**Eveliina Jussila**

# RFID-implantit ja tietosuoja

Tietotekniikan kandidaatintutkielma

24. toukokuuta 2021

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

**Tekijä:** Eveliina Jussila

**Yhteystiedot:** jussiiet@jyu.fi

**Ohjaaja:** Timo Tiihonen

**Työn nimi:** RFID-implantit ja tietosuoja

**Title in English:** RFID implants and data protection

**Työ:** Kandidaatintutkielma

**Opintosuunta:** Kaikki opintosuunnat

**Sivumäärä:** 21+0

**Tiivistelmä:** RFID-mikrosiruimplantit kehittyvät jatkuvasti. Jo monella tuhannella ihmisillä on siru kädessään. Näillä implanteilla voitaisiin seurata terveystietoja, maksaa kaupassa ja tunnistautua työpaikalla. Ongelmana ovat kuitenkin RFID-implanttien aiheuttamat yksityisyysongelmat. Onko oikein, että kehossa on laite, jota ei voi kytkeä pois päältä? Toisena ongelmana on myös mahdolliset kyberhyökkäykset, joilla voidaan saada käyttöön henkilön yksityistietoja. RFID-implantit pitää suunnitella eettisesti ja turvallisesti, ja niiden kehitystä pitää valvoa valmistajien ja järjestöjen sekä viranomaisten toimesta.

**Avainsanat:** RFID, mikrosiruimplantti, IEEE, EGE, yksityisyys

**Abstract:** The advancement of RFID microchip implants is on a constant rise. A few thousand people already have a chip in their hand. One could follow one's health information, pay at a store and identify at a workplace with a microchip. A problem that arises from RFID implants is the privacy issues they cause. Is it right that there's a device in one's body that can't be turned off? Another problems are the possible cyber attacks that could gain access to a person's private information. RFID implants need to be designed ethically and securely, and their development needs to be monitored by the manufacturers and organizations aswell as the authorithies.

**Keywords:** RFID, microchip implant, IEEE, EGE, privacy

# Sisällys

# 1 Johdanto

Mikrosiruimplanttien käyttö on lisääntynyt nopeasti vuoden 2010 jälkeen. Jo 2000 ihmisellä oli VeriChip-siru vuonna 2013 (Michael ja Michael 2013) ja sen jälkeen luku on vain kasvanut ja kehittäminen laajentunut. VeriChipin lopettamisen jälkeen on tullut uusia RFID-implanttien valmistajia, kuten esimerkiksi ruotsalainen Biohax. RFID-implanttien myyntiin tulemisen aika voi olla jo lähellä, mutta mahdollisten uhkien takia näin ei ole tapahtunut vielä. Uhkia ovat esimerkiksi tietosuojaongelmat ja implanttien eettisyys. RFID-implanttien ongelmia yritetään selvittää ja myöskin pohtia esimerkiksi sitä, rikkovatko ne ihmiskehon yksityisyyttä.

Mikrosiruimplanttien eettisistä ongelmista on kirjoitettu runsaasti, mutta ratkaisuja niihin ei ole pohdittu yhtä paljon. Tämän tutkielman tarkoituksena on tarkastella RFID-mikrosiruimplanttien keräämiin tietoihin liittyviä uhkia ja pohtia ratkaisuja niihin. Tehtävänä on käydä läpi mitä uhille voidaan jo tehdä ja mihin ongelmiin on vaikeampaa löytää ratkaisuja tällä hetkellä. Tavoitteena on nähdä, mitä kaikkea on vielä tehtävä ennen kuin RFID-implantit voitaisiin saada käyttöön.

Tutkielmassa käytetään RFID-implantteihin liittyviä lähteitä, jotka on julkaistu vuoden 2010 jälkeen, jotta tiedot ovat mahdollisimman ajankohtaisia. Teknologia on kehittynyt paljon viimeisen vuosikymmenen ajan, joten tässä tutkielmassa käytetään tuoreita lähteitä. Aiemmissa lähteissä olevia asioita on jo saatu ratkaistua.

RFID-implanttien eettisyyden turvaaminen on tärkeää ennen niiden myyntiintuloa. Käyttäjien tulee kokea olonsa turvalliseksi implantin ottaessaan. Tarvitaan siis eri järjestöjä ja viranomaisia, jotka pitävät huolen, että näiden implanttien käyttö on turvallista ja eettistä. Tässä tutkielmassa mainitaan kaksi esimerkkiä tällaisista järjestöistä, jotka sopivat hyvin RFID-implanttien eettisyyden takaamiseen. Järjestöjen ja viranomaisten lisäksi mainitaan myös käyttäjien vastuu RFID-implanttien käytössä, ja miten he voivat itse vaikuttaa heistä kerättävään dataan.

Ensimmäisessä luvussa käydään läpi RFID-implanttien toimintaa ja käyttöä nykypäivänä. Tämän lisäksi katsotaan myös mikrosirujen tulevaisuuden mahdollisuuksia. Toisessa luvus-

sa tarkastellaan sirujen keräämien tietojen uhkia, joiden takia siruja ei ole vielä ihmisillä yleisessä käytössä. Kolmannessa luvussa pohditaan ratkaisuja toisessa kappaleessa mainittuihin uhkiin. Todetaan, mitä mahdollisia tapoja meillä on jo selvittää mikrosiruimplanttien eettisiä ongelmia, ja mihin ongelmiin meidän pitäisi panostaa enemmän.

