilöllisyyden toteamisella matkustusasiakirjoista EU:n kansalaisille tai muille vapaaseen liikkuvuuteen oikeutetuilta. Muille kuin EU:n kansalaisille tehdään Schengenin rajasäännöstön mukaan perusteellinen tarkastus ja tutkitaan maahantuloedellytysten täyttyminen. Sisärajat voi ylittää kansalaisuudesta riippumatta millä tahansa rajanylityspaikalla ilman rajatarkastusta. Kansallinen poliisiviranomainen voi pyytää henkilötodistusta tai passia sisärajoilla ilman rajavalvontatarkoitusta.

6 E-passin tulevaisuus

Matkustusturvallisuutta parannetaan jatkuvasti. Matkustusasiakirjojen turvatekijöitä lisätään ja kehitetään, joten e-passilla on tulevaisuutta. Biometrinen teknologia on valmista, mutta se vain odottaa vielä laajempaa käyttöönottoa. Globalisoituminen on aiheuttanut erityisesti vaatimuksia matkustusasiakirjojen turvallisuustekijöihin, toteaa Kundra et al. [37]. Samaa voi päätellä e-passi sovelluksen implementaatioista. Yhä useammat maat ovat ottaneet ICAO:n määrittelyt matkustusasiakirjoihin, mutta biometria vaatii toimivan prosessin. E-passeihin on lisätty biometrisia tunnisteita ja selkeitä turvatekijöitä, jolloin kansalaisten luottamus on kasvanut. Rebnen [56] mukaan viranomaisten toiminnalla on suuri merkitys siinä, kuinka ihmiset luottavat biometriaan. Esimerkiksi Malesian, Japanin ja Etelä-Korean alueilla biometriaan suhtaudutaan myönteisellä asenteella ja biometriikka on siellä jokapäiväistä. Turvatekijöillä pyritään suojaamaan e-passia kopioinnilta ja jäljennöksiltä ja sen tietosisältöjen muuttamiselta. Pienin kehitysaskelin saavutettu luottamus näkyy lisääntyvinä e-passinhaltijoina. Matkustamisen arvioidaan kaksinkertaistuvan 2030 -luvulla nykyisestä tasosta. E-passin ominaisuuksien tulee vastata kasvaviin turvallisuusvaatimuksiin, mutta myös käyttäjien tulee hyväksyä teknologiaratkaisut.

E-passin mikrosirun kertakirjoitettavuuden muutos on tietosuojauksen kysymys. Määrittelyssä on huomioitava tarkasti se, mitä tietoja sirulle päivitetään. Esimerkiksi rajatatarkastuksen leimaukset, tarkoittaen maahansaapumista ja -lähtöä koskevia tietoja, ovat sirulle talletettavia uusia tietoja: viisumien maahantuloleimaus (entry) ja maastalähtöleimaus (exit). Jos nämä päivämäärätiedot olisivat koneellisesti luettavissa, helpottuisi alueella oleskelun laskeminen ja muu tarkastustoiminta. Sähköisen leimauksen etuna on parempi yhtenäisyys, korkeampi tietoturvasuoja ja helppokäyttöisyys tietojen katselemiseksi.

On esitetty ajatuksia siitä, että passin mikrosiru keräisi tietoa matkustajan matkoista, jolloin sirulla olisi tallessa henkilön matkustushistoria. Turvallisuusviranomaisille tästä voi olla hyötyä, jos rekistereistä saa irti ajantasaista tietoa. Rekistereitä syntyy, mutta tulisi selvittää, millä resursseilla tietoja hyödynnetään. Perusteellinen ja realistinen arviointi siitä, onko edes turvallisuusviranomaisten tarpeen kontrolloida matkustajaa tällä tasolla olisi hyödyllinen. Tekniset parannukset pitää

olla nivottuna prosesseihin. Esimerkiksi tietoturvaa parantava päätelaitteiden vahvempi autentikointi vaatii laajaa tietojärjestelmäuudistusta ja koordinointia.

Kehitysvaiheessa neljännen sukupolven e-passi on jo suunnitteilla. Loogisen tietorakenteen (LDS2) ratkaisua työstetään ICAO:n teknisessä työryhmässä. LDS2 ratkaisu laajentaisi e-passin mikrosirua, mikä merkitsisi dynaamisuutta matkustustietoihin. Sen luvataan myös antavan lisäsuojaa väärennyksiä vastaan. Ratkaisu estäisi tietojen kopiointia ja valtuuttamattomien tahojen pääsyä lukemaan tai lisäämään sirulle tietoja. Sirun dynaamisuuden ja tietosuojan kehittämiseen vaikuttaa sitä hyödyntävän teknologian kehittäminen. E-passin kopiointia haittaavia turvatekijöitä ovat myös esimerkiksi tietosivun läpinäkyvä ikkuna ja muuttuva laser-kuviointi. Passin tietosivu voi sisältää useita laser-kuvioita ja -kaiverruksia. E-passin valmistusmateriaalina voidaan käyttää polykarbonaattia tai muuta vaikeasti jäljiteltävää erikoismateriaalia, joihin turvatekijöitä voi helposti kehittää.

Ehdotettuja teknologioita on valikoitu ja analysoitu, mistä tuloksena on, että uusia protokollia voidaan vain osittain kelpuuttaa e-passin mikrosirulle. Vaikka teknisiä ratkaisuja hyväksytään, vaatii varsinainen käyttöönotto lainmuutokset. Tekniset ratkaisut pitäisi aina taipua hyötyihin, jotta ne olisivat järkevässä suhteessa kustannuksiin. Erityisesti prosessinäkökulmasta laillisuus ja tasasuhtaisuus, verrannollisuus ja yhdenvertaisuus ovat tärkeitä seikkoja, joita tulevassa e-passin sovelluksessa tulee olla huomioituna.

6.1 E-passin etiikka

Etiikka on laaja-alainen käsite. Se on teoreettinen ja pohdiskeleva tiede, joka tutkii ihmisen käsityksiä hyvästä ja pahasta sekä moraalia oikeasta ja väärästä. Moraalilla tarkoitetaan ihmisen käytännön elämän eri tilanteissa tekemiä valintoja. Jos yksilöllä on kykyä ja mahdollisuuksia harkintaan valittavissa olevien vaihtoehtojen välillä, on teko moraalinen. Harelin [25] näkemys on, ettei suuri yleisö vielä tiedä tarpeeksi biometriasta, ja vastustaa siihen liittyvää vaistonvaraisesti. Negatiivinen suhtautuminen sormenjälkien keräämiseen voi johtua mielleyhtymästä rikollisuuteen. Biometrian kokonaismerkitystä ei ilmeisesti täysin ymmärretä. Harelin johtopäätös on, että ihmisiä yritetään vapaaehtoisesti saada erilaisten houkuttimien avulla suostumaan biometrisien järjestelmien käyttäjäksi. Henkilö voi saada jotain etua palvelua käyttäessään, esimerkiksi hän pääsee jonon ohi tai voi saada muutoin erityiskohtelua [25].

