Matti Heikkilä

RFID- JA NFC-SIRUJEN KÄYTTÖ TUNNISTAUTUMISEN VÄLINEENÄ

Tietojenkäsittelyn koulutusohjelma
2020

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

RFID- JA NFC-SIRUJEN KÄYTTÖ TUNNISTAUTUMISEN VÄLINEENÄ

Heikkilä, Matti
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
maaliskuu 2020
Sivumäärä: 51
Liitteitä:0

Asiasanat: etätunnistus, tietoliikennetekniikka, RFID-teknologia, langaton tekniikka

---

Työssä tutkittiin RFID-teknologiaan perustuvien sirujen käyttöä erilaisissa tunnistautumisen välineissä. Aluksi esiteltiin teknologian historiaa ja taustaa, sitten perinpohjaisesti teknisiä ominaisuuksia. Tämä tehtiin siksi, että lukija ymmärtäisi paremmin myöhemmissä luvuissa esiteltyjä käytännön esimerkkejä. Työssä käytiin läpi eri taajuusalueita ja eri tekniikkaa käyttäviä RFID-siruja ja niiden mahdollisia käyttökohteita. Esimerkkien avulla pyrittiin saamaan lukijalle ymmärrys siitä, että miten arkipäiväistä sirutekniikan käyttö loppujen lopuksi on. Standardointia käsiteltiin yhden alaluvun verran, jotta tietoturvalle merkittävimmät seikat selviävät, ja standardoinnin pääasiallinen syy valkenee lukijalle.

Ajankohtaisimpia tunnistautumisen keinoja, kuten biometrinen passi ja mobiilivarmenne käsiteltiin tarkasti, ja selitettiin niiden toimintaa käytännössä. Tietoturvan ja yksityisyyden merkitys otettiin huomioon jokaisessa käsiteltävässä aiheessa. Myös ekologisuuden edistämistä RFID-tekniikan saralla pohdittiin. Mobiilimaksamiselle on oma osuus, jossa käytiin läpi paljon puhuttanutta lähimaksun turvallisuutta ja oiottiin mahdollisia väärinkäsityksiä NFC-sirujen avulla tehtävistä mobiilimaksuista. Työn loppupuolisko on omistettu tietoturvalle ja tulevaisuuden implementaatioille sekä ihonalaisille siruille. Asioiden Internetille on oma lukunsa.

IMPLEMENTATION OF RFID- AND NFC-CHIPS FOR IDENTIFICATION

Heikkilä, Matti
Satakunta University of Applied Sciences
Degree Programme in Data Processing
March 2020
Number of pages: 51
Appendices: 0

Keywords: remote reading, telecommunications technology, RFID-technology, wireless technology

---

The use of RFID-based chips in different identification devices were investigated in this thesis. At first, the history and background of technology was introduced, followed by a thorough introduction to technical features. This was done in order to give the reader a better understanding of the practical examples presented in later chapters. A brief overview of RFID chips using different frequency bands and technologies and their possible applications was made. The examples used are intended to give the reader an understanding of how commonplace the use of chip technology is after all. Standardization was dealt with in one subsection in order to clarify the most important aspects of data security, and the main reason for standardization becomes clear to the reader.

The most recent means of identification, such as the biometric passport and the mobile certificate, were carefully discussed and explained in practice. The importance of security and privacy was considered in each of the topics covered. The promotion of ecology in RFID technology was also considered. Mobile Payments has its share, in which I went through much-talked-about near-payment security and anticipated possible misconceptions about mobile payments using NFC-chips. The latter half of the thesis is devoted to security and future implementations, subcutaneous chips and the Internet of Things has its own chapter.

SISÄLLYS

Opinnäytetyössä käytetyt lyhenteet

DOS = Denial of Service, palvelunestohyökkäys
HF = high frequency eli korkea taajuus
ID = Indentifier, yksilöllinen tunniste
IoT = Internet of Things, asioiden internet
ISO = International Organization for Standardization
kHz = kilohertsi
LF = low frequency eli matala taajuus
MHz = megahertsi
MITM = Man-In-The-Middle, eräänlainen tietojenkalastelumetodi
NFC = Near Field Communication
RFID = Radio Frequency Identification
SATU = sähköinen asiointitunnus
UHF = ultrahigh frequency eli ultrakorkea taajuus
WORM = write once, read many eli kerran uudelleenkirjoitettava siru

1 ENSIMMÄINEN LUKU/ JOHDANTO

Tunnistautuminen on viime vuosien aikana siirtynyt pääsääntöisesti sähköisesti tehtäväksi. Erilaiset mobiilivarmenteet ja pankkitunnuksilla tunnistautuminen ovat arkipäivää ja tekniikat tunnistautumisen nopeuttamiseen ja helpottamiseen kehittyvät kaiken aikaa. Passeissa on henkilön biometriset tunnistetiedot sisältävä siru, ja erilaisia älylukkoja koteihin ja työpaikoille kehitetään jatkuvasti. RFID-tekniikkaa on päivittäin käyttämissämme laitteissa kuten kulkutunnisteissa ja mobiililaitteissa, ja sen käyttö yleistyy kovaa vauhtia. Mahdollisesti tulevaisuuden maailmassa perinteiset tunnistautumiskeinot, kuten verkkopankkitunnuksilla tunnistautuminen tai Kela-kortin esittäminen terveyskeskukseen saavuttaessa, korvautuvat yhä enemmän mobiilivarmenteella. Kotiin saavuttaessa ovi aukeaa älypuhelimen NFC-sirua käyttäen, työpaikalla RFID-sirun sisältämällä kulkutagilla kirjaudutaan tietokoneeseen, erillisiä salasanoja ei tarvita. Kun koira viedään eläinlääkärille, ei erillisiä todistuspapereita tarvita, vaan eläimen korvaan implantoitu RFID-siru luetaan vastaanotolla, ja saadaan tarvittavat tiedot. Luetellut skenaariot ovat jo osittain toteutuneet ja jatkuvasti yleistymässä.

Tässä työssä perehdyn RFID- ja NFC-sirujen jo hyväksi havaittuihin käyttömahdollisuuksiin tunnistautumisen välineenä sekä pohdin tulevaisuuden ratkaisuja tunnistautumisen kentällä. Lisäksi käsittelen mahdollisia riskejä, kuten esimerkiksi identiteettivarkaudet, tagien ekologisuus ja turvallisuus. Yksityisyys ja tietoturva ovat aihealueita, joita tuon esille korostetusti, sillä sirutekniikasta puhuttaessa huoli yksityisyydensuojasta nousee monesti puheenaiheeksi. Biometrisen tunnistautumisen hyötyjä ja haittoja on käsitelty, sillä se on ollut Suomessa puheenaiheena passien ja henkilökorttien uudistuksen jälkeen.
Perinpohjainen esittely sirujen tekniikasta auttaa lukijaa hahmottamaan toimintamekanismin ja ymmärtämään paremmin arkipäiväisiä käyttökohteita. Esimerkiksi kuinka työpaikan oven avaaminen kulkutunnisteella tapahtuu tekniikan näkökulmasta, ja kuinka tämän voisi tulevaisuudessa hoitaa ilman kulkutunnisteavainta, vaikkapa omaan sormeen implantoidulla sirulla. Lisäksi pohdintaa sirujen mahdollisesta fyysisten korttien ja kulkutunnisteiden

syrjäyttämisestä ja miten tämä mahdollisesti vaikuttaisi muun muassa identiteettivarkauksien määrään.

Perinteisten tunnistautumistapojen, kuten henkilökortin tai ajokortin käyttäminen tehdään vaivalloisemmaksi, ja niiden hankkiminen vie aikaa sekä resursseja myös kortit toimittavilta tahoilta. Luvussa kolme käsitellään kansalaisvarmenteen ja mobiilivarmenteen käyttöä tunnistautumisen välineenä, sirutekniikkaa apuna käyttäen. Mobiilimaksaminen NFC-sirulla varustettujen älylaitteiden avulla on ajankohtainen aihe: NFC-tekniikan yleisin käyttötarkoitus on nimenomaan maksaminen. Työssä käsitellään tunnistautumisen ohessa siis myös mobiilimaksamista, sen hyötyjä ja mahdollisia tietoturvariskejä.