# 2 Implantit ja RFID-tunnistaminen

Tässä luvussa käydään ensiksi läpi RFIDn määritelmä ja, miten RFID-implantteja käytetään nykypäivänä. Seuraavassa kappaleessa katsotaan, mitä eroja passiivisilla ja aktiivisilla RFID-implanteilla on. Lopuksi tarkastellaan, miten RFID-implantteja voitaisiin hyödyntää tulevaisuudessa.

RFID eli radiotajuuden etätunnistus on jo käytössä monissa laitteissa. RFID-transponderi (signaalilähetin) sisältää yksilöllisen, 16 numeroisen, tunnisteen, joka luetaan, kun tämä laite tulee lukijayksikön kantama-alueelle. Kun lukija lukee RFID-sirun, siru menee päälle ja palauttaa tunnisteensa lukijalaitteelle. Tätä ominaisuutta käyttävät esimerkiksi pankkikorttien etälukijat. RFID-implantin järjestelmään kuuluu itse implantti, RFID-lukijalaite ja back-end serveri, joka sisältää tietokannan. Lukijalaite lähettää kyselyjä RFID-tunnisteelle, joiden vastaukset se lähettää tietokannalle. Tietoja säilytetään tietokannassa myöhempää käyttöä varten. (Moosavi ym., 2014b)

RFID-implantteja käytetään nykypäivänä esimerkiksi eläinten tunnistamisessa. RFID-implanttien käyttö ihmisissä ei ole myöskään uutta. Ensimmäinen lääketieteellinen RFID-implantti annettiin vuonna 2004 (Rotter ym., 2012b). Kyseessä oli VeriChip-siru. Implantti oli passiivinen ja sen kantamaetäisyys oli 10-15cm. Rotter ym. (2012b) kirjoittavat, että VeriChip-siru tehtiin VeriMedin käyttöön, ja sen avulla lääkärit pääsivät käsiksi potilaidensa terveystietoihin. Rotter ym. (2012b) kertovat, että ensimmäinen hengenpelastus RFID-implantilla tehtiin vuonna 2006. Potilas, jolla oli VeriChip-siru kädessään, oli joutunut autokolariin. Lääkärit pääsivät käsiksi VeriMedissä oleviin potilastietoihin tunnistenumeron avulla ja pystyivät tarjoamaan potilaalle tarvittavaa hoitoa, jota tarvittiin hänen henkensä säilyttämiseksi.

Ruotsissa Biohax International -niminen yritys on alkanut myymään siruja Ruotsiin, ja tuhansilta ruotsalaisilta löytyy jo sellainen kädestään (Jefferson 2017). Junassa konduktöörit lukevatkin matkalipun sijaan heidän kätensä. Lisäksi heidän ei tarvitse muistaa salasanojaan, koska siru hoitaa sen heidän puolestaan. Siruilla pyritään helpottamaan ihmisten elämää. Mikrosirujen kehitys ja käyttömahdollisuudet ovat siis suuressa kasvussa jatkuvasti.

## 2.1 Passiiviset ja aktiiviset implantit

RFID-implanttia kehittäessä tulee pohtia, mitä toimintoja implantille haluaa. Haluaako, että sirun kantamaetäisyys on suurempi ja, että se voi sisältää paljon muistia vai riittääkö, että se toimii vain lukijalaitteen kantamaetäisyydellä. Tästä valinnasta riippuu, tuleeko implantista aktiivinen vai passiivinen.

Mikrosiruimplantin tulee olla alle kaksi prosenttia henkilön painosta (Bazaka ja Jacob 2013). Bazaka kirjoittaa, että sirun ollessa aktiivinen, se tulee ladata tietyin väliajoin. Akku lisää huomattavasti sirun painoa, minkä takia sen suunnittelu voi olla hankalampaa. Sirusta ei voida tehdä liian isoa, jotta se voidaan asettaa ihon alle. Lisäksi, jos siru pitää poistaa kehosta esimerkiksi lataamisen ajaksi, tulee tämä tehdä kirurgisesti, mikä voi aiheuttaa paljon kustannuksia. Passiivisen sirun hyvä puoli on sen pienempi koko, koska se ei sisällä akkua.

On kuitenkin löydetty tapoja, joilla implantit voidaan ladata langattomasti. Esimerkiksi kuulolaitteita voidaan ladata radioaalloilla, ultraäänellä tai magneettikentällä (Bazaka ja Jacob 2013). Passiivisesti toimiva siru ladattaisiin vain tarvittavaksi ajaksi transponderin avulla, kun siru lähestyy lukijalaitetta (Aubert 2011). Passiivinen siru olisi siis paljon helpompi suunnitella. Pienen kokonsa takia implantin RFID siru ei yltäisi sateelliitteihin asti, minkä takia sirulla ei voitaisi seurata käyttäjän reaaliaikaista sijaintia (Aubert 2011).