E-passi sovelluksen taustalla on lait ja asetukset arkaluontoisista henkilötiedoista ja turvallisuudesta. Biometristen järjestelmien käyttö tarkoittaa eettisesti hyväksyttäviä yhteiskunnallisesti huomioitavia asioita muun muassa suunnittelun ohjeistuksissa, esittelyvaiheessa sekä toiminnallisessa vaiheessa. Teknologian läpinäkyvyys tarkoittaa esimerkiksi sitä, että järjestelmä kommunikoi selvästi siitä, mikä on biometrisen tunnistamisen luonteeseen liittyvää. Henkilötunnistamisessa vertailualgoritmi täytyy tuottaa tarkkoja vastaavuuksia tuloksissa erilaisista henkilöistä riippumatta iästä, sukupuolesta tai etnisestä taustasta. Tämä puolestaan vaatii biometrisen tunnisteen laadulta entistä suurempaa tarkkuustasoa ja laatutekijöitä. Se taho, jolla on vastuu biometrisesta henkilötunnistamisesta täytyy toimia vastuullisesti. Vastuullinen toimija ottaa täyden kontrollin käytetystä teknologiasta ja sillä tulee olla oikeus olla hyväksymättä prosesseja ja tuloksia. Henkilötunnistamisessa käytetyn järjestelmän tulee tarjota tilastotietoa laadunvalvonnan ja suorituskyvyn analysointia varten.

Euroopan komission ohjelmassa on suunnitteilla tutkimuksia mm. uusista biometrisen tiedon mahdollisuuksista e-passin sirulle. Mallinnustekniikka, tekoäly (artificial intelligence) ja multimodaaliset biometriset ratkaisut e-passeissa sekä rajatarkastuksissa ovat olleet esillä. Hakutoiminnallisuuksia halutaan helpottaa, mutta kuitenkin tietoturvatason tulee olla korkea. Keskustelua aiheuttavat eettiset, yhteiskunnalliset ja tiedon suojauksen näkökulmat ja näiden sopusuhtainen sisällyttäminen biometriikka-järjestelmiin. EU komission tavoite on parantaa kasvotunnistusta ja nopeuttaa biometrista käsittelyä. Käytännön kokemuksiin perustuen olisi käyttäjäystävällisempää operoida yhteydettömällä kosketusvapaalla sormenjälkitietojen käsittelyn laitteella, kuin sellaisella laitteella, johon sormenjälkitietojen kerääminen tapahtuu painamalla sormet lasille. Mobiililaitteet yleistyvät myös biometriikan käsittelyssä.

E-passin sovellusmahdollisuus on olla eettisen arvokkuuden edistäjänä. Sen toiminnallinen pyrkimys on estää väärennöksiä. Se puolestaan tuo vakautta henkilötunnistamisen menetelmiin. Saman toteavat Morshed et al. [48], mutta tutkijat pitävät e-passin RFID-tunnistetta haasteellisena tietosuojan näkökulmasta. Pyrkimys tietojen parempaan suojaamiseen on otettava vakavasti. Kyseessä on yksityisyyden suojan periaate. On kuitenkin olemassa hienoinen riski, että yksityisyyden suoja vie liikaa huomiota läpinäkyvyyden, yhdenvertaisuuden ja vastuullisuuden näkökulmista. Yksityisyyden suoja kapenee johtuen maailman turvallisuustilanteesta. Yksityisyyden suojalle riittää säilyminen sillä tasolla, että se estää väärinkäytökset, mut-

ta ei käytännön toimintaa. Tasapaino yhdenvertaisuuden ja vastuullisuuden kanssa ovat yksityisyyden suojan tulevaisuuden haasteita.

Kattava suunnittelu sosioeettisiin vaatimuksiin nähden sisältää esimerkiksi sen, että tallennusteknologian täytyy tuottaa riittävän hyvälaatuista kuvaa henkilöistä riippumatta iästä, sukupuolesta tai etnisestä taustasta. Lisäksi biometrian keräys ja tallennus tulee olla riittävän laadukasta henkilöille, joilla on erilaiset fyysiset ja psyykkiset ominaisuudet sekä tiedolliset taidot.

Yhteiskunnallisesta sosioeettisestä näkökulmasta katsoen vaatimukset käytännöistä ja menettelytavoista tulee huomioida ihmisarvoisesti. Aina tulee olemaan prosessissa poikkeustilanteita, joissa ilmenee esimerkiksi virhetilanteita biometriassa ja tilanteessa, joissa järjestelmästä ei löydy vastaavuutta. Näihin seikkoihin tulee löytää ihmisarvon kunnioittavia menettelytapoja. Kaikki ihmiset eivät ole nokkelia, ketteriä ja nopeita. Matkustajat, jotka eivät pysty itse käyttämään biometrisia järjestelmiä tilapäisen tai pysyvän olosuhteen vuoksi, tulisi saada selkeät käyttöohjeet henkilötunnistamisen tilanteisiin. Maailmassa on noin 1,5 miljardia ihmistä, jotka eivät pysty todistamaan identiteettiään. Useimmat ovat rekisteröimättömiä lapsia ja aikuisia köyhistä olosuhteista. Erityistilanteiden ja etenkin virhetilanteiden käsittelystä tulisi kehittää universaalit menettelytavat ja toimintaperiaatteet. E-passin etiikkaa on syytä tarkastella jatkuvasti.

6.2 E-passin uhat ja mahdollisuudet

ICAO [29] dokumentaation mukaan e-passin tietoturvaa koskevat määrittelyt ovat tarkoitettu yhteiseksi kansainväliseksi kehykseksi. Näin kuuluu ollakin, jotta tasapuolinen ja yhdenvertainen kohtelu toteutuu henkilötunnistamisessa. Parannuksilla pyritään estämään e-passin peukalointi ja luvaton tietoihin kajoaminen. Bogari et al. [4] toteavat, että siitä lähtien kun RFID-tunniste otettiin käyttöön e-passeissa, on siihen kohdistunut tietoturvahaavoittuvuuksia. E-passeissa käytetty julkisen avaimen salausmenetelmän allekirjoitussuojaus toimii mikrosirun tiedoille, mutta se ei estä mahdollisen hyökkääjän kopiointitoimenpidettä ja juuri tätä pidetään asiantuntijapiireissä huolenaiheena e-passissa.

Choi et al. [8] mukaan e-passin uhka liittyy yksityisyydensuojaan. Suurin ongelma on henkilökohtaisten tietojen vuotaminen oikeudettomalle taholle. Kun tietovuoto tapahtuu olosuhteissa, joista lukutapahtumasta ei jää mitään jälkeä tai tietoa passinhaltijalle, on edessä mahdollisesti isoja sosiaalisia ongelmia, jollei asiaa korja-

ta.

On olemassa riski, että kerättyjä biometrisia tietoja haltuunsa saanut taho käyttää biometrisia tunnistamistietoja hyväkseen ja esiintyy toisena henkilönä. Tätä kutsutaan identiteettivarkaudeksi, johon on tulossa Suomessa rikoslakiin oma rangaistava rikosnimike pykälineen. Tämänkaltaista toimintaa on vaikea etukäteen estää muutoin kuin noudattamalla erityistä huolellisuutta henkilötietojen käsittelyssä, kuten henkilötietolaki [26] kehottaa.