Digitalisaatio-aspekti on otettu työssä huomioon, siruteknologian tulevaisuutta käsitellään luvussa neljä. Kovasti kasvavan Esineiden Internetin ja RFID-teknologian yhteisiä tekijöitä ja mahdollisuuksia on pohdittu, vielä hieman tuntematonta käsitettä on havainnollistettu esimerkein arkipäiväisistä IoT-laitteista.
Työn tarkoitus on olla sivistävä sekä oikoa ennakkoluuloja RFID-tekniikkaa käyttäviin siruihin liittyen sekä lisätä tietoa näiden mahdollisista käyttökohteista.

2 RFID- JA NFC SIRUT

2.1 RFID-sirujen historiaa

RFID on lyhenne sanoista Radio Frequency Identification ja sitä käytetään yleisnimityksenä tekniikoille, jotka välittävät tietoa radiotaajuuksia pitkin. Yksinkertaistetummin tämä tarkoittaa radiotaajuuksista etätunnistamista. Tunnistaminen tapahtuu tunnisteen ja lukijan välillä, jotka kommunikoivat keskenään tietyllä erikseen määrätyllä taajuudella. Näiden radiotaajuuksien käyttö on standardoitu kansainvälisten määritysten mukaisesti. RFID-tunniste voi olla esimerkiksi puhtaasti siru, jossa on antenni, tai tagi, joka kiinnitetään tuotteeseen. Tagina voi toimia myös tarra, jonka sisällä siru sijaitsee. Yleinen käyttökohde on myös kulkuavain, jonka sisällä RFID-tunniste sijaitsee, ja tämän lukija voi olla vaikkapa työpaikan ovessa. Seuraavassa alaluvussa selitetään tarkemmin tagin käyttöä tunnistautumisessa ja sen tekniikkaa.
(Toptunnisteen www-sivut 2019)

RFID:n kaltaista tekniikkaa sovellettiin jo toisen maailmansodan aikoihin. Iso-Britannian ilmavoimat käytti lentokoneisiin asennettavaa lähetintä, joka tuottaa omaperäisen signaalin. Tutkan avulla kyettiin tunnistamaan taivaalla lentävä kone, sillä omien koneiden signaali oli lähettimen takia erilainen kuin vihollisten koneilla. (Saeng 2019) Tämänkaltaisia transpondereita eli lähettimiä käytetään lentokoneiden tunnistamiseen edelleen.
Samankaltaista tekniikkaa hyödyntää myös sodan jälkeen syntynyt innovaatio nimeltään EAS, jota käytetään myymälävarkauksien ehkäisyyn. Tuotteessa oleva tagi on aktiivinen, kunnes tuote maksetaan, ja tagin aktivointi puretaan. Jos asiakas yrittää lähteä maksamatta tuotetta, laukaisee edelleen aktiivisena oleva tagi hälytyksen uloskäyntiporteilla. Nämä tagit voivat olla tekniikaltaan passiivisia RFID-tageja. EAS on ensimmäisiä ja käytetyimpiä RFID-pohjaisia ratkaisuja edelleen. (Smiley 2017)

Hieman myöhemmin, vuonna 1973 patentoitiin ensimmäiset nykytekniikkaa muistuttavat RFID-tunnisteet. Aktiivinen tunniste, jossa oli päällekirjoitettava muisti sekä passiivinen, joka taas muistutti enemmän nykyäänkin käytettävää kulkuavain-

tyyppistä tunnistetta. Ensimmäinen RFID-pohjainen avaimeton ovenavausjärjestelmä kehitettiin siis jo 1973. (Advanced Mobile Groupin www-sivut 2015)
1970-luvulla tekniikkaa kehitettiin kansainvälistä kauppaa, kuljetusliikennettä ja eläinten merkkaamista varten, 1980-luvulle tultaessa RFID:tä aletaan laajamittaisesti käyttämään tunnistautumiseen eläimissä ja autoissa ympäri maailman. (Ward 2009)

Myöhemmin kehitettiin muun muassa Euroopassa tietullien keräämiseen ETC-järjestelmä, joka perustuu RFID-tekniikkaan. Tämän tyyppistä tekniikkaa käytetään edelleen esimerkiksi Norjassa raskaan liikenteen tietullimaksujen keräämiseen.
Autoissa on RFID:tä käyttävä tunniste ja tietullin kerääjänä toimii lukija. Järjestelmä otettiin käyttöön Norjassa vuonna 2015. (Autopassin www-sivut n.d)

Ensimmäinen etätunnistetekniikkaa käyttävä passi kehitettiin Malesiassa vuonna 1998. Tämä biopassiksikin kutsuttu henkilöllisyystodistus sisältää RFID-sirun, johon on tallennettuna henkilötietoja ja kasvokuva, aivan kuten perinteisessäkin passissa. (Gelin 2018)
2000-luvulle tultaessa RFID-teknologia on kaupallistunut, tagien ja sirujen hinnat ovat laskeneet sekä niille on syntynyt uusia käyttökohteita uusien innovaatioiden myötä. Jo vuoteen 2000 mennessä RFID:hen liittyviä patentteja oli haettu yli tuhat kappaletta.
(Advanced Mobile Groupin www-sivut 2015)

Nykyään tätä tekniikkaa käyttäviä laitteita on suurimmalla osalla ihmisistä päivittäisessä käytössä. Mobiililaitteella lähimaksaminen hyödyntää RFID-tekniikkaa käyttävää NFC:tä. Työpaikkojen kellokortit sisältävät usein myös tunnistesirun, teollisuusalalla tuotteiden valmistuksen seuraamiseen ja optimointiin käytetään samaa tekniikkaa, aikaansaamalla tehokkaampi valmistusprosessi.

Radiotaajuuksisen etätunnistetekniikan kehitys on tuonut mukanaan tehostumista, nopeutumista ja tarkkuutta prosesseihin niin työn kentällä kuin ihmisten vapaa-ajan toimintoihinkin Hyvänä esimerkkinä erään hyväntekeväisyysjärjestön kanta-asiakkaiden sisäänkirjautumisajat lyhenivät kahdeksasta minuutista 75 sekuntiin, kun heidän kortteihinsa asennettiin RFID-tunnisteet.
(Morimoto 2018)

RFID:n käyttö tulevaisuudessa lisääntyy entisestään, sillä esimerkiksi IoT:n kaltaiset järjestelmät yleistyvät arkipäiväisessä elämässä ja asioita automatisoidaan entistä enemmän.

2.2 RFID-tekniikkaa

RFID:n peruspilarit ovat tunniste, jota kutsutaan myös tagiksi sekä lukijalaite, joka voi olla esimerkiksi mobiililukija tai kiinteä, automaattinen lukija. Tagissa oleva siru sisältää tunnistetietoja, ja on yhteydessä tagin antenniin, jota käytetään tiedon välittämiseen tagin ja lukijan välillä. Lukijassa on myös antenni, joka välittää radiosignaalia. (Garska 2018)

Tunnisteen käyttötarkoituksen mukaan valitaan sen koko, käyttötaajuus, antennityyppi ja muistikapasiteetti. Sen sisältämä tieto voidaan välittää lukijasta eteenpäin tietokoneelle, jolloin voidaan suorittaa esimerkiksi kulunvalvontaa työnpaikalla, jos kulkuavaimessa olevaan tagin muistiin on merkitty työntekijän ID. Tässä tapauksessa tagia voidaan käyttää myös tietokoneelle kirjautumisessa, jos koneeseen on kytketty RFID-lukija. Tämä vähentää erilaisten tunnusten tekemistä, kun kaikki identifiointiin tarvittavat tiedot ovat työntekijän RFID-tagissa. Tagit voivat olla tyypiltään vain-luku-tyyppisiä, tai sellaisia, joihin voi tallentaa vain yhden kerran dataa tai informaatiota, joka tekee tagista henkilökohtaisen, jos siihen on esimerkiksi tallennettu tietyn työtekijän tiedot. Näitä tageja kutsutaan nimellä ”write once, read many” (WORM). Näissä tageissa on tietty uniikki järjestysnumero, josta tagin voi tunnistaa ja joka estää tietojen päivittämisen. (IdTechExin www-sivut 2004)

Uudelleenluettavat- ja kirjoitettavat tagit ovat kansainvälisemmältä nimeltään ”read-write”. Tietojen päivittäminen onnistuu useamman kerran toisin kuin WORM-mallin tageissa, mutta tämän mallin tageistakin löytyy tagin yksilöivä järjestysnumero, joka on siihen painettu jo tehtaalla. Järjestysnumeroa ei voi muuttaa. (RFID-Journalin www-sivut n.d.)