Moosavi ym., 2014b kirjoittavat, että RFID-implantti asetetaan kehoon kirurgisesti, ja passiivista implanttia voidaan pitää jopa kymmenen vuotta, koska siinä ei ole mitään liikkuvia osia. Passiivisessa sirussa on siis myös hyvää sen käyttöikä. Tähän asti valmistetut RFID-implantit, esimerkiksi VeriChip ja Biohax, ovat olleet molemmat passiivisia, ja niin tulee olemaan luultavasti tulevaisuudessakin passiivsen sirun yksinkertaisuuden takia. Jos aktiiviset sirut olisivat pienempiä, ja jos niiden lataaminen olisi helmpompaa, niin niillä voisi olla enemmän käyttömahdollisuuksia kuin passiivisilla siruilla. Seuraavaksi käydään läpi, mitä kaikkea RFID-implanteilla voitaisiin tehdä tulevaisuudessa.

## 2.2 RFID-implanttien tulevaisuuden käyttökohteet

Vaikka mikrosiruimplantteja on käytetty jo ihmisissä, niiden ei-lääketieteellinen käyttö on kuitenkin vähäistä yksityisyysongelmien takia. Ihon alle laitettavat RFID-mikrosirut tulisivat keräämään tietoja ihmisten terveydestä ja/tai sijainnista sekä voisivat toimia myös etätunnistuslaitteena kuten esimerkiksi pankkikorttina (Michael ja Michael 2013).

Niillä pystyttäisiin myös paikantamaan sortuneiden rakennusten alle jääneitä ihmisiä (Michael ja Michael 2013). Ihmisiä ei voisi seurata reaaliajassa, kuten aikasemmassa luvussa mainittiin, mutta on toinen tapa. Toinen vaihtoehto on etsiä heitä RFID-lukijalaitteella. Jos lukija tulee RFID-sirun kantamaetäisyydelle, tiedetään, että ihminen on lähettyvillä. Toimintaa voisi verrata metallinpaljastimeen. Näin etsintää voitaisiin nopeuttaa, koska ei tarvitsisi tutkia alueita, joissa ihmisiä ei ole.

RFID-implantteja voitaisiin hyödyntää entistä enemmän lääketieteessä. Diabeteksen hoidossa käytettävä implantti alkaa hälyyttämään, jos henkilön glukoosiarvot nousee liian korkeaksi (Aubert 2011). Aubert kirjoittaa, että tulevaisuudessa RFID-implantti voisi käyttää tätä samaa toimintaa. Se voisi havaita minkä tahansa sairauden ja laite antaisi käyttäjälleen varoituksen. Jos tälläinen keksitään, käyttäjän hoito voitaisiin aloittaa heti ja paranemismahdollisuudet olisivat huomattavasti suuremmat. Lääkäreiden työ helpottuisi ja kansanterveys paranisi. Lai, Chan ja Singh 2015 tekemän tutkimuksen mukaan RFID-mikrosirut pystyvät myös tappamaan tai häiritsemään syöpäsolujen kasvua kasvaimiin istutettuina. Siruista voisi tulla siis myös uusi syövän hoitomenetelmä.

Lisäksi tunnistautumista voitaisiin parantaa RFID-implanteilla. Käyttäjien ei tarvitsisi muistaa salasanojaan, sillä implantin sisältämä siru toimisi tunnistautumisvälineenä. Se olisi myös paljon luotettavampi kuin sormenjälki- tai kasvojentunnistus, koska tunnistenumeroa ei voi olla kenelläkään muulla. Lisäksi esimerkiksi kirjasto- ja kuntosalikortit voitaisiin myös yhdistää implantin tunnisteeseen. Näin jokaisen ei tarvitsisi aina kantaa kaikkia kortteja mukanaan, vaan ne olisi kaikki yhdistettynä samaan paikkaan.

RFID-implanttien tulevaisuuden mahdollisuuksien lisäksi niillä on myös paljon uhkia, minkä takia implantit eivät ole vielä kaikkien käytössä. Seuraavassa luvussa perehdytään näihin ongelmiin tarkemmin.

# 3 RFID-implanttien tietosuojauhat

RFID-implanteista kirjoitetaan jatkuvasti ja pohditaan niiden eettistä hyväksyttävyyttä. Rotter, Daskala ja Compañó, 2012a kirjoittavat, että Googlen julkaisemassa tutkimuksessa vuonna 2011 RFID:stä oli kirjoitettu 55 miljoonaa artikkelia, joista yli 25 prosenttia liittyi yksityisyyteen. Pelätään, että omat yksityistiedot näkyvät esimerkiksi jollekin suuryritykselle, eikä yksityisyys ole enää omassa hallinnassa.

Implanttien terveyshaitoista on esiintyy myös keskustelua. Tämä tutkielma keskittyy kuitenkin enemmän implanttien keräämien tietojen uhkiin kuin fyysisiin uhkiin. Ruotsalaisen RFID-implanttien valmistajan Biohaxin toimitusjohtaja kuitenkin väittää, että implantin laittaminen on turvallisempaa kuin lävistäminen ja yhtä vaarallista kuin verikokeen ottaminen sairaalassa (Jefferson 2017).

Tässä luvussa käydään läpi RFID-implanttien yksityisyysuhkia. Todetaan, mitä uhkia RFID-tunnisteella, tietosuojilla ja datan keräämisellä on. Tunniste voidaan yhdistää sen käyttäjään sekä hänen ostoksiinsa. Käyttäjää pystytään myös seuraamaan lukijalaitteiden avulla, kun hänen tunniste on saatu selville. Tunnisteen lisäksi ongelmana on tietokannan hallinta. Kuka pääsee käyttäjien tietoihin käsiksi? Siru tulisi olemaan henkilön kehossa jopa loppuelämän ajan. Tämän takia sen käyttäjällä tulee olla turvallinen olo sitä käyttäessä, minkä takia seuraavat uhat on ratkaistava. Seuraavassa kappaleessa selvitetään, mitä yksityisyysuhkia RFID-tunnisteella on.