Morshed et al. [48] ovat tutkineet RFID-tunnisteen tietosuojaa e-passeissa ja päätyneet passiivisen hyökkäyksen simulaatiotesteissään siihen, että RFID-järjestelmässä 12- ja 16-bittinen tieto on täysin haavoittuvaa tietoturvahyökkäyksille. 32-bittisessä RFID-tunnisteessa on jonkin verran haavoittuvutta. Hyvä tietosuoja- ja tietoturvataso saavutetaan 64-bittisellä ratkaisulla. Morshed et al. tutkimuksissaan toteavat, että hyökkäysyritykset 64-bittistä RFID-tunnistetta kohtaan pysyivät suojattuna. Varmuuden vuoksi he kuitenkin suosittelevat e-passin RFID-tunnisteelle ja lukijalle 96-bittisyyttä tai 128-bittisyyttä. Tämä takaisi parempaa tietoturvaa.

Automaattisen henkilötunnistamisen mahdollisuudet ovat lähes rajattomat. Yksityisellä sektorilla biometrisia tunnisteita käytetään hyvinkin monipuolisesti. Julkisen sektorin sovellukset koskevat laajaa ihmisjoukkoa joko kansallisesti tai kansainvälisesti. Lainsäädäntö ja prosessi on oltava yhtenevä ja toisiaan tukevaa. EU:n tasolla tavoitellaan koneluettavien matkustusasiakirjojen (MRTD) ja erityisesti e-passin tarkastuksen standardia. Rajatarkastuksissa puoliautomaattiset, automaattiset sekä manuaaliset tarkastusmenetelmät vaatisivat tarkastusstandardin. Rajatarkastuksissa havaitaan paljon matkustusasiakirjojen väärinkäyttötapauksia. Vuonna 2015 Euroopan unionin rajaturvallisuusvirasto Frontexin vuosittaisen riskianalyysiraportin [18] mukaan oli havaittu 8 373 matkustusasiakirjan huijaustapausta. Nämä tapaukset raportoitiin rajanylitystilanteissa, joissa kolmannen maan kansalainen saapui EU maahan. Kolmansien maiden kansalaisilla tarkoitetaan muita kuin Pohjoismaiden, EU-maiden, Liechtensteinin tai Sveitsin kansalaisia. Väärennettyjen matkustusasiakirjojen määrä on laskenut yli kymmenellä prosentilla verrattuna aikaisempiin vuosiin, mutta silti falsifikaattien lukumäärä on huomattava.

Frontexin [18] riskianalyysin yhteenvedossa on kolme isoa haastetta, joihin rajatarkastuksissa tulee varautua: ennakoimaton maahantulijoiden virta, lisääntynyt terrorismin uhka ja tasaisesti kasvava matkustajien määrä. Nämä kaikki vaikuttavat henkilötunnistamiseen, e-passeihin ja muihin matkustusasiakirjoihin liittyviin rajavalvonnan ja -tarkastuksen järjestelyihin. Passin tarkastajalta vaaditaan entistä

enemmän tehokkuutta ja lopputulokselta vaikuttavuutta, laadusta tinkimättä.

Sisärajaton vapaan liikkuvuuden alue kattaa jo suurimman osan Eurooppaa. Schengen-alueen sisällä e-passia ei välttämättä tarvita. Vapaa liikkuuvuus on lisännyt matkustamista. Mihin e-passia sitten tarvitaan, jos kansalainen liikkuu vain vapaan liikkuvuuden rajoittamalla alueella? Voisiko liikkuvuutta rinnastaa autojen rekisteriotteisiin? Aikaisemmin autoissa piti olla aina mukana rekisteriote. Nykyään se ei ole pakollista, sillä tietojärjestelmistä voi viranomainen tarkistaa autossa aina kiinnitettynä olevasta rekisteritunnuksesta auton tiedot. Matkustajan tunnistaminen perustuu mahdollisesti samaan; aina matkustajalla mukana oleviin biometrisiin tunnisteisiin, joita tarvittaessa tietojärjestelmistä tarkastetaan.

Rikollisuus ei katso sisä- tai ulkorajoja. Rajat ylittävä rikollisuus on lisääntynyt. Yksi huolestuttava ilmiö on ihmiskauppa. Yhdysvaltain ulkoministeriön mukaan ihmiskaupan uhreja tunnistetaan noin 40 000 vuositasolla, mutta 20 miljoonaa jää tunnistamatta. Euroopan komission jäsenmailtaan koostamassa tilastossa arvioi vuosina 2013 - 2014 olleen yli 15 000 ihmiskaupan uhria, joista 67 % seksuaalisen hyväksikäytön uhreja. Kyse on valtavan mittakaavan ongelmasta. Suomea käytetään läpikulkumaana, mutta se on myös kohdemaa naisten ja tyttöjen seksuaaliseen ihmiskauppaan. Suomeen jää enimmäkseen ihmiskaupan uhreista miehiä ja naisia työperäisen ihmiskaupan uhreiksi. Määrät liikkuvat kymmenistä satoihin henkilöihin vuositasolla. Rajavalvonnan on erittäin vaikea havaita näitä tapauksia matkustusasiakirjojen perusteella. Jos käytettävissä olisi matkustajan matkustushistoria, voisi tilanne olla toinen. Rajanylitysrikoksiin e-passin sirun dynaaminen sisältö voisi olla yksi tekninen ratkaisu. EU komission mukaan ihmiskaupan uhrien tunnistaminen on avaintekijä. Matkustusasiakirjojen käsittely sekä esimerkiksi konsulaattien ja rajatarkastusten prosessien yhtenäisyys ovat tärkeitä.

Ihmiskaupan, terrorismin ja muun vakavan rikollisuuden torjunta tulevat olemaan haasteellisia tehtäviä tulevaisuudessa. Turvallisuusviranomaiset ovat kiinnittäneet huomiota ilmiöön, jossa jotkut EU-kansalaiset matkustavat ulkomaille ja liittyvät siellä terrorismijärjestöihin. He muodostavat palatessaan vakavan riskin EU:n sisäiselle turvallisuudelle [16]. Tässäkin tapauksessa matkustushistoria yhdistettynä muihin tietoihin voisi antaa turvallisuusviranomaiselle vinkkejä ja analyysidataa. Se puolestaan parantaisi EU:n lisäksi muun maailman turvallisuutta.

Turvallisuuden nimissä viime aikoina on monet valtiot pyytäneet lentoliikenteen toimijoita luovuttamaan tietoja matkustajista. Passin yksityiskohtaisia tietoja on vaadittu rikollisten liikkeiden jäljittämiseksi. Yksityisyyden suojaa tulee kun-

nioittaa ja näissäkin tapauksissa henkilökohtaisen tiedon käsittelyssä pitää noudattaa tietosuojasäännöstöjä. Viranomaisten yhteistyö luotettavan tiedonsiirron kautta on keskeistä rajat ylittävässä rikollisuuden torjunnassa.