Tagit korvaavat viivakoodeja, sillä (riippuen käytetystä tekniikasta) niiden lukunopeus ja etäisyys on tehokkaampaa kuin perinteisen viivakoodin etsiminen ja lukeminen.

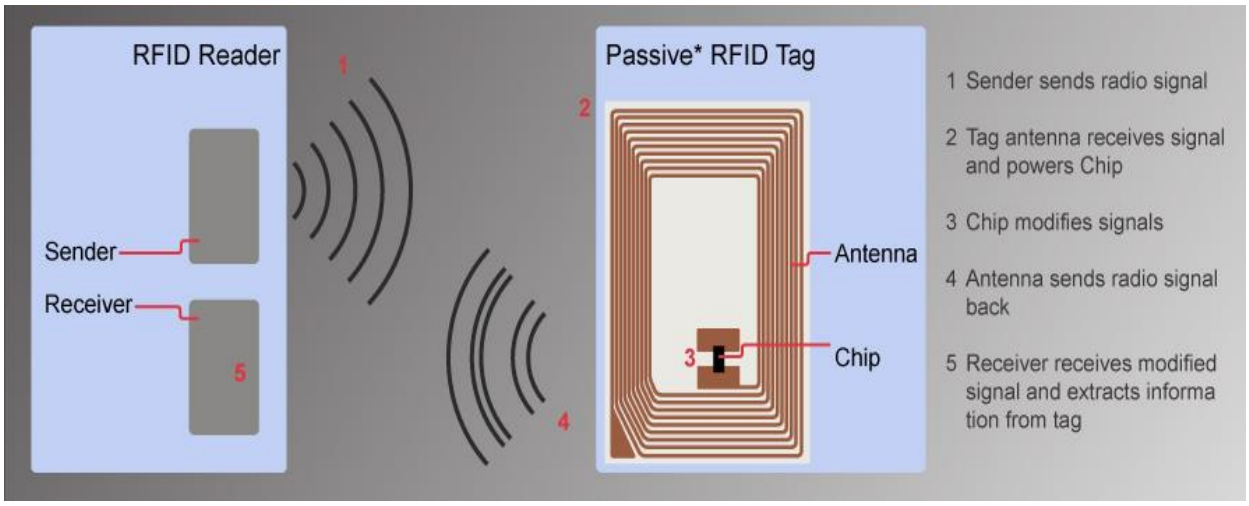
RFID-tunnisteilla varustetuttuja tuotteita voidaan lukea useita samaan aikaan, eivätkä ne kulu käytössä kuten viivakoodeille saattaa tapahtua. Viivakoodeja korvaavat tagit tulisivat olla vain-luku-tyyppisiä, sillä muulloin väärinkäyttömahdollisuudet kasvavat. Käytännössä tämä tarkoittaa sitä, että pyrkimykset muuttaa tagiin kirjoitettua tietoa, eli tässä tapauksessa tuotteen hintaa, koituisivat kauppojen ongelmaksi.

2.2.1 Passiiviset RFID-tunnisteet

Tagin ja lukijan välinen tiedonsiirto tapahtuu passiivisissa tunnisteissa lukijan lähettämän radiosignaalin välityksellä: lukija lähettää tiettyä radiotaajuutta, joka indisoituu sähkövirraksi, ja aktivoi tagissa olevan antennin, joka lähettää sirulla olevan tiedon lukijalle. Tämän vuoksi passiivisissa tageissa ei tarvita omaa virtalähdettä. (Smiley 2016)

Virtalähteen puuttumisen takia passiiviset tunnisteet ovat kooltaan pieniä ja edullisia valmistaa ja niiden käyttöikä on pidempi kuin virtalähteellisissä tunnisteissa. Lukuetäisyys on lyhyt, noin muutamasta senttimetristä metriin, mutta tämän voi nähdä hyvänä asiana, sillä mahdolliset virheluvut jäävät pois. Passiivisten tagien muistin määrä on yleensä pieni, sillä muutaman millimetrin kokoiseen siruun ei mahdu kovinkaan paljon muistia. Lukijan vaikutusalueen ulkopuolella oleva tunniste ei käytännössä tee mitään, se vain sisältää pienen määrän siihen tallennettua tietoa. Ihmisille ihon alle asennetut RFID-tunnisteet ovat kokonsa, käyttöikänsä ja turvallisuutensa takia passiivisia tunnisteita. (Technovelgyn www-sivut n.d)

Yleisimmät käyttötarkoitukset passiivisille tunnisteille ovat eläinten rekisteröinti: lemmikkieläimen tai tuotantoeläimen yksilökohtainen ID on esimerkiksi korvaan implantoidussa RFID-sirussa. Passiivisten tunnisteiden etuna mainittakoon vielä puolipassiivisiin ja aktiivisiin tunnisteisiin verrattuna tehokas nesteiden ja kosteiden pintojen läpäisy. (Dua 2016)



Kuva 1. Passiivisen RFID-tunnisteen toiminta kuvattuna

2.2.2 Puolipassiiviset RFID-tunnisteet

Puolipassiiviset tunnisteet eroavat passiivisista siten, että ne sisältävät oman virtalähteen. Ero ei kuulosta suurelta, mutta virtalähde mahdollistaa lisäominaisuuksia, kuten seurannan ja ääniefektien lisäämisen. Tämä vaikuttaa hieman tunnisteen kokoon ja hintaan, myös lukuetäisyys kasvaa pidemmäksi mitä passiivisilla tunnisteilla. Puolipassiivinen tunniste voi siis ilmoittaa äänimerkillä vaikkapa sisäänpääsyn epäämisen tai ilmoittaa hoitohenkilökunnalle, jos potilas poistuu sairaalan alueelta. Sairaaloissa käytettävissä rannekkeissa käytetään monesti puolipassiivisia tunnisteita, joihin on liitetty reaaliaikainen seurantaominaisuus. (Miller 2019)

Virtalähteen käyttöikä on kahdesta viiteen vuotta. Aktiivisista tunnisteista puolipassiiviset eroavat lähetystehon osalta, niissä ei ole omaa lähetintä, joten lukijan tuottamaa virtaa tarvitaan myös puolipassiivisten tunnisteiden lukemisessa. Erillinen virtalähde tunnisteessa mahdollistaa myös passiivista tunnistetta pidemmän lukuetäisyyden. (Bonsor & Fenlon, 2007, 4)

Puolipassiivisia tunnisteita käytetään laajalti elintarvike- ja lääketeollisuuden parissa, sillä niiden mahdollistama lämpötilasensori on hyödyllinen tuotteiden kylmäketjun katkeamattomuuden seurannassa. Esimerkiksi avaamatonta insuliinia tulisi säilyttää kylmässä, sillä lämpö heikentää lääkkeen toimintakykyä. Puolipassiivinen tagi, joka

seuraa lääkkeen kylmäketjun toteutumista on lääkettä tarvitseville siis erittäin hyödyllinen innovaatio. (Lantto 2017)

Kuva 2. Puolipassiivista RFID-tekniikkaa käyttävä tunniste kylmäketjun toteutumisen seurantaan

2.2.3 Aktiiviset RFID-tunnisteet

Aktiiviset RFID-tunnisteet sisältävät oman virtalähteen, tyypillisesti jonkinlaisen pariston, sekä lähettimen. Yleisimmin aktiiviset tunnisteet käyttävät tekniikkaa, jossa signaalia lähetetään muutaman sekunnin välein. Jatkuvan signaalin jakaminen nopeuttaa tunnistamisen toimintaa, mutta ongelmaksi muodostuu virtalähteen kuluminen. Patterin käyttöiän tullessa loppuun täytyy tagi vaihtaa. Patteri on käyttöiältään kolmesta viiteen vuotta, joissain patterityypeissä kymmenenkin vuotta. (GaoRFID:n www-sivut 2018)