## 3.1 RFID-tunnisteen yksityisyysongelmat

Yksityisyysongelmiin pyritään etsimään ratkaisuja, jotta RFID-implantit saataisiin kuluttajien käyttöön. Keho on ihmiselle yksityinen asia, joten onko oikein, että kehossamme on laite, joka seuraa sen toimintaa jatkuvasti?

Sijainnin seuraaminen on myös suuri uhka henkilön yksityisyydelle. Rotter, Daskala ja Compañó, 2012a kirjoittavat RFID-implanttien yhtenä ongelmana olevan "sijainnin yksityisyys". Siinä henkilön sijaintia pystytään seuraamaan lukijalaitteiden avulla. Lukijalaitteita sijoite-

taan paikkoihin, joihin epäillään henkilön menevän. Näin henkilön liikkeitä pystytään seuraamaan. Rotter ym. (2012a) mainitsevat esimerkkinä yrityksen, joka voisi seurata työntekijöidensä sijaintia ja näin ollen heidän tuottavuuttansa. Yrityksen ei tarvitsisi edes piilottaa lukijoita, koska työpaikoilla ne toimivat yleensä turvavalvotetuilla alueilla. Tämä rikkoo työntekijöiden yksityisyyttä.

Toisena ongelmana Rotter ym. (2012a) mainitsevat RFID-tunnisteen käyttämisen pankkikorttina. On mahdollista, että ostaja voidaan tunnistaa ja tietää mitä hän osti. Tuotteiden RFID-tunnuksesta voidaan saada selville, mikä tuote on kyseessä. Näillä tiedoilla voidaan selvittää yksityisiä tietoja henkilöstä esimerkiksi sairaudet tai ostomieltymykset ja ostokäyttäytyminen.

Lisäksi Rotter ym. (2012a) mainitsevat ongelmana, että käyttäjä yhdistyy tunnisteeseen, mutta ei toisin päin. Eli, jos käyttäjä katkaisee yhdistämisen (heittää tuotteen pois, menettää/myy sen yms.), tietokantoihin jää silti tieto tästä yhdistämisestä. Jos tuotetta käytetään myöhemmin johonkin pahantahtoiseen toimintaa, sen alkuperäinen omistaja voi joutua syytteeseen.

Edellä mainituissa uhissa on käytetty hyväksi RFID-tunnistetta ja sen yhdistämistä yksityiseen henkilöön. Seuraavassa kappaleessa pohditaan, ketkä pääsevät käyttäjien tietoihin käsiksi ja miten tätä voidaan valvoa.

## 3.2 RFID-implanttien tietokantojen hallinta

Kuka pääsee näkemään kaikki henkilön tiedot? Monia voi pelottaa ajatus, että yritys saa tietää kaiken heistä sirujen avulla. Jos suuri yritys myisi siruja esimerkiksi pankkikorttien tilalle, voisi yrityksen saamia henkilötietoja rajoittaa helpommin kuin, jos hallitus tekisi tämän. Jos hallitus määräisi kaikille mikrosirut, kukaan ei voisi seurata, että noudattaako hallitus eettisiä normeja. Hallitusta valvoo vain hallitus itse (Billette 2019). Sirujen sisältämien tietojen rajoittamiseen tarvitaan siis joku, joka valvoo niiden eettisyyttä ja turvallisuutta. Lisäksi tuottajilla ja viranomaisilla on vastuu eettisyyden takaamisessa. Näistä tullaan kertomaan myöhemmin lisää. Seuraavassa kappaleessa käydään läpi kyberhyökkäyksiä, joilla hakkeri voi saada tarkempia tietoja sirun käyttäjästä.

## 3.3 Kyberhyökkäykset

Mikrosiruista tulisi tehdä mahdollisimman turvallinen kyberhyökkäyksiä vastaan. Siru itsessään ei sisällä käyttäjän tietoja, mutta sen sijaan tiedot löytyvät yrityksen tietokannasta. Jos tietokanta hakkeroidaan, kaikkiin henkilön yksityisiin tietoihin voidaan päästä käsiksi (Billette 2019).

Toinen Billetten (2019) mainitsema uhka on valelukijat. Vale-RFID-lukija lukee implantin tunnisteen ja näin hakkeri voi käyttää omistajan tunnistetta itse. Tämän välityshyökkäyksen on testattu olevan mahdollista, eikä siihen ole vielä keksitty ratkaisua. Rotter ym. (2012a) myös kirjoittavat, että RFIDn yksityisyysuhat liittyvät pääosin siihen, että RFID vastaa mihin tahansa lukijaan. Rotter ym. (2012a) mainitsevat myös, että implantin muisti ei sisällä tietoa lukijalaitteista. Mahdollisia valelukijoita ei voida siis havaita jälkikäteen. RFID-implantteja ei voida antaa yleiseen käyttöön, ennen kuin tälläiset hyökkäykset saadaan estettyä. Implanttien keräämiä tietoja tulee piilottaa paremmin, jotta mahdollisessa kyberhyökkäyksessä tietokantaan pääsy ei antaisi kaikkia henkilökohtaisia tietoja. Seuraavassa luvussa käydään läpi, miten voidaan pitää huoli, että datan kerääminen ja RFID-implantin asettaminen on eettistä.