Kenen turvallisuutta painotetaan? Maailman turvallisuudestako tässä kaikessa on kysymys. Van der Ploeg [74] näkemys on ettei valtion turvallisuus ole yhtäpitävää kansalaisen turvallisuuden kanssa. Henkilökohtainen turvallisuus on jotain muuta kuin organisaation turvallisuus. Tämä pitää varmasti paikkansa. Hollantilainen professori, van der Ploeg vakuuttaa, että keskiverto kansalainen ei tiedä biometrisen e-passin tietosisällöstä. Kansalainen ei ole tietoinen RFID:sta eikä siitä mihin kerätty henkilökohtainen tieto rekisteröidään, missä ja kuinka sitä käsitellään, minne tallennetaan. E-passinhaltija ei välttämättä tule edes ajatelleeksi sitä, kuinka tietojen avulla voidaan jäljittää ihmistä ja miten tämä vaikuttaa ihmisen vapauteen. Kansalainen luottaa omaan valtioonsa ja demokratiaan. Van der Ploegin mukaan on olemassa tekijöitä, jota estävät läpinäkyvyyden ja jäljitettävyyden biometrisissä järjestelmissä. Valtiot vetoavat valtion turvallisuuteen, terrorismin vastaiseen taisteluun ja rikosten ennaltaehkäisyyn ja pitäytyvät täydestä avoimuudesta.

E-passien tietoturvan kehitys täytyy olla jatkuvaa. Tietoturvan tulee ulottua biometriatietoihin, sillä ne ovat olennainen osa e-passin käsittelyketjussa. Automaattinen tarkastus tapahtuu laitteilla, jotka ovat kytketty tietoverkkoon ja integroituihin tietojärjestelmiin. Tietoturva kaikissa vaihessa tulee nostaa sille tasolle, että uhat vähenee. Biometriaa ei säilytetä turhaan. Esimerkiksi Suomen passitietokannassa sormenjälkitiedot ovat kymmenen vuotta säilytettävänä, kun Schengen-alueen viisumitietojärjestelmässä viisumihakijoiden sormenjälkitiedot ovat viisi vuotta tallessa. Salausmenetelmiä on kehitettävä lisää ja niitä on monipuolistettava. Tämä varmasti vaati tietojärjestelmiin kapasiteettia ja kyvykkyyttä. Tietoturva on asennekysymys. Teknisesti on mahdollista muuttaa e-passin elinkaari pidemmäksi ja samalla tietoturvallisemmaksi.

Tulevaisuuden e-passi sukupolven ratkaisuissa on todennäköistä tietoturvallisuuden kehityksen huomiointi kansainvälisen turvallisuuden näkökulmasta. Kehittämisen yhteydessä olisi suotavaa, jos yksityisyydensuojaa huomioitaisiin yhteiskunnan ja yksittäisen henkilön näkökulmasta, jos ja kun henkilökohtaisia tietoja lisätään e-passeihin. Vaudenayn [75] mukaan myös muuta henkilökohtaista tietoa on tarkoitus liittää tulevaisuuden e-passeihin, mikäli standardit hyväksytään ja lainsäädäntö näin vaatii. Näitä ehdotettuja muita henkilökohtaisia tietoja ovat muun muassa passin hakijan muut nimet, syntymäpaikka, sähköpostiosoite, puhelinnu-

mero, ammatti, titteli sekä muut henkilöt, joita passiin voi liittää (esimerkiksi lapset) tai jopa uskonto. Tietosuojan ja yksityisyyden suojan näkökulmasta näitä tietoja passinhaltija ei välttämättä halua näyttää viranomaisille, eikä mielellään esimerkiksi kaupoissa tai hotellin vastaanottotiskillä asioidessaan. On siis edelleen olemassa erinäisiä tilanteita, joissa passia joudutaan näyttämään muillekin kuin viranomaisille ja silloin on olemassa riski, että passin tietoja kerätään muuhun kuin viranomaistarkoituksiin.

Loogisen tietorakenteen kehittäminen mahdollistaisi lisää biometriatunnisteita sirulle. Primäärisesti e-passin sirulla on kasvokuva. Toissijaisena biometrisena tunnisteena Euroopassa on jo sormenjälkitiedot, mutta esimerkiksi iiris tunnistetta ei ole vielä juurikaan käytössä. Kasvokuvan päivittäminen olisi myös etu, sillä automaattista kasvojen tunnistamisen järjestelmiä kehitetään rajatarkastuksiin. Kun mikrosirulle voisi myös passin valmistamisen jälkeen tallettaa sekondäärisen biometrisen tunnisteen, olisi enemmän mahdollisuuksia hyödyntää kansallisia biometrisia ohjelmia ja luoda esimerkiksi luotettavan matkustajan ohjelmia.

Multibiometria on tulevaisuutta. Biometriassa tullaan käyttämään multimodaalisia järjestelmiä. Käytännössä esimerkiksi sormenjälkitieto ja iiristunnistus voidaan yhdistää tehokkaammaksi, kun molemmat näytteet kerätään henkilöltä ja ne yhdistetään järjestelmän vertailuvaiheeseen. Mitä useampaa ominaisuutta voidaan kerätä ja verrata, sitä varmempia tuloksia saavutetaan. Tunnistetietojen väärinkäyttö on toki mahdollista, jolloin entistä haastavampaa on ratkaista keinoja useamman tunnistetiedon suojaamiseen.

Vaikka useampaa biometrista tunnistetta käytetään, kohdistuu haku yhteen tietokantaan, josta multimodaalinen vastaus saadaan kerralla. Tämä tunnistamiseen tarkoitettu menettely vaatii myös uusia sensoreita ja entistä kehittyneimpiä yhdistelmään kykeneviä tekniikoita. Biometriset tunnisteet ovat dynaamisia. Se tekee asiasta kiehtovan. On huomioitava, että biometristen tunnisteiden vertailu ei välttämättä tuota absoluuttista totuutta. Se tuottaa todennäköisyyden sille, että hakutulos ja vertailutulos on lähellä jotakin jo kerättyä aineistoa. Ihmiselle jää tulkinnanvaraan mahdollisuus ja se on hienoa.

Jos e-passi kehittyy sirultaan dynaamisemmaksi, on mahdollista myös e-viisumien käyttöönotto. E-viisumi olisi sovellusalueena omansa, mutta huomattava etu olisi siinä, että sähköinen viisumi voidaan lisätä asiakirjaan melkein välittömästi. Se tarkoittaisi viisumiasioiden asiakaspalveluun melkoista virtaviivaisuutta. Sähköinen viisumi vähentäisi kuluja, mitä tulee nykyisellään koko viisumikäsittelyprosessis-

ta mukaan lukien viisumitietojen tallennukset useassa eri vaiheessa sekä erinäiset viisumien leimaamiset. Jos viisumi saadaan lisättyä suoraan passiasiakirjaan, se vähentäisi tietokantaan kohdistuvia hakuja merkittävästi. Läpikulkumatkailu sujuvoituisi, sillä myös kolmansien maiden kansalaisen tunnistaminen helpottuisi tarkastustilanteissa.