Sisäinen virtalähde parantaa tunnistamisen lukuetäisyyttä merkittävästi, tehokkaimmissa aktiivisissa tunnisteissa tämä on satoja metrejä. Tämä voidaan nähdä etuna suurissa rakennuksissa, joissa tarvitaan vain yksi lukija ja muutama toistin, kun tagit ovat kaukaa luettavissa. Tunnisteen koko ja kustannukset ovat suurempia verrattuna passiivisiin ja puolipassiivisiin tageihin, molempiin vaikuttavat eniten lisävarusteet kuten tägin lian- ja kosteudenkestävyyden vaatimukset ja vaadittu käyttöikä. Tämä on myös suurin tekijä hinnan muodostumisessa, sillä perusmallinen

aktiivinen tagi voi maksaa alle kymmenestä eurosta yli sataan euroon. Esimerkkinä kalliimman mallin tagista voisi olla tagi, joka on tarkoitettu raskaaseen käyttöön ja on vedenpitävä ja iskunkestävä. (Ray 2018)

Aktiivisiin RFID-tunnisteisiin voi tallentaa enemmän tietoa mitä puolipassiivisiin ja passiivisiin, sekä tiedonsiirtonopeus aktiivisissa tageissa on suurempi. Suuremman lukemisetäisyyden lisäksi aktiivisia tunnisteita voidaan myös lukea useita kerralla. (Bibi 2019)

Tämä on erittäin hyödyllistä esimerkiksi satamissa, joissa tulevia kontteja on useita ja ne ovat eri paikoissa. RFID-tunnisteet konteissa auttavat varmistamaan, että kaikki kontit ovat saapuneet oikeaan paikkaan.

Kuva 3. Aktiivista RFID-tekniikkaa käyttäviä tunnisteita

2.3 RFID-tunnisteiden käyttämät taajuudet

Tässä alaluvussa käsitellään RFID-tunnisteiden käyttämiä taajuuksia, jotka jakautuvat taajuusalueisiin ja standardeihin. Itse tunniste ja lukija kommunikoivat tietyllä taajuudella ja tämän taajuuden valinta vaikuttaa oleellisesti myös lukuetäisyyteen ja lukemisen tarkkuuteen. Matalan ja korkean taajuuden RFID-tunnistejärjestelmät toimivat magneettien indisoimalla sähkövirralla, ultrakorkean taas sähkökentän tuomalla virralla. (Koskinen 2007, 4)

Taajuuksia Suomessa hallitsee Viestintävirasto, matalia ja korkeita taajuuksia on standardoitu tietylle taajuus- ja tehoalueelle. Globaalit standardit UHF-taajuusalueelle vaihtelevat, esimerkiksi Euroopassa sallittu taajuusalue on 865-868mHz, Yhdysvalloissa vastaava frekvenssi on 902-928MHz. (Smiley 2014)

Laitteet yleensä asetetaan käyttämään tiettyä taajuusaluetta jo valmistusvaiheessa, joten Yhdysvalloista UHF-tageja ja lukijaa hankkiessa täytyy varmistaa, onko taajuusalue muutettavissa. HF-taajuusalueen laitteita voidaan käyttää ympäri maailman taajuudella 3-30MHz (suurin osa kuitenkin taajuudella 13.56Mhz), samoin LF-taajuusalueen käyttö Euroopan alueella 125–34 kilohertsin taajuudella on rajoittamatonta. (RFIDInEuropen www-sivut. n.d.)

Taajuusalueiden standardoinnin lisäksi on asetettu standardeja, joilla pyritään maailmanlaajuiseen toimivuuteen, sillä standardien puutteen vuoksi monet valmistajat ovat kehittäneet omia järjestelmiään, joissa on omat taajuudet, ja vain tämän valmistajan laitteet toimivat tietyllä taajuudella. Viivakoodien EAN-koodejakin valmistava kansainvälinen EPCGlobal-niminen järjestö on pyrkinyt standardoimaan RFID-tekniikkaa ja tekemään siitä yhtenäisempää. EPC- ja ISO-standardit käsitellään tarkemmin myöhemmissä luvuissa.

Käsiteltävänä olevat taajuusalueet ovat LF, UHF ja HF. Sivuan myös NFC-tekniikkaa korkean taajuuden tunnisteiden alaluvussa. RFID-teknologiaa hyödyntävä NFC, eli lyhyen matkan langaton teknologia käyttää yleisesti HF-taajuusaluetta, jonka lukuetäisyys on yleensä kosketusetäisyyden mittainen. NFC-teknologia on sisäänrakennettuna uusimmissa mobiililaitteissa valmiina, eikä sen käyttöönottoon vaadita välttämättä erillisiä sovelluksia. NFC-tageja käytetään kulunvalvontaan, maksamiseen ja tunnistautumiseen. (Bluebiten www-sivut 2020)

HF-taajuusaluetta käytetään usein myös logistiikan valvontaan ja kirjastoissa kirjojen hyllypaikkojen löytämiseen tai varkaudenestoon. Tämä tehostaa työskentelyä ja vähentää varkauksista koituvia kuluja. (ElectronicSpecifierin www-sivut 2010) LF-taajuusalue on samantyyppinen, mutta tiedonsiirtonopeudeltaan hitaampi. Sitä käytetään eniten eläinten tunnistukseen sekä joidenkin ajoneuvojen käynnistyksenestojärjestelmissä.

Taajuuksia mitataan hertseinä, joka on taajuuden mittaamisen yksikkö. Kun lasketaan tietyn asian toistuminen tietyllä ajanjaksolla, ja jaetaan toistojen määrä ajanjakson pituudella, saadaan taajuus. Yksi hertsi on siis yksi tapahtuma yhdessä sekunnissa, vastaavasti 300 hertsiä olisi kolmesataa tapahtumaa sekunnissa.

2.3.1 LF-taajuusalueen tunnisteet

LF – eli Low Frequency-taajuusalueella RFID:tä käyttävillä tekniikoilla ei ole mitään virallista käyttöstandardia, mutta yleisin käytetty taajuusalue on välillä 125–134 kilohertsiä. Näillä matalampaa taajuusaluetta käyttävillä tunnisteilla on hitaampi datansiirtonopeus mitä kahdella muulla edellä mainitulla taajuusalueella. Tunnisteen tulee olla lähellä lukijaa ja mieluiten paikallaan, jotta tagissa oleva data siirtyy lukijaan. Useaa kohdetta ei ole mahdollista lukea samaan aikaan, toisin kuin korkeamman taajuuden tunnisteissa. Matalan taajuuden tunnisteet ovat hieman hintavampia kuin korkean ja ultrakorkean taajuuden vastaavat. Matalaa taajuutta käyttävien tunnisteiden etuna on materiaalin- ja nesteenläpäisykyky, ja niitä käytetäänkin usein esimerkiksi lemmikkieläinten tunnistamiseen. Taajuus ei ole herkkä radiotaajuukselliselle kohinalle, joka saattaisi heikentää lukemisprosessia. (Impinjin www-sivut, 2018)

Mahdollisessa lemmikkieläimen karkaamistapauksessa eläimessä oleva siru voidaan lukea, ja siinä oleva data kertoo kodin sijainnin, johon eläin palautetaan. Ne ovat myös suosittuja lihakarjan merkinnässä Eläimiin laitettavat tunnistesirut ovat aina passiivisia, sillä virtalähde saattaisi vahingoittaa eläintä. Passiivinen tunniste on myös kokonsa puolesta paras ratkaisu, sillä se on kivuton ja helppo asentaa kohteelle. LF-taajuudella toimivat tunnisteet ovat yleisestikin passiivisia RFID-tunnisteita, ja niitä voidaan lukuetäisyytensä ja hyvän kestävyytensä vuoksi käyttää myös kulkutunnistetageina. (Miller 2019)

Kuva 3. Passiivinen, matalan taajuuden RFID-tunniste eläinten merkintään http://www.rfidcardcube.com/news/the-hygienic-rfid-tag-for-livestock-tracking-o-10644684.html

2.3.2 HF-taajuusalueen tunnisteet

HF- eli High Frequency taajuusaluetta ei ole kansainvälisesti standardoitu, vaan korkean taajuuden RFID-pohjaiset tekniikat toimivat 3–30MHz välimaastossa ympäri maailman. Suurin osa korkean taajuuden tunnisteista kuitenkin operoivat taajuusalueella 13.56MHz, ja sitä voidaankin pitää epävirallisena standardina. (AtlasRFIDstoren www-sivut n.d.)