# 4 Eettinen sääntely

Mikrosiruja valmistavien yritysten ei pidä olla ainoita, ketkä pitävät huolen sirujen eettisyydestä. Käyttäjän pitää pystyä luottamaan omaan turvallisuuteensa ja kokea, ettei hänen terveydelleen koidu mitään haittaa. Tämän takia yksityisyysongelmien ratkaisuihin tarvitaan lisäksi muita osapuolia, jotka voivat pitää huolen, että sirun toiminta on eettisesti hyväksyttävää. Tälläisiä eettisiä sääntöjä ja normeja seuraavat esimerkiksi IEEEn ja EGEn jäsenet. Seuraavaksi käydään läpi nämä kaksi järjestöä, jotta saadaan kuva, mitä asioita tulee ottaa huomioon eettisyyden valvomisessa.

## 4.1 Teknologian tuottajia yhdistävät järjestöt

Yritysten valmistaessa RFID-implantteja tarvitaan sääntöjä, joita noudattaa, jotta implanteista saadaan eettisesti hyväksyttäviä. Tuotteen kehittämisen tulee seurata näitä sääntöjä, jotta tuotteen luotettavuus ja turvallisuus paranevat.

Yksi esimerkki tälläisestä järjestöstä on IEEE. IEEE, eli Institute of Electrical and Electronics Engineering, on maailman suurin tekniikan ammattijärjestö tekniikan edistämiseksi. Sen standardit ovat julkaistuja asiakirjoja, joissa määritetään spesifikaatiot ja menettelyt, jotka on suunniteltu maksimoimaan tuotteen/palvelun luotettavuutta. Niillä pyritään myös parantamaan tuotteen turvallisuutta ja tukemaan kansanterveyttä (IEEE). Billette 2019 mukaan IEEEn standardeja ja eettisiä sääntöjä voidaan käyttää hyväksi RFID-implanttien yksityisyysongelmien ratkaisemiseen.

IEEEn eettisiä sääntöjä on kymmenen kappaletta, joita jokaisen järjestön jäsenen tulee noudattaa. Eettiset säännöt ovat samanlaisia kuin IEEEn standardit. Niillä pyritään parantamaan luotettavuutta ja turvallisuutta sekä lisäksi pitämään huoli, että eettisiä normeja noudatetaan (IEEE 2020). Säännöt jakautuvat kolmeen eri osaan. Ensimmäinen osa keskittyy rehellisten, vastuullisten ja eettisten käyttäytymisen normien noudattamiseen ammatillisissa tilanteissa. Sääntöinä ovat esimerkiksi terveyden ja yksityisyyden ylläpito sekä kritiikin hyväksyminen. Toinen osa keskittyy enemmän sosiaalisiin tilanteisiin. Kaikkia tulee kunnioittaa ja kohdella reilusti. Ketään ei saa syrjiä rodun, uskonnon tai muun vastaavan takia. Kolmanteen osaan

kuuluu vain yksi sääntö, sääntöjen noudattamisen valvominen. Kollegoiden pitää tukea toisiaan ja pitää huoli, ettei sääntöjä rikota. Näiden sääntöjen noudattamisella voidaan saada RFID-implanttien kehittämisestä eettistä ja turvallista.

## 4.2 Käyttäjien oikeuksia ajavat järjestöt

Lisäksi tarvitaan järjestöjä, jotka pitävät huolen RFID-implanttien käyttäjien oikeuksista. He tarkastavat, että datan kerääminen tapahtuu eettisesti ja, että jokaisella on mahdollisuus vaikuttaa omaan kehoonsa.

Esimerkki tällaisesta järjestöstä on EGE. EGE, eli European Group on Ethics in Science and New Technologies, on Euroopan komission puheenjohtajan nimittämä riippumaton monialainen elin, joka neuvoo kaikissa käytännöissä, joissa eettiset, yhteiskunnalliset ja perusoikeuskysymykset risteävät tieteen ja uuden tekniikan kehityksessä (EGE). EGEn tavoite on siis samanlainen kuin IEEEn. Yksi heidän mielipiteistään on, että henkilöllä tulee olla mahdollisuus vaikuttaa mitä dataa hänestä kerätään. (EGE 2012) He pitävät tätä haasteellisena ongelmana, koska joskus henkilöiden dataa säilytetään ilman heidän suostumustaan. Henkilöillä tulisi olla mahdollisuus poistaa heihin liittyvää tietoa, jos laki ei estä sitä. Nykyaikana ongelmana on esimerkiksi kuvien leviäminen netissä, sillä kuvia on vaikea saada poistettua kaikkialta. EGE kirjoittaa, että näiden ongelmien takia kyseistä datan muokkaamisen oikeutta tulisi täsmentää, ja tarvittaessa, vahvistaa. Tätä voisi myös hyödyntää RFID-implanteissa. Jos käyttäjät eivät halua, että heistä kerätään jotain tietoa, he voivat estää sen.