Esimerkiksi Euroopan komission sekä EU:n IT Viraston yhteistyössä suunniteltu Registered Traveller Program (RTP) sekä Smart Borders - älykkäät rajat konsepti hyötyisi dynamiikasta. Usein rajanylittävä matkustaja saisi erityiskohtelua rekisteröityessään luotettavaksi matkustajaksi. Älykkäät rajat -ohjelma sisältää useita rajantarkastuksiin liittyviä parannuksia, kuten esimerkiksi viisumien leimauksen sähköisesti (Entry Exit System). Automated Border Control (ABC) -teknologia hyötyy e-passeista, koska standardisoitu, luotettava ja tietosuojavaatimukset täyttävä matkustustieto palvelisi rajatarkastuksia. Tietojärjestelmien avulla reaaliaikaista ja systemaattista matkustajatietoa olisi saatavilla ja tällä tavoin havaittaisiin tyypilliset rajatarkastuksiin liityvät seikat; saapumis- ja lähtemisleimojen vastaavuus tai tietojen muutosyritykset matkustajan taholta. Älykkäät rajat ja ABC ovat olleet hankkeita, joiden hyötyä matkustussujuvuudessa on arvioitu erilaisilla käyttäjäkohtaisilla galluppeilla ja tyytyväisyyskyselyillä. Kysymys on uuden teknologian hyväksymisestä tietyissä tilanteissa. Joillekin ihmisille maasta toiseen matkustaminen on arkipäivää, mutta keskimääräiselle matkustajalle jokapäiväistä rajanylitys ei ole.

E-passin mikrosirun dynaamisuus vaikuttaa moniin osapuoliin. Viranomaisten tehtävä on varmistaa kansalaisten yksityisyyden suojaa koskevat asiat sekä tietoturva henkilötietojen käsittelyssä. Mahdolliset teknologiset muutokset koko sovellusalueella koskee vaatimuksineen passien valmistajia, biometrialaitteiden valmistajia ja automatisoitujen järjestelmien laajaa alaa sekä e-passiin liittyviä rooleja.

7 Yhteenveto

E-passi on tärkeä matkustusasiakirja henkilölle, joka matkustaa maansa rajojen ulkopuolelle. Yhä useammat tekevät niin. Maailmalla kiertävät sadat miljoonat e-passit sisältävät mikrosirulla biometriset tunnisteet. Se seikka, onko hyväksyttävää ja eettistä, että ihmisen biologiset ominaispiirteet kartoitetaan tarkasti ja tallennetaan digitaaliseen formaattiin, jää lukijan ratkaistavaksi tässä tutkimuksessa. Biometria mahdollistaa useamman tiedon keruun kehosta. Kaikkea tietoa ei tarvitse tallentaa e-passille.

E-passin mikrosiru on väliaikainen tallennuspaikka, sillä e-passi on voimassa rajatun ajan. Minne tiedot päätyvät lopulta? Mikä estää kaupallisen toiminnan? Mikä on kasvokuvan, sormenjäljen, silmän verkkokalvon, äänen hinta - biometrian hinta ihmiskunnalle. Kiihtyvän teknologisen kehityksen tuloksena syntyy järjestelmiä, jotka integroituvat pikkuhiljaa toisiinsa ja muodostavat kuvaa ihmisestä. Tutkimuksen perusteella tietosuojausta pyritään varmistamaan lainsäädännöllä, mutta onko se riittävää?

Yksityisyyden raja kapenee. Yksityisyys on oma oikeus määrätä itseään koskevista asioista ja tiedoista. Tietoyhteiskunnassa yksityisyys on ihmisen oma kyky itse päättää siitä kenelle kertoo ja mitä paljastaa itsestään ja missä yhteydessä. Ihminen tarvitsee tilaa ja vapautta ajatella mitä tahtoo, eikä henkilökohtaisesta tiedosta tule tehdä julkista. Tietoyhteiskunnassa julkisen ja yksityisen raja voi olla häilyvä.

Kansalaiset uskovat, että hallitus tai julkisen hallinnon palvelut pitävät huolen kansalaisen identiteetistä varkaita vastaan tai yksityisyyden suojan loukkauksia vastaan. Mistä tämä uskomus johtuu, kun tosiasia on, että identiteettivarkauksia tapahtuu paljon. Identiteetti on arvokas. E-passin tehtävänä on todistaa identiteetti luotettavasti.

ICAO:n tilastojen mukaan 166 valtiota käyttää Interpolin varastettujen tai hukattujen matkustustusasiakirjojen tietokantaa, jonne tehtiin vuonna 2013 yli 800 miljoonaa hakua. Interpolin mukaan vuonna 2016 tuohon tietokantaan tehtiin jo yli 1,8 miljardia hakua. Varastetusta passista voi ilmoittaa viranomaiselle, joka voi mitätöidä passin pätevyyden ja asettaa sen kieltolistalle. E-passin tietoturvan uhkana on se, että passi varastetaan ja sirun tietoja hyväksikäytetään identiteettihuijauksissa.

E-passien turvatekijät kehittyvät ja Suomi on noudattanut omien kansalaistensa e-passien käyttöönotossa viimeisimpiä turvatekijöitä. Yhdysvaltojen, Euroopan ja Suomen e-passien väliset erot liittyvät kansallisiin piirteisiin, perusasioissa ei merkittäviä eroja enää ole muutoin kuin biometristen tunnisteiden käytön osalta. Yhdysvaltojen e-passissa on vain kasvokuva. Siellä kulttuuri ei ole tosiaankaan kypsä muille biometrisille tunnisteille. Eurooppa käyttää ja vaatii kansalaisiltaan antamaan e-passille myös sormenjälkitietoja. Kulttuureissa on siis eroja.

Turvallisuus on kultturikysymys. Kuinka paljon siedetään epävarmuutta, missä tulee sietokyvyn raja vastaan ja tunne vaaratilanteesta. Eurobarometri 2015 [15] kertoo muun muassa, että suomalaisista yli 80 prosenttia uskoo, että tietoverkkorikollisuus lisääntyy. Muut jäsenmaat ovat 63 % osuudellaan samaa mieltä. Luottamus tietoturvaan vaikuttaa suoraan siihen mitä digitaalisia palveluja tullaan tulevaisuudessa käyttämään. Luottamus rakentuu hitaasti, epäluottamus nopeasti.

Tuleeko teknologiaan sellaista säätelyä, jolla tunnistamista rajoitetaan? RFID toteutuksien osalta on huomattava, että sen kautta on mahdollisuus tuottaa ja saada todella runsaasti tietoa ja dataa esineistä, asioista, eläimistä ja ihmisistä. Tutkimuksen kautta ilmeni, että e-passissa RFID on vain pieni, mutta toki tärkeä osa e-passin kokonaisuudessa. RFID-siru toimii tietojen tallennuspaikkana.

Tutkimus keskittyi e-passeihin, jolloin RFID-järjestelmän strateginen merkitys saattoi jäädä hieman kapeaksi. RFID -järjestelmien katsotaan kuitenkin olevan askel kohti ”Internet of Things” - esineiden internettiä. Sovellusalueen jatkotutkimuksena voisi olla mielenkiintoista selvittää mm. sitä, kuinka e-passi ja siihen liittyvä biometria ja sitä jatkossa hyödyntävä automaattinen tunnistus (kasvotunnistus tai iiristunnistus) tai kosketusvapaa sormenjälkitunnistus otetaan maailmalla vastaan, jos e-passi on osa esineiden internettiä.