Pienestä luku/kirjoitusetäisyydestä huolimatta (noin 10cm–1m) korkean taajuusalueen tunnisteilla on mahdollista lukea noin kymmentä kohdetta samanaikaisesti. Lyhyt toimintasäde estää käytön esimerkiksi teollisuudessa tai liikenteenvalvonnassa, mutta häiriönsietokyky ja nesteiden läpäisykyky parantavat tämän taajuusalueen tunnisteiden käyttökohteiden skaalaa. Yleisimmin HF-taajuudella toimivia tunnisteita käytetään kirjastoissa ja kulunvalvonnassa, eli esimerkiksi työpaikan avainkortista saattaa löytyä HF-taajuutta käyttävä tunnistesiru. (Resource Labelin www-sivut 2018)

Nesteenläpäisykyvyn vuoksi myös ihmisten ja eläinten tunnistukseen voidaan käyttää korkeaa taajuutta käyttäviä tunnisteita. Tietyt nestemäiset lääkeaineet voidaan myös merkitä tunnistamista ja apteekissa varastointia varten korkean taajuuden siruilla.
(Radiotaajuinen tunnistus eli RFID teollisuuden sovelluksissa, n.d, 1-2)

Korkeaa taajuusaluetta käyttää myös RFID-tekniikkaa hyödyntävä NFC, suomennettuna lyhyen kantaman teknologia. Sen käyttö on standardoitu taajuusalueelle 13.56MHz, ja tarkka lukuetäisyys on alle 10 senttimetrin etäisyys lukijasta.
Tätä voi itse testata kauppareissulla, sillä jos maksaessaan lähimaksulla liikuttaa korttia nopeasti maksupäätteen vieressä, ei lukijan sisältämä maksupääte onnistu hyväksymään maksua, sillä tunnisteessa eli kortissa olevan tiedon lukeminen epäonnistuu. Asialla on hyvätkin puolensa, sillä tämä estää maksuvälinepetosten tekemisen lähimaksuominaisuutta hyväksikäyttäen. On hyvin epätodennäköistä, että varas pääsisi niin lähelle lähimaksuominaisuudella varustettua korttia, etteikö kortin omistaja huomaisi tapahtumaa ja onnistuisi estämään sen, koska kortin tulee olla todella lähellä lukijaa ja maksutapahtuman tapahtumiseen menee muutama sekunti.
(NFC-Forumin www-sivut, 2019)

NFC:tä on yhtenäistämisen vuoksi standardoitu ja ISO 14443 & ISO 18000-3-standardit kuvaavat NFC:n olevan lyhyen kantaman tiedonsiirtoa varten. Kansainvälisen standardoinnin ja toimivuuden vuoksi monen yrityksen on helppo ottaa NFC käyttöön.
(Triggs 2018)

Tutuin käyttötarkoitus Suomessa on lähimaksaminen, joko pankkikortilla, joka sisältää NFC-sirun tai mobiililaitteella, jossa on siru ja sovellus. Maksutilanteessa sovellus hyödyntää NFC-tekniikkaa ja kommunikoi maksupäätteen kanssa. Suurimassa osassa mobiililaitteita on tänä päivänä sisäänrakennettuna lyhyen matkan langatonta siruteknologiaa käyttävä siru. Merkittävänä erona RFID-teknologian muihin laitteisiin on se, että NFC:tä käyttävät laitteet voivat toimia niin lukijalaitteena kuin tunnisteenakin. Etäluettavat tunnistekortit esimerkiksi kuntosalilla tai joukkoliikenteessä sisältävät useimmiten NFC-tekniikkaa. Tulevaisuudessa on mahdollista asentaa henkilön mobiililaitteeseen tai jopa implantoida työntekijän

käteen siru, jolla työpaikan ovi aukeaa. Muistikapasiteetin ollessa suurempi voisi samaan siruun myös tallentaa useamman eri paikan tunnistetiedot, joten avaimia ei tarvitsisi enää kantaa mukana. Tästä aiheesta perusteellisemmin seuraavassa luvussa. HF-taajuutta käyttävät tagit ja NFC-sirut ovat edullisia, eniten hintaan vaikuttavat tagin koko ja kestävyysominaisuudet. (Dua 2019)

NFC-tekniikkaa käytetään yhä useammin myös NFC-tarroissa, joihin voi säilöä tietoa, jonka voi lukea mobiililaitteella viemällä laitteen tarran läheisyyteen. Yleensä tarraan säilötään esimerkiksi internetosoite tai yhteystiedot, mutta riippuen tarran koosta, voidaan siihen säilöä enemmänkin tietoa. Mahdolliset käyttötarkoitukset ovat rajattomat, ja tarraan voi esimerkiksi tallentaa myös asetuksia ja komentoja mobiililaitteille. Esimerkiksi tulevaisuudessa ylioppilaskirjoituksiin saavuttaessa oppilaiden ei tarvitsisi käsin sammuttaa puhelimiaan, sillä se saattaa jännittävässä tilanteessa unohtua, vaan he voisivat jo ovella lukea NFC-tarran, joka käskee puhelinta sulkeutumaan. (Chandler 2012)

Kuva 4. Sosiaalisen median tunnusten jakoon tehtyjä NFC-tarroja

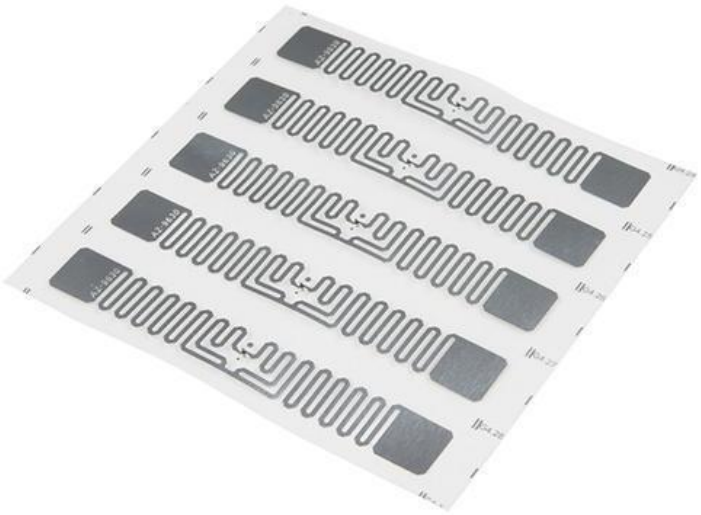
2.3.3 UHF-taajuusalueen tunnisteet

Viimeiseksi pääsemme standardoiduimpaan taajuusalueeseen, UHF:ään. Ultra High Frequency eli ultrakorkean taajuuden tunnisteet toimivat Suomessa taajuudella 865.6–867.6MHz. Samaa, luvasta vapaata taajuusaluetta saa käyttää esimerkiksi hälytysjärjestelmien tai radiopuhelinten taajuudeksi. Suurin sallittu teho UHF RFID-järjestelmissä Suomessa on kaksi wattia, tehon ja taajuusalueiden standardit määrittää Viestintävirasto. (Laukkanen 2019, 3)
Ultrakorkealla taajuudella toimivien tunnisteiden lukeminen onnistuu kymmenenkin metrin päästä. Lisäksi on mahdollista lukea useita tunnisteita samaan aikaan. Lukuteho- ja etäisyys riippuvat siitä, onko itse tunniste aktiivinen vai passiivinen RFID-siru, ja siitä, mikä on sallittu maksimaalinen teho watteina. Yhdysvalloissa sallitut tehot ovat hieman suurempia kuin Suomessa, joten aktiivista tunnistetta käytettäessä lukuetäisyyden ero voi olla jopa kymmeniä metrejä. Tunnisteen lukemista haittaavat merkittävästi nesteet tai metallit, joten tämä tulee käyttötarkoitusta ajatellessa ottaa huomioon. (Laukkanen 2019, 32)