## 4.3 Viranomaisten vastuu

Järjestöjen lisäksi suuri vastuu on viranomaisilla. He päättävät laista, jotka vaikuttavat RFID-implanttien antamiseen ja käyttämiseen. Implantit laitetaan kirurgisesti ja valtio vaikuttaa siihen esimerkiksi siten, onko niiden asettaminen ilmaista. Ihmiset myös luottavat viranomaisiin, joten heidän tulee olla varmoja, että mikrosiruimplantin laittaminen on turvallista.

Monahan ja Fisher 2010 mainitsevat yhtenä RFID-implanttien ongelmana olevan se, että siru pakotetaan ottamaan. He kirjoittavat, että pelätään, että ihmisille tullaan laittamaan mikro-

siruimplantti vasten tahtoansa. Vanhemmat saattavat päättää mikrosiruimplantista lastensa puolesta. Monahan ym. (2010) sanovat, että viranomaisten tulee tehdä laki pakottamista vastaan, jotta siitä ei synny ongelmaa tulevaisuudessa. Seuraavassa luvussa katsotaan tarkemmin, mitä muita tapoja on torjua mikrosiruista syntyviä ongelmia.

# 5 RFID-implanttien uhkien torjuminen

Tässä luvussa käydään läpi, mitä ratkaisuja RFID-implanttien uhkiin on jo tehtävänä. Implanttien toimintojen mahdollisuudet voivat olla jo paljon suuremmat niiden mahdollisiin uhkiin verrattuna. Kuten Aubert 2011 mainitsi, niin implanteilla voitaisiin saada selville, jos käyttäjä on sairastunut. Tämä parantaisi kansanterveyttä huomattavasti, mikä voisi olla tärkeämpää kuin mahdolliset uhat. RFID-implanttien tietosuojaongelmat täytyy kuitenkin saada ratkaistua ennen niiden tulemista myyntiin. RFID-implantit tulee olla turvallisia ja vaikeasti hakkeroitavissa. Lisäksi käyttäjilläkin tulee olla mahdollisuus vaikuttaa omaan turvallisuuteensa. Heidän tulee voida päättää, mitä dataa heistä kerätään, ja heidän tulee tietää, miten he voivat pitää oman yksityisyytensä turvassa.

## 5.1 RFID-implanttien uhkien torjuminen kehitysvaiheessa

RFID-implanttien kehitysvaiheessa voidaan jo suunnitella mitä ominaisuuksia siihen tulee. Implantin toimintojen päättäminen määrä, mitä mahdollisia uhkia siitä voi syntyä.

Jotkut voivat pitää uhkana heidän sijaintitietojensa seuraamista. Henkilön reaaliaikaista jäljitystä ei kuitenkaan onnistuttaisi tehdä vielä tällä hetkellä. RFID-implantteja ei voi seurata, sillä satelliitit ovat liian kaukana toimiakseen passiivisen RFIDn kanssa (Aubert 2011). Esimerkiksi Biohaxin siruissa ei ole GPS toimintaa niiden pienen kokonsa vuoksi. Jos siruista tulee passiivisia, kuten Biohaxilla, ne toimisivat vain henkilön tunnistamisessa. Siruissa olisi uniikki koodi, jota voisi käyttää tunnistautumisessa ja pankkikorttina.

Lisäksi sirua ei tarvitsisi koskaan ladata,jos se olisi passiivinen, vaan se voisi pysyä aina ihon alla ja saisi virtaa tarvittavaksi ajaksi lukijalaitteen avulla. Näin käyttäjien ei tarvitse poistaa sirua kirurgisesti aina lataamisen ajaksi ja vältytään kustannuksilta. Tulevaisuudessa voidaan kuitenkin keksiä helpompia lataustapoja aktiivisille siruille, kuten esimerkiksi radioaallot tai ultraääni.

## 5.2 Käyttäjien oma vastuu

Käyttäjilläkin on vaikutus heidän omaan turvallisuuteensa. Vaikka tietosuojauhat saataisiin ratkaistua, käyttäjien pitää itsekin pitää tietonsa turvassa muilta.

Mikrosirun asennusvaiheessa käyttäjät voisivat itse valita, mitä tietoja heistä kerätään. Jotkut eivät ehkä halua sijaintitietojensa näkyvän ollenkaan. Jotkut voivat haluta, että heidän siru toimii vain maksuvälineenä, eikä sairauksien seuraajana. Näin henkilöt ovat itse vastuussa omista tiedoistaan ja voivat päättää mitä dataa heistä kerätään.

Rotter ym. (2012a) kirjoittavat, että RFID-implanttien käyttäjien tulee tietää mahdolliset tietouhat. Näin saadaan käyttäjille myös vastuu pitää huoli omasta turvallisuudestaan. Vaikka monet tietävät, että salasanan tulee olla vahva, jotta hakkereilla on vaikeampaa selvittää sitä, he silti kirjoittavat salasanan muistilapulle ja liimaavat sen tietokoneen näyttöönsä. Monet suhtautuvat tietosuojauhkiin välinpitämättömästi ja tästä aiheutuvat ongelmat eivät ole enää valmistajien käsissä. Käyttäjien tulee siis pitää huolta omasta turvallisuudestaan. Jos käyttäjät tietävät, että mahdollisena uhkana on esimerkiksi heidän sijaintinsa seuraaminen, niin he osaavat varautua siihen ja päättää, että haluavatko he edes ottaa implanttia.