Tietoturvallisuuteen liittyvät seikat nousevat varmasti arvioitavaksi siinä vaiheessa kun e-passin RFID-mikrosirulle tallennetaan lisää biometriaa. Mikrosirun uudelleenkirjoitus sekä päivitysominaisuus tarvitaan, jotta sille voi tallettaa viisumitietoa ja henkilön matkustushistoriaa. Miten hyvin infrastruktuuri sopeutuu matkustusmäärien arvioituun määrien kaksinkertaistumiseen seuraavien 15 vuoden aikana. Jatkokysymys onkin, miten varmistetaan se, ettei kukaan muu kuin se viranomaistaho, joka tietoa tarvitsee pääse lukemaan matkustushistoriaa tai muuta arkaluontoista henkilötietoa. Miten varmistetaan tietoturva ja yhteentoimivuus globaalisti? Tämä olisi mielenkiintoinen jatkotutkimusaihe.

Lähteet

[1] ABID, M., KANADE, S., PETROVSKA-DELACRÉTAZ, D., DORIZZI, B., JA AFIFI, H. Iris based authentication mechanism for e-passports. Julkaisusarjassa *2nd International Workshop on Security and Communication Networks (IWSCN)* (2010), IEEE, pp. 1–5.

[2] ACCURSIO, E. *Latent Fingerprint Examination : Elements, Human Factors and Recommendations*. Nova Science Publisher, Inc., New York, 2014.

[3] AILISTO, H., AHONEN, P., JA LINDHOLM, M. *Biometrisen tunnistamisen tietoturvallisuus ja yksityisyyden suoja*. Liikenne- ja viestintäministeriö, VTT Elektroniikka, Oulu, 2005.

[4] BOGARI, E. A., ZAVARSKY, P., LINDSKOG, D., JA RUHL, R. An Analysis of Security Weaknesses in the Evolution of RFID Enabled Passport. Julkaisusarjassa *Proceedings of Word Congress on Internet Security (WorldCIS-2012)* (2012), IEEE, pp. 158–166.

[5] BRINGER, J., JA CHAPANNE, H. Biometric identification paradigm: Towards privacy and confidentiality protection. Kirjassa *Biotechnology in Agriculture, Industry and Medicine. Biometrics: Theory, applications and issues*, E. R. Nichols, Ed. Nova Science Publishers, Inc., 2011, ch. 6, pp. 123–141.

[6] BROMBA, M. U. The biometric society–risks and opportunities. Julkaisusarjassa *Advanced Research Workshop-Identity, security, and democracy. Jerusalem* (2006).

[7] BUTT, M., MARTI, S., NOUAK, A., KOPLIN, J., RAGHAVENDRA, R., JA LI, G. Towards e-passport duplicate enrollment check in the European Union. Julkaisusarjassa *European Intelligence and Security Informatics Conference (EISIC)* (2013), IEEE, pp. 247–251.

[8] CHOI, Y.-S., JEON, Y.-J., JA PARK, S.-H. A study on secure protocol using the public key infrastructure approach in an e-passport. Julkaisusarjassa *The 12th International Conference on Advanced Communication Technology (ICACT)* (2010), vol. 1, IEEE, pp. 458–463.

[9] COPPOCK, C. A. *Contrast: an investigator's basic reference guide to fingerprint identification concepts*. Charles C Thomas Publisher, 2007.

[10] COSMI, E., MELONI, P., MARZANO, S., JA SACCO, R. Biometrics: Security vs Privacy. A scientific and bioethical point of view. *Identity, Security and Democracy* (2009), 57.

[11] COUNCIL REGULATION (EC). No 2252/2004 of 13 december 2004 on standards for security features and biometrics in passports and travel documents issued by member states. *OJ L 385* (29.12.2004), 1–6.

[12] EGLITIS, T., PUDZS, M., JA GREITANS, M. Bimodal palm biometric feature extraction using a single RGB image. Julkaisusarjassa *International Conference of the Biometrics Special Interest Group (BIOSIG)* (2014), IEEE, pp. 1–7.

[13] EUROOPAN IHMISOIKEUSSOPIMUS. Euroopan ihmisoikeustuomioistuin. URL `http://www.echr.coe.int/Documents/Convention_FIN.pdf`, viitattu 23.05.2016.

[14] EUROOPAN KOMISSIO. EU-kansalaisten matkustusasiakirjat. URL `http://europa.eu/youreurope/citizens/travel/entry-exit/eu-citizen/index_fi.htm`, viitattu 08.06.2016.

[15] EUROOPAN KOMISSIO. Eurobarometri. URL `http://ec.europa.eu/public_opinion/archives/ebs/ebs_432_fact_fi_fi.pdf`, viitattu 17.08.2016.

[16] EUROOPAN KOMISSIO. Viestinnän pääosasto. Rajavalvonta ja turvallisuus. URL `http://ec.europa.eu/dgs/home-affairs/e-library/docs/brochure-borders-and-security/brochure_borders_and_security_fi.pdf`, viitattu 08.06.2016.

[17] EUROOPPA-NEUVOSTO. PRADO - Aitojen henkilö- ja matkustusasiakirjojen julkinen online-hakemisto. URL `http://www.consilium.europa.eu/prado/FI/prado-start-page.html`, viitattu 31.01.2016.

[18] FRONTEX. European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union. Risk Analysis for 2016. URL `http://frontex.europa.eu/assets/Publications/Risk_Analysis/Annula_Risk_Analysis_2016.pdf`, viitattu 08.06.2016.

[19] GEMALTO. Looking at the future of travel. The fourth generation of ePassport. *Government Programs* (2014).

[20] GLOVER, B., JA BHATT, H. *RFID essentials*. O'Reilly Media, Inc. , 2006.

[21] GREENWOOD, R. The case for supporting traveller identity verification with epassport and automated data sharing. Tekninen raportti VOL.10 - NO.1, ICAO, 2015.

[22] GS1. EPC Tag Data Standard. *Version 1.9* (2014).

[23] GUTIERREZ, P. D., LASTRA, M., HERRERA, F., JA BENITEZ, J. M. A high performance fingerprint matching system for large databases based on GPU. *IEEE Transactions on Information Forensics and Security 9*, 1 (2014), 62–71.

[24] GUTMANN, P., NACCACHE, D., JA PALMER, C. C. E-passport threats. *IEEE Security and Privacy 1*, 1 (2004), 72–75.

[25] HAREL, A. Biometrics, identification and practical ethics. Julkaisusarjassa *Proceedings of the NATO Advanced Research Workshop on Identity, Security and Democracy: The Wider Social and Ethical Implications of Automated Systems for Human Identification Jerusalem, Israel* (2009), IOS Press, pp. 69–84.

[26] HENKILÖTIETOLAKI 523/1999. *Valtion säädöstietopankki Finlex*. Viitattu 01.12.2015, http://www.finlex.fi.