UHF-taajuusaluetta käyttävien tunnisteiden hinnat vaihtelevat suuresti, sillä passiivinen UHF-tunniste on halvimpia tunnisteita markkinoilla, kappalehinnaltaan alimmillaan noin 20 senttiä, kun taas aktiiviset tunnisteet maksavat ominaisuuksien mukaan kahdestakymmenestä eurosta ylöspäin. Ajoneuvojen, konttien tai kuormalavojen tunnistukseen käytetään useimmiten UHF-tekniikalla varustettuja RFID-tunnisteita. Tietullien keräämiseen Euroopassa on suunniteltu järjestelmä, joka toimii moottoriteiden varrella olevien palkkien sisään upotetuilla UHF-tunnisteilla. Tämä nopeuttaa tietullien keräämistä, sillä järjestelmä tunnistaa ajoneuvon 20 metrin säteellä ja jopa 250 km/h vauhdista.
(Dima 2018)

Suomalaislähtöinen Lindström Group käyttää työvaatteiden elinkaaren seurantaan UHF-taajuusalueella toimivia passiivisia tunnisteita. Tunnistesirun tyypin ja taajuusalueen valintaan vaikuttivat eniten passiivisten tunnisteiden kilpailukykyinen hinta sekä UHF-taajuusalueen mahdollistama usean eri tunnisteen samanaikainen luku. Työvaatteiden siirtyessä pesuun, voidaan ne kaikki pakata samaan säiliöön ja ajaa lukijaportin läpi. Vaatteiden läpäistessä lukijan järjestelmään kirjautuu tieto

tapahtumasta. Yrityksessä voidaan helposti laskea, monestiko tietty vaate on pesty ja paljonko työvaatteita lukijan läpi pesuun on kulkenut tietyssä ajassa. Tällä saavutetaan parempi asiakastyytyväisyys sekä parannetaan ekologisuutta.
(Jokinen 2019)



Kuva 5. Passiivisia, UHF-taajuusaluetta käyttäviä tunnistetarroja

2.4 RFID:tä koskevat standardit

Standardeissa kerrotaan, miten RFID-järjestelmät toimivat, millä taajuuksilla ne operoivat, miten tietoja siirretään ja kuinka lukijan ja tunnisteen välinen viestintä toimii.
RFID: n standardointi on tehty varmistamaan, että tekniikkaa käyttävät tuotteet ovat yhteentoimivia myyjästä tai käyttäjästä riippumatta. Osa tuotevalmistajista on kehittänyt omia standardeja tuotteilleen kansainvälisten standardien puuttuessa, joten allamainitut järjestöt ovat ottaneet asiakseen yhtenäistää RFID-tekniikkaa ja sen piirissä toimivia laitteita. Yhteensopivuuden lisäksi standardeissa annetaan ohjeistusta siitä, miten yritykset voivat kehittää erityyppisiä tuotteita, kuten tageja, lukijoita ja niiden lisävarusteita. (TraceID:n www-sivut, 2018)

Yhtenäiset standardit auttavat myös laajentamaan markkinoita ja lisäävät alan kilpailua, mikä alentaa standardoitujen RFID-tuotteiden hintoja. Kansainvälinen standardointi auttaa myös lisäämään ihmisten luottamusta radiotaajuksellisen etätunnistamisen tekniikkaan. Standardeita kehittävät globaalisti ISO (International Organization for Standardization) sekä GS1, molemmat näistä järjestöistä ovat voittoa tavoittelemattomia ja työskentelevät yhdessä tehdäkseen RFID-tekniikasta yhtenäisempää ja kansainvälisesti toimivampaa. (ISO:n www-sivut, 2020)
Taajuusalueiden standardointi käytiin jo läpi edellisessä alaluvussa, joten seuraavaksi käsitellään muutamaa merkittävintä määrittelystandardia RFID-tekniikan saralla.

2.4.1 ISO 11784 / ISO 11785

ISO 11784/85 ovat kansainväliset standardit eläinten tunnistamiseen RFID-tekniikkaa käyttäen. Yleisesti se toteutetaan implantoimalla mikrosiru eläimeen tai laittamalla sille korvamerkki, joka sisältää RFID-tunnisteen. Jäljittämällä tietyn alueen eläimet voidaan torjua paremmin tartuntatauteja, sekä kuluttajille suunnattujen tuotteiden alkuperän jäljitettävyys paranee. Sirutuksesta on hyötyä myös karjatilalliselle, sillä hänen on helpompi valvoa eläinten lukumäärää. Euroopan komissio vaatii Euroopan alueella maansisäisesti tai rajojen yli liikkuvien tuotantoeläinten rekisteröimistä kansainväliseen tietokantaan. Tällä asetuksella saavutetaan mahdollisuus nopeisiin varotoimiin ja muiden karjatilallisten informointiin yllättävän tautiepidemian tapahtuessa.
(Euroopan Unionin www-sivut, 2016)

ISO 11784-standardi määrittelee tunnistuskoodin rakenteen, 11785 määrittelee lähetysprotokollien ominaisuudet. Käytännössä tämä tarkoittaa sitä, että määritelty taajuusalue eläinten tunnistamiseen on 134.2 kHz, ja jokaisessa transponderissa on uniikki 64-bittinen koodi, joka sisältää maatunnuksen ja transponderin maakohtaisen yksilöivän numeron. (ISO 11784:1996, 4)
ISO-hyväksytyt protokollat ovat Full-Duplex (kaksisuuntainen järjestelmä), jossa lähetys ja vastaanottaminen voivat tapahtua samaan aikaan, sekä Half-Duplex, jossa lähettäjiä on kerrallaan vain yksi, eli lähetys ja vastaanottaminen tapahtuvat eri aikaan. Half-Duplexissa eli vuorosuuntaisessa järjestelmässä lähettäjät voivat vuorollaan

vaihtua, joten yhteys on vaihtelevasti kaksisuuntainen. Esimerkiksi myös radiopuhelinliikenne on vuorosuuntaista, sillä molemmat lähettäjä ja vastaanottaja ovat samalla taajuudella. (MaxMicrochipin www-sivut, n.d.)

ISO 14223-standardi on jälkeenpäin luotu täydentämään kahta edellä mainittua standardia, ottaen huomioon myös nykyaikaisemmat, kehittyneemmät RFID-järjestelmät.
(ISO 14223-1:2011, 4)

2.4.2 ISO 14443

Moniosainen standardi ISO 14443 määrittelee kontaktittomat älykortit ja niiden kanssa käytettävät lähetysprotokollat. Se pätee myös RFID-tekniikkaa käyttävien maksukorttien määrittelyssä. Protokollassa määritellään kaksi eri korttityyppiä, A ja B, jotka eroavat toisistaan eniten modulaation osalta, sillä A-versiossa modulaatio on täydellinen eli 100 prosenttia. B-tyypin korteilla se on vastaavasti 10%. A-versio kehitettiin vuonna 1990 Philipsin toimesta, ja B-versio vuonna 1995 kilpailevan yrityksen, TI:n toimesta korjaamaan puutteita, joita A-versiosta löytyi. Toinen mainittava ero näissä korttityypeissä on koodaustekniikka. B-tyypin versio on tehokkaampi, nopeampi ja vähemmän herkkä häiriöille. (Wehr 2003)

Standardin osa 1 määrittelee kortin fyysiset ominaisuudet kuten käyttölämpötilan, sietokyvyn ja mitat. (ISO/IEC 14443-1:2018, 1)
Osa 2 määrittelee kortin taajuuden ja tehon, määritetty taajuus on 13,56 MHz, lukijan tulee tuottaa kortin aktivoiva teho. Tämä määritelmä pätee molempiin A- ja B-tyypin kortteihin. Protokollassa erikseen mainitaan, että lukijalaitteen ollessa toimeton, tulee sen käyttää vuorotellen A- ja B-korttityypin modulointimenetelmää, kunnes korttityyppi havaitaan. Yhden korttityypin modulointimenetelmä voi olla kerrallaan käytössä, istunto katkeaa kentän katketessa tai kortin häipyessä lukukentästä. Molemmille tyypeille määritellään myös kommunikaatiorajapinnat. (ISO/IEC 14443-2:2016, 1)