## 5.3 Mahdollisia ratkaisuja RFID-implanttien tietosuojauhkiin

Tietosuojan kehittämisessä on vielä parannettavaa kaikissa palveluissa ja laitteissa, myös RFID-implanteissa. Kuten aikaisemmin mainittiin, näillä implanteilla on paljon uhkia liittyen RFID-tunnisteeseen ja datan keräämiseen. Moosavi ym., 2014a mainitsevat muutaman jo kehitetyn ratkaisun RFID-implanttien tietosuojauhkiin. Ensimmäisenä ja helpoimpana ratkaisuna he mainitsevat Weisin (2004) esittämän hajautusfunktion. Tämä ratkaisisi tunnisteen yksityisyysongelmat, mutta jäljitysongelmat voitaisiin ratkaista toisella algoritmilla. He kirjoittavat, että tämä onnistuisi satunnaisella hajautusfunktiolla. Kuitenkin nämä kaksi eivät ratkaisisi skaalautuvuusongelmaa. Tämä tarkoittaa, että molemmissa algoritmeissa tunnisteen ja lukijan välisen viestinnän onnistuminen edellyttää sitä, että lukijan on tarkistettava kaikki RFID-tunnisteen mahdolliset salaiset avaimet. Suurissa järjestelmissä tämä ei olisi mahdollista, sillä se kuormittaisi tietoverkkoa liikaa.

Moosavi ym. (2014a) mainitsevat lisäksi Ohkubon ym. (2003) esittämän järjestelmän, jossa aina, kun RFID-tunniste luetaan, hajautusfunktio asetetaan tunnisteen numeroon. Sitten käyttämällä toista hajautusfunktiota, tunniste hajautetaan vielä kerran. Vaikka heidän esittämässä järjestelmässä henkilön yksityisyys on turvassa, se tuottaa myös paljon kuormitusta tietokannan serverille. Tässä algoritmissa kaikki mahdolliset hajautusarvot täytyy laskea, kunnes törmäys tapahtuu. Moosavi ym. (2014a) mainitsevat seuraavaksi Henricin ja Müllerin tekemän järjestelmän. Kun lukijalta on saatu pyyntö, tunniste kasvattaa tapahtumanumeroansa yhdellä ja lähettää lukijalle tunnuksensa hajautusarvon, sen nykyisen transaktionumeron hajautusyhdistelmän ja sen ID:n sekä lopuksi $\Delta$ TID :n, joka on viimeisimmän onnistuneen transaktion numeron vähennys olemassa olevasta transaktionumerosta. Tässäkin järjestelmässä suurin heikkous on sen skaalautuvuusongelma. Kun tunnisteiden määrä kasvaa, tallennettujen tunnisteiden määrä kasvaa.

Seuraavaksi Moosavi ym. (2014a) kirjoittavat Tsudikin (2007) esittämästä YA-TRAP:n kommunikaatioprotokollasta. Tässä protokollassa, tunniste, lukija ja tietokanta serveri jakavat yhteisen salaisuuden, joka eroaa muista järjestelmässä saatavilla olevista salaisuuksista. YA-TRAP-protokolla aloitetaan, kun lukija lähettää viimeisimmän aikaleiman tunnisteelle. Sitten tunniste tarkastaa, onko aikaleima uudempi kuin edellinen aikaleima. Jos aikaleima ei ole uudempi, tunniste käyttää vain pseudosattumanumerogeneraattoria tuottakseen k-bittisen satunnaisluvun. Muussa tapauksessa, tunniste rekisteröi viimeisimmän aikaleiman ja laskee sen hajautusarvon käyttämällä salaista avainta. Lopuksi lukija lähettää hajautusarvon palvelimelle todentamista varten. Tsudik huomasi kaksi heikkoutta protokollassaan. Ensiksi, protokolla on heikko palvelunestohyökkäykselle, kun hyökkääjä poistaa tunnisteen käytöstä, joko pysyvästi tai väliaikaisesti tai lähettää väärän aikaleiman vastaanottajalle. Toinen heikkous on toistohyökkäys. Se tapahtuu, kun aikaleimaa käytetään vain todentamistarkoituksessa. Tässä hyökkääjä pystyy lähettämään joitakin odotettujen aikaleimojen sekvenssejä tunnisteeseen ja tallentamaan sen vastaukset. Kun näiden aikaleimojen ajat muuttuvat todellisiksi, tunniste voi vastata kaikkiin lukijan esittämiin pyyntöihin jopa ilman tunnisteen läsnäoloa.

On vaikea keksiä toimivaa tietosuojaprotokollaa, joka ei kuormita tietokanta serveriä liikaa. Tähän ratkaisuna Moosavi ym. (2014a) mainitsevat Molnarin puupohjaisen yksityisen tun-

nistusjärjestelmän. Tässä järjestelmässä jokainen tunniste yksilöidään puun lehdellä. Kun lukija vaatii tunnisteen tunnistamista, menettely alkaa puun juuresta. Tämä järjestelmä on kuitenkin haavoittuvainen datan vuodolle. Se tarkoittaa, että, jos hyökkääjä kaappaa osan järjestelmän tunnisteista, hän voi päästä käsiksi salaisiin avaimiin.