[27] HENLEY & PARTNERS. Visa Restriction Index 2016. URL `https://www.henleyglobal.com/files/download/HP/hvri/HP%20Visa%20Restrictions%20Index%20160223.pdf`, viitattu 31.05.2016.

[28] HOEPMAN, J.-H., HUBBERS, E., JACOBS, B., OOSTDIJK, M., JA SCHREUR, R. W. Crossing borders: Security and privacy issues of the European e-passport. Julkaisusarjassa *International Workshop on Security* (2006), Springer, pp. 152–167.

[29] ICAO DOC 9303. *Machine Readable Travel Documents*, 2015.

[30] ISO/IEC 14443 (ALL PARTS). *Identification cards – Contactless integrated circuit cards – Proximity cards*, 2008.

[31] JÄRVINEN, P. *Tietoturva & yksityisyys*. Docendo, 2002.

[32] JÄRVINEN, P. *Salausmenetelmät*. Docendo, 2003.

[33] JENG, A. B., JA CHEN, L.-Y. How to enhance the security of e-passport. Julkaisusarjassa *International Conference on Machine Learning and Cybernetics* (2009), vol. 5, IEEE, pp. 2922–2926.

[34] KAUBA, C., REISSIG, J., JA UHL, A. Pre-processing cascades and fusion in finger vein recognition. Julkaisusarjassa *International Conference of the Biometrics Special Interest Group (BIOSIG)* (2014), IEEE, pp. 1–6.

[35] KERTTULA, E. *Tietoverkkojen tietoturva*. Edita, Helsinki, 1998.

[36] KUMAR, V. N., JA SRINIVASAN, B. Biometric passport validation scheme using radio frequency identification. *International Journal of Computer Network and Information Security 5*, 5 (2013), 30.

[37] KUNDRA, S., DUREJA, A., JA BHATNAGAR, R. The study of recent technologies used in e-passport system. Julkaisusarjassa *IEEE Global Humanitarian Technology Conference-South Asia Satellite (GHTC-SAS)* (2014), IEEE, pp. 141–146.

[38] LAKI HENKILÖTIETOJEN KÄSITTELYSTÄ RAJAVARTIOLAITOKSESSA 579/2005. *Valtion säädöstietopankki Finlex*. Viitattu 01.12.2015, http://www.finlex.fi.

[39] LAKI VÄESTÖTIETOJÄRJESTELMÄSTÄ JA VÄESTÖREKISTERIKESKUKSEN VARMENNEPALVELUISTA 661/2009. *Valtion säädöstietopankki Finlex*. Viitattu 04.12.2015, http://www.finlex.fi.

[40] LAKI VAHVASTA SÄHKÖISESTÄ TUNNISTAMISESTA JA SÄHKÖISISTÄ ALLEKIRJOITUKSISTA 617/2009. *Valtion säädöstietopankki Finlex*. Viitattu 04.12.2015, http://www.finlex.fi.

[41] LEHPAMER, H. *RFID Design Principles*. Artech House, 2007.

[42] LEHTO, A. *Radioaaltojen maailma*. Otatieto, Tampere, 2006.

[43] LEHTONEN, M., MICHAHELLES, F., STAAKE, T., JA FLEISCH, E. Strengthening the security of machine readable documents by combining RFID and optical memory devices. Kirjassa *Developing Ambient Intelligence*. Springer, 2006, pp. 77–92.

[44] LIU, Y., KASPER, T., LEMKE-RUST, K., JA PAAR, C. E-passport: Cracking basic access control keys. *On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS* (2007), 1531–1547.

[45] MEINGAST, M., KING, J., JA MULLIGAN, D. K. Embedded RFID and everyday things: A case study of the security and privacy risks of the US e-passport. Julkaisusarjassa *IEEE International Conference on RFID* (2007), IEEE, pp. 7–14.

[46] MOHAMED, A. B., ABDEL-HAMID, A., JA MOHAMMED, K. Implementation of an Improved secure system detection for E-passport by using EPC RFID tags. *World Academy of Science, Engineering and Technology Journal 6* (2009), 1–5.

[47] MORDINI, E., JA GREEN, M. *Identity, Security and Democracy: The Wider Social and Ethical Implications of Automated Systems for Human Identification*, vol. 49. Ios Press, 2009.

[48] MORSHED, M. M., ATKINS, A., JA YU, H. Privacy and security protection of RFID data in e-passport. Julkaisusarjassa *5th International Conference on Software, Knowledge Information, Industrial Management and Applications (SKIMA)* (2011), IEEE, pp. 1–7.

[49] NATIONAL RESEARCH COUNCIL AND WHITHER BIOMETRICS COMMITTEE AND OTHERS. *Biometric recognition: challenges and opportunities*. National Academies Press, 2010.

[50] NEUVONEN, R. *Yksityisyyden suoja Suomessa*. Lakimiesliiton kustannus, 2014.

[51] PASSILAKI 671/2006. *Valtion säädöstietopankki Finlex*. Viitattu 01.12.2015, http://www.finlex.fi.

[52] PEETERS, R., HERMANS, J., JA MENNINK, B. Speedup for European epassport authentication. Julkaisusarjassa *International Conference of theBiometrics Special Interest Group (BIOSIG)* (2014), IEEE, pp. 1–6.

[53] PELTOMÄKI, J., JA NORPPA, K. *Rikos meni verkkoon*. Talentum, 2015.

[54] POLIISI. Suomen passien ominaisuudet. URL `https://www.poliisi.fi/passi/suomen_passien_ominaisuudet`, viitattu 12.11.2015.

[55] RÄISÄNEN, A., JA LEHTO, A. *Radiotekniikan perusteet*. Otatieto, Helsinki, 2003.

[56] REBNE, D. S. Biometrics and e-identity (e-passport) in the European union: overcoming POC-cultural diversity for common cause.

[57] REGULATION (EC). No 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States. *OJ L 142* (6.6.2009), 1–4.

[58] SALMINEN, M. *Tietosuoja sähköisessä liiketoiminnassa*. Talentum, 2009.

[59] SANA, A., GUPTA, P., JA PURKAIT, R. Ear biometrics: A new approach. Kirjassa *Advances in Pattern Recognition*. World Scientific, 2007, pp. 46–50.

[60] SCHENGENIN RAJASÄÄNNÖSTÖ. *EUR-Lex*. URL `http://eur-lex.europa.eu`, viitattu 09.06.2016.

[61] SECUNET. The Acknowledged Standard Solution for the Readout of Electronic ID Documents. URL `https://grtplatinum.secunet.com/fileadmin/user_upload/GRT_Microsite/PDF/sn_GRT_Platinum_Edition_FS_GB.pdf`, viitattu 04.06.2016.

[62] SEPPÄ, H., JA UUSIKYLÄ, M. *Vallankumouksellinen RFID. Etätunnistusteknologian kehitys meillä ja maailmalla*. Tekes, Helsinki, 2009.

[63] SUOMEN PERUSTUSLAKI 731/1999. *Valtion säädöstietopankki Finlex*. Viitattu 01.12.2015, http://www.finlex.fi.