Standardin kolmannessa osassa määritellään molempien tyyppien alustus sekä korttien eri toimintatilat. Törmäystenhallintaa ja lukijalaitteen eri komentoja useamman kortin kanssa toimiessa määritellään myös.
(ISO/IEC 14443-3:2018, 1)

Neljännessä standardin määrittelyosassa määritellään vuorosuuntaisen siirtomenetelmän eli Half-Duplexin tiedonsiirtoprotokolla ja tämän protokollan aktivointi sekä deaktivointi molempien korttityyppien osalta. (ISO 14223-1:2011, 4)

2.4.3 ISO 15693

Standardi 15693 on ISO 14443:n ohella suosittu lyhyen etäisyyden kontaktittomienkorttien standardi. Sen yleisimmät käyttökohteet ovat kirjastojen RFID-järjestelmät ja erilaiset kulkukortit. Kirjastoissa järjestelmä toimii siten, että itse kirjoissa on kiinni tunniste, jonka avulla voidaan hoitaa varkaudenesto sekä lainaus- ja palautusprosessin nopeuttaminen. Lukijoita on uloskäyntiporteissa sekä kirjaston työntekijöillä.
(RFID Cardin www-sivut, 2018)

ISO 15693 noudattaa samaa kaavaa edellisessä luvussa kuvaillun standardin kanssa, ensimmäisessä osassa määritellään kortin fyysiset ominaisuudet, kuten koko ja etämaksuominaisuus. Tämä standardi ja sen määrittämät kortit ovat hyvin lähellä NFC-standardia. Merkittävimpänä erona näiden kahden standardin välillä on lukuetäisyys, joka on NFC:llä noin 10 senttimetriä tai alle, kun taas ISO 15693-standardin mukaisilla korteilla se voi olla jopa metrin luokkaa.
(ISO/IEC 15693-1:2018, 1)

Standardin toisessa osassa määritellään lähietäisyydellä käytettävän kortin ja lukijalaitteen rajapinnat, eli sähköiset ominaisuudet kuten tehon ja viestintä. ISO 15693 käyttää samaa taajuutta kuin NFC ja suurin osa muista korkean taajuusalueen tunnisteista, eli 13,56 megahertsiä. (ISO/IEC 15693-2:2019)
Kolmannessa standardin osassa määritellään protokollia, komentoja ja parametreja kortin ja lukijalaitteen välisen tiedonsiirron aloittamiseen. Määrittelyn kohteena ovat

myös törmäyksenesto eli ”Anti-Collision”. Siinä kerrotaan useiden korttien samanaikaisesta käytöstä sekä tapoja helpottaa oikean kortin lukemista monien joukosta sovelluskriteerien avulla.
(ISO/IEC 15693-3:2019, 1)

3 KÄYTTÖ TUNNISTAUTUMISEN VÄLINEENÄ

Yksi yleisimmistä ja tärkeimmistä käyttökohteista RFID-tekniikalle on tunnistautuminen. Työpaikoilla tapahtuva kulunvalvonta käsitetään usein vain sisäänpääsyn oikeuttamiseen, mutta RFID-tekniikkaa käyttävän kulunvalvontajärjestelmän avulla voidaan seurata myös työajan noudattamista. Työnantaja voi seurata tiettyjen tilojen käyttöä tarkasti, järjestelmään kirjautuu minuutilleen oikea tieto siitä, kuka meni tilaan ja milloin. Työvälineisiin voidaan asentaa RFID-siruja, joiden avulla voidaan seurata niiden käyttäjiä ja käyttöikää. Sairaaloissa tai vankeinhoitolaitoksissa RFID-sirun sisältävien rannekkeiden avulla voidaan vahtia, että potilas ei lähde ilman lupaa ulos sairaalasta, yhtä lailla vankiloissa voidaan seurata, että vankeja on oikea määrä. Yhdysvalloissa usean eri osavaltion vankiloissa on jo käytössä RFID-pohjainen järjestelmä vankien seurantaan. (Heyden 2008)

Eläinten seurantaan käytetään RFID-pohjaisia järjestelmiä, eniten matalan taajuuden siruja, joko implantoituna eläimeen tai jonkinlaisen pannan/korvamerkin muodossa. Tästä on hyötyä niin tuotantoeläinten kuin lemmikkieläintenkin omistajille sillä tunnistussiruun taltioidut tiedot auttavat eläinten huolenpidossa. Tuotantoeläimiä kasvattava henkilö voi skannata sirumerkityn karjansa ja helposti laskea eläinten määrän. Eläinlääkärikäynneillä voidaan skannata eläimen siru ja saada tietoa hoitoon tulleesta eläimestä ja tallentaa siruun esimerkiksi hoitohistoriaa. Eläintä siirrettäessä toiseen maahan, voidaan seuraavassa sijainnissa skannata sama siru ja saada tiedot eläimen voinnista ja historiasta. Kotieläimen omistajaa RFID-pohjainen tunnistusjärjestelmä auttaa mahdollisessa katoamistapauksessa. Löytöeläinkodissa tai

eläinlääkärissä voidaan lukea löytyneen eläimen RFID-siru ja saada tieto siitä, missä karanneen eläimen koti on ja mitkä ovat hänen omistajansa yhteystiedot.
Uusimpia innovaatioita eläinten tunnistuksen RFID-tekniikan saralla ovat UHF-taajuutta käyttävät tunnisteet, joiden avulla voidaan seurata eläimen liikkumista, ruokailutottumuksia sekä mahdollisesti jopa terveydentilaa, kuten sydämensykettä reaaliaikaisesti. (Smiley 2015)
Alaluvuissa käsitellään erilaisia RFID-tekniikkaan liittyviä tunnistautumistapoja.

3.1 Biometrinen tunnistautuminen

Nykyaikaiset passit sisältävät biotunnisteen, eli tietoja henkilöstä, joilla hänet voidaan yksilöidä – kuten sormenjälki, kasvokuva tai DNA. Nämä tiedot biometristä tunnistautumista varten ovat säilötty passin sisältämälle RFID-sirulle. Sirulla on myös tieto henkilön nimestä, syntymäajasta sekä kansalaisuudesta. Passeissa olevat tunnistesirut ovat passiivisia, ja näin ollen saavat käyttövirtansa lukulaitteelta. Sirut ovat tyypiltään WORM – eli niihin voidaan kerran kirjoittaa henkilön tunnistetiedot, jälkeenpäin informaation muuttaminen on mahdotonta. Tämä on tehty parantamaan biometrisen passin tietoturvaa, toinen tietoturvaa parantava lisä on digitaalinen allekirjoitus, jolla voidaan varmistaa, että sirulle tietoja kirjoittanut taho on Suomen valtio eikä kukaan ulkopuolinen. (Poliisin www-sivut, 2019)

Julkisuudessa on kritisoitu biometrisen passin hintaa verrattuna aikaisempaan sekä lyhyttä voimassaoloaikaa. Aikaisemmin oli myös mahdollista liittää lasten passit omaan passiin, ikään kuin rinnakkaispasseiksi. Biometrisen tunnistautumisen passeissa se ei enää ole mahdollista. Suuri syy passin voimassaoloajan lyhyydelle on se, että sirujen tietoturvaa päivitetään tietyn ajanjakson välein, ja biometristen passien tietoturva heikkenisi merkittävästi, jos ne uusittaisiin esimerkiksi kymmenen vuoden välein nykyisen viiden sijasta. (Muikkula 2017)

Tietokoneissa on ollut jo vuosia mahdollisuus kirjautua käyttäjätilille sormenjälkeä käyttäen, ja viime aikoina myös mobiililaitteisiin on tullut biometristä tunnistautumista käyttäviä ominaisuuksia. Uusimmissa matkapuhelinmalleissa on mahdollista käyttää puhelimen lukituksen avaamiseen sormenjälkitunnistusta tai

kasvojentunnistusta. Oman kokemukseni perusteella tämä on varmempi tapa suojata mobiililaite verrattuna salasanalla suojaamiseen. Puhelimissa voidaan myös varmentaa sovelluskaupan sisäisten ostojen suorittamisen turvallisuutta biometrisen tunnistautumisen kautta. Mahdollisessa varkaustapauksessa puhelimen anastanut taho ei saa laitetta auki, ja vaikka lukitus olisi varkauden hetkellä pois päältä, ei maksutapahtumien suorittaminen onnistuisi, jos ne on suojattu oikean omistajan sormenjälkitunnisteella. Biometristen tunnisteiden ehdoton hyöty on niiden nopeus verrattuna salasanan kirjoittamiseen sekä turvallisuus. Niitä on erittäin hankala huijata, sillä jokaisella ihmisellä on erilaiset kasvonpiirteet ja sormenjälki.
Omia biometrisiä tunnisteitaan on lähes mahdoton hukata, mikä parantaa niiden tietoturvaa entisestään. (Evifinin www-sivut n.d.)