Vielä kaikkiin tietosuojauhkiin ei ole helppoa ratkaisua. Pitää löytää tietosuojaprotokolla, joka ei kuormittaisi tietokanta serveriä, ja jossa ei olisi haavoittuvaisuuksia. Näitä keksittyjä protokollia tulee soveltaa, jotta voidaan löytää hyvä tapa, jolla RFID-implantit voidaan todeta turvallisiksi. Aina tietomurtoja voi sattua, mutta mikrosirun käyttäjällä tulee olla turvallinen olo, että hänen tietonsa ei ole varastettavissa.

# 6 Yhteenveto

RFID-implantit kehittyvät jatkuvasti ja niiden uhat tulevat entistä selkeämmiksi. Näillä implanteilla voitaisiin mahdollisesti parantaa kansanterveyttä ja helpottaa normaalia elämää, mutta niihin liittyy kuitenkin paljon uhkia, jotka täytyy ratkaista. Ensimmäinen tässä tutkielmassa mainittu uhka on RFID-tunnisteen yksityisyysongelmat. Tässä yksilön tunniste voidaan yhdistää hänen ostoksiinsa, ja hänen sijaintiansa voidaan seurata lukijalaitteiden avulla. Tähän ja kyberhyökkäysongelmiin ei ole vielä keksitty ratkaisua, mutta esimerkiksi hajautusfunktioilla voidaan saada tähän sopiva tietosuojaprotokolla. Toinen uhka on datan hallinta, eli kuka pääsee RFID-laitteiden tietoihin käsiksi, ja ketkä ovat vastuussa implanttien eettisyydestä. Implanttien kehittäminen tulee olla yritysten tehtävä ja niiden valvominen esimerkiksi hallituksen tai järjestön, kuten IEEEn, tehtävä. Jokaisella RFID-implantin hankkijalla tulee olla mahdollisuus vaikuttaa sirun keräämiin tietoihin. Näin toteutetaan EGEn mielipide, että henkilön tulee itse pystyä valitsemaan mitä dataa hänestä saadaan. Lisäksi mikrosirua ei voi pakottaa kenellekään, vaan sen tulee olla henkilön oma päätös. Jokaisella tulee olla valta vaikuttaa omaan kehoonsa. Kuten Monahan ja Fisher 2010 mainitsivat, niin tulee tehdä laki, joka estää RFID-implantin laittamisen ilman henkilön suostumusta. Ongelmaksi jää vain, että mitä, jos henkilö voisi pysyä elossa vain, jos hänelle asetetaan RFID-implantti. Tällä hetkellä on keskityttävä sirujen tietosuojauhkiin, jotta niistä voidaan saada turvallisempia. Näiden uhkien ratkaistua, voidaan nopeuttaa RFID-implanttien tulemista jokaisen käyttöön.

# Lähteet


Aubert, Hervé. 2011. “RFID technology for human implant devices”.

Bazaka, Kateryna, ja Mohan V. Jacob. 2013. “Implantable Devices: Issues and Challenges”.

Billette, Robert. 2019. “Human RFID Implants: The Good And Bad”.

EGE. 2012. “Ethics of information and communication technologies”.

———. *European Group on Ethics in Science and New Technologies (EGE).* Saatavilla WWW-muodossa, https://ec.europa.eu/info/research-and-innovation/strategy/support-policy-making/scientific-support-eu-policies/ege_en, viitattu 07.04.2021.

IEEE. 2020. *IEEE Code of Ethics.* Saatavilla WWW-muodossa, https://www-ieee-org.ezproxy.jyu.fi/about/corporate/governance/p7-8.html, viitattu 10.02.2021.

———. *IEEE Standards.* Saatavilla WWW-muodossa, http://standards.ieee.org/, viitattu 08.02.2021.

Jefferson, Graham. 2017. *Are embedded microchips dangerous? Ask the Swedes — and pets.* Saatavilla WWW-muodossa, https://eu.usatoday.com/story/tech/talkingtech/2017/07/25/do-microchip-implants-pose-health-risks-ask-swedes-and-pets/507408001/, viitattu 07.03.2021.

Lai, Henry C., Ho Wing Chan ja Narendra Pal Singh. 2015. “Effects of radiation from a radiofrequency identification (RFID) microchip on human cancer cells”.

Michael, Katina, ja M G. Michael. 2013. “The future prospects of embedded microc-hips in humans as unique identifiers: the risks versus the rewards”.

Monahan, Torin, ja Jill A. Fisher. 2010. “Implanting inequality: Empirical evidence of social and ethical risks of implantable radio-frequency identification (RFID) devices”.

Moosavi, Sanaz Rahimi, Antti Hakkala, Johanna Isoaho, Seppo Virtanen ja Jouni Isoaho. 2014a. “Specification Analysis for Secure RFID Implant Systems”.

Moosavi, Sanaz Rahimi, Ethiopia Nigussie, Seppo Virtanen ja Jouni Isoaho. 2014b. “An Elliptic Curve-based Mutual Authentication Scheme for RFID Implant Systems”.

Rotter, Pawel, Barbara Daskala ja Ramon Compañó. 2012a. *Human ICT Implants: Technical, Legal and Ethical Considerations: Passive Human ICT Implants: Risks and Possible Solutions.* T.M.C. Asser Press.

Rotter, Pawel, Barbara Daskala, Ramon Compañó, Bernhard Anrig ja Claude Fuhrer. 2012b. *Human ICT Implants: Technical, Legal and Ethical Considerations: Potential Application Areas for RFID Implants.* T.M.C. Asser Press.