[64] SUOMEN STANDARDISOIMISLIITTO SFS. *Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät.Vaatimukset*. 2006.

[65] SUOMEN STANDARDISOIMISLIITTO SFS RY. *SFS-Käsikirja 301-1.RFID. Osa 1: Opas. Johdatus tekniikkaan*. 2010.

[66] SUOMEN STANDARDISOIMISLIITTO SFS RY. *SFS-Käsikirja 301-2.RFID. Osa 2: Standardi I*. 2011.

[67] SUOMEN STANDARDISOIMISLIITTO SFS RY. *SFS-Käsikirja 301-3.RFID. Osa 3: Standardi II*. 2011.

[68] SWAMINATHA, T. M., JA ELDEN, C. R. *Wireless security and privacy: best practices and design techniques*. Addison-Wesley Longman Publishing Co., Inc., 2002.

[69] TIETOSUOJAVALTUUTETUN TOIMISTO. Biometrinen tunnistus, mikä se on? URL http://tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfqPiEON/Biometrinen_tunnistus_mika_se_on.pdf, viitattu 01.01.2017.

[70] TIITS, M., KALVET, T., JA MIKKO, K.-L. Social acceptance of epassports. Julkaisusarjassa *International Conference of the Biometrics Special Interest Group (BIOSIG)* (2014), IEEE, pp. 1–6.

[71] U.S PASSPORTS & INTERNATIONAL TRAVEL. Passports Statistcs. URL https://travel.state.gov/content/passports/en/passports/statistics.html, viitattu 09.06.2016.

[72] VALTIONEUVOSTON ASETUS PASSEISTA ANNETUN VALTIONEUVOSTON ASETUKSEN 1 JA 2 §:N MUUTTAMISESTA 362/2015. *Valtion säädöstietopankki Finlex*. Viitattu 19.11.2016, http://www.finlex.fi.

[73] VALTIOVARAINMINISTERIÖ. Valtionhallinnon tietoturvasanasto VAHTI 8/2008. URL http://www.vahtiohje.fi, viitattu 16.11.2015.

[74] VAN DER PLOEG, I. Machine-readable bodies: biometrics, informatization and surveillance. *Identity, security and democracy* (2009), 85–94.

[75] VAUDENAY, S. E-passport threats. *IEEE Security & Privacy 5*, 6 (2007), 61–64.

[76] VIOLINO, B. The History of RFID technology. *RFID journal 1338* (2005), 1–2.

A Ensimmäinen liite

Taulukko A.1: ICAO Doc 9303 -standardit koneluettavista matkustusasiakirjoista. [29]

Osa	Määrittelykuvaus (eng)
1:	*Introduction*
2:	*Specifications for the Security of the Design, Manufacture and Issuance of MRTDs*
3:	*Specifications Common to all MRTDs*
4:	*Specifications for Machine Readable Passports (MRPs) and other TD3 Size MRTDs*
5:	*Specifications for TD1 Size Machine Readable Official Travel Documents (MROTDs)*
6:	*Specifications for TD2 Size Machine Readable Official Travel Documents (MROTDs)*
7:	*Machine Readable Visas*
8:	*reserved for future use*
9:	*Deployment of Biometric Identification and Electronic Storage of Data in eMRTDs*
10:	*Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)*
11:	*Security Mechanisms for MRTDs*
12:	*Public Key Infrastructure for MRTDs*

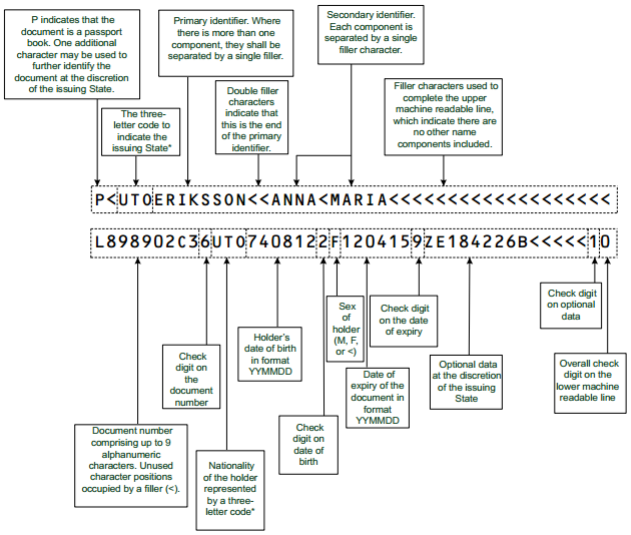
B Toinen liite

Taulukko B.1: ICAO Doc 9303 -standardit koneluettavista matkustusasiakirjoista (suom). [29]

Osa	Määrittelykuvaus
1:	*Johdanto*
2:	*Määrittelyt turvallisuustekijöistä suunnittelu ja valmistusvaiheessa*
3:	*Matkustusasiakirjojen yhteisiä määrityksiä*
4:	*Määrittelyt koneluettaviin passeihin ja muihin matkustusasiakirjoihin*
5:	*Määrittelyt matkustusasiakirjoihin (TD 1) (henkilökortti)*
6:	*Määrittelyt koneluettaviin matkustusasiakirjoihin (TD 2)*
7:	*Määrittelyt koneluettaviin viisumeihin*
8:	*Varaus tulevaan käyttöön*
9:	*Biometristen tunnisteiden jakelu ja tallennus elektronisissa koneluettavissa matkustusasiakirjoissa*
10:	*Sirun looginen tietorakenne ja tallennuspaikka biometriikalle ja muulle yhteydettömälle sirutiedolle*
11:	*Matkustusasiakirjan tietoturvamekanismit*
12:	*PKI matkustusasiakirjoille*

Määrittelydokumentit ovat vuoden 2015 seitsemännen painoksen kuvauksia.

C Kolmas liite



Kuva C.1: Koneluettavan MRZ-rivin rakenne e-passissa ICAO Doc 9303 -standardissa [29].

C.1 MRZ-rivin esimerkki pitkästä nimestä

ICAO Doc 9303 -standardi [29] havainnollistaa todella pitkän nimen tiivistämistä esimerkillä seuraavasti. Jos passinhaltijan nimi on Dingo Potoroo Bennelong Wooloomooloo Warrandyte Warnambool, esitetään nimi passin tietosivulla muodossa: BENNELONG WOOLOOMOOLOO WARRANDYTE WARNAMBOOL, DINGO POTOROO. Koneluettavassa rivissä pitkä nimi voidaan tiivistää ensisijaisen tunnisteen osalta kolmella vaihtoehtoisella tavalla optisesti luettavalle MRZ-riville:
vaihtoehto a: V<UTOBENNELONG<WOOLOOMOOLOO<WARRANDYTE<W«DI
tai
vaihtoehto b: V<UTOBENNELONG<WOOLOOM<WARRAND<WARNAM«DINGO
tai
vaihtoehto c: V<UTOBENNEL<WOOLOO<WARRAN<WARNAM«DINGO<POTO.

D Neljäs liite

Kuva D.1: Malli Suomen uudesta e-passista (voimaan 1.1.2017). Lähde Poliisi.