Kuva 6. Biometrinen passi, kuvassa tarkennettuna RFID-tunnistesiru

3.2 Kansalaisvarmenne ja mobiilivarmenne

Kansalaisvarmenne on Suomessa myönnettävä sähköinen henkilöllisyystodistus, jota käytetään sähköiseen tunnistautumiseen esimerkiksi viranomaisten palveluissa, kuten TE-palveluissa tai Omakanta-palvelussa. Kansalaisvarmenne itsessään sisältää henkilön etu- ja sukunimen sekä yksilöllisen sähköisen asiointitunnuksen. SATU:a eli sähköistä asiointitunnusta käytetään yksilöimään henkilö verkkoasioinnissa. Kansalaisvarmenteen saannin edellytys on, että henkilö on Suomen kansalainen tai ulkomaalainen, jonka kotikunta on Suomessa. Henkilöllisyys on todistettava varmennetta haettaessa ja ulkomaalaisilla tulee olla voimassa oleva oleskelulupa.
(Digi- ja Väestötietoviraston www-sivut, 2019)

Henkilökortissa olevaan siruun on tallennettu henkilön SATU, ja sitä voi käyttää sähköisen tunnistautumisen lisäksi matkustusasiakirjana tai henkilöllisyystodistuksena. Passin ohella henkilökortti toimii kaikkiin EU-maihin matkustaessa. Matkapuhelinta voi käyttää tunnistautumiseen, jos puhelimen omistaja ottaa mobiilivarmenteen käyttöön. Mobiilivarmenne on eräänlainen sähköinen henkilöllisyystodistus puhelimessa, joka toimii SIM-kortissa sijaitsevan tunnisteen avulla. Sitä voi käyttää tunnistautumiseen eri verkkopalveluissa kuten sähköistä asiointitunnustakin, mutta vielä hieman laajemmin. Varmenne on voimassa viisi vuotta kerrallaan, ja uusimisen koittaessa tarvitsee tilata uusi SIM-kortti. Operaattoria vaihtaessa tai puhelinnumeroa muuttaessa tulee mobiilivarmenne myös aktivoida uudestaan. Tämä tehdään tietoturvan parantamisen vuoksi. (Mobiilivarmenteen www-sivut 2017)

Mobiilivarmenteen käyttöönotto ja tunnistautuminen sen avulla on yksinkertaista ja nopeaa verrattuna esimerkiksi pankkitunnuksilla tunnistautumiseen.

Tämä tapahtuu siten, että liittymän omistaja tunnistautuu joko liittymän tarjoajan palvelupisteessä tai sähköisessä asiointipalvelussa vahvaa tunnistautumista, kuten verkkopankkitunnuksia käyttäen. Suomessa Telia, DNA sekä Elisa tarjoavat mobiilivarmennetta tunnistautumiseen. Se toimii kaikissa uudemmissa matkapuhelimissa ja uusissa SIM-korteissa. Mobiilivarmenteen mahdollistama tekniikka löytyy myös suurimmasta osasta vanhoja SIM-kortteja, kortin sarjanumeron perusteella voidaan selvittää, onko kyseisessä kortissa mobiilivarmenteen käyttömahdollisuus. (Simonaho 2013, 16)

Käyttäjä saa tunnistautumisen jälkeen mobiilivarmenteen käyttöön lisättyään siihen henkilökohtaisen salasanansa. Tämän jälkeen tunnistautumiseen vaaditaan enää tunnistautumispyynnön tullessa oma puhelinnumero ja nelinumeroinen tunnusluku.

Kuva 7. Mobiilivarmenteen luoma tunnistuspyyntö tunnistautumishetkellä

Mobiilivarmenteen tietoturvasta puhuttaessa nousee esiin uhkakuva, jossa henkilön mobiililaite anastetaan ja sen avulla hänen identiteettinsä varastetaan mobiilivarmennetta hyödyntäen. Tämän rikoksen tekemistä hankaloittaa mobiilivarmenteen erillinen tunnusluku tai puhelimen sormenjälkitunnistinta käyttävä tunnistus. (Kärkkäinen 2019)

Skenaariona onnistunut mobiilivarmenteen anastus on pelottava, sillä varmenteella voi tunnistautua pankkipalveluihin, hakea lainaa sekä kirjautua kaikkiin Suomen valtion ylläpitämiin palveluihin kuten TE-palveluihin tai Poliisin asiointipalveluun. Turvallisuutta parantaa biometrisen tunnistautumisen käyttöönotto, eli joko sormenjäljellä tai kasvojentunnistuksella puhelimen lukituksen avaaminen, sekä mobiilivarmenteen tunnusluvun peittäminen aina sitä kirjoittaessa. Pidän itse henkilökortin ja luottokortin sisältävän lompakon varkautta suurempana uhkana kuin sitä, että matkapuhelimeni onnistutaan anastamaan ja varas saa purettua kasvojentunnistuksella ja salasanalla varustetun lukituksen sekä arvaamaan mobiilivarmenteen tunnusluvun oikein.

Toinen mahdollinen varkausmenetelmä on lähettää väärennetty tunnistuspyyntö henkilön puhelimeen, ja odottaa, että se ajattelematta hyväksytään ja tietojen kalastelija saa haluamansa. Väärennettyjen tunnistepyyntöjen luominen ja lähettäminen puhelimeen vaatii paljon vaivaa, sekä herättää varsin helposti epäilyksen käyttäjässä, sillä mobiilivarmenne ei pyydä tunnistuspyyntöä ilman, että olet itse ensin valinnut sen tunnistautumistavaksi johonkin palveluun.

3.3 Mobiilimaksaminen ja tunnistautuminen NFC-sirua käyttäen

Mobiilimaksamista on Suomessa harjoitettu jo aikaa ennen varsinaisia älylaitteita, sillä jo ennen 2000-lukua mobiilimaksua pystyi harjoittamaan, jos omisti matkapuhelimen. Puhelinsoitolla tai tekstiviestillä tehty maksu lisättiin operaattorin puhelinlaskuun. Tänäkin päivänä on mahdollista ostaa joukkoliikenteen matkalippuja tekstiviestillä. (Mobiilimaksuinfon www-sivut 2019)

Mobiilimaksamisen käsite muuttui 2010-luvulle tultaessa merkittävästi, kun mobiililaitteissa yleistyivät NFC-sirut, joita voidaan käyttää lyhyen matkan tunnistautumis- ja maksutapahtumissa. Lähimaksun hyväksyvissä maksupäätteissä voi maksaa NFC-sirun sisältämällä mobiililaitteella, kuten matkapuhelimella, älykellolla tai -rannekkeella. Erillisillä mobiilisovelluksilla voidaan siirtää rahaa nopeasti: esimerkiksi maksaessa kaverille ruokatilausta ei tarvitse enää kysellä tilinumeroa tai kantaa pankkitunnuksia mukana, kun maksaminen onnistuu puhelinnumeroita vaihtamalla. Älylaite, jossa on NFC-siru, voi toimia niin lukijana kuin tunnisteenakin, joka mahdollistaa sekä rahan lähettämisen että vastaanottamisen. Tällä hetkellä suosituimpia mobiilimaksusovelluksia ovat Pivo, MobilePay, GooglePay ja ApplePay. Maksutapahtuman onnistuminen edellyttää tietysti saman maksusovelluksen omistamista ja tunnistautumista sovellukseen.
(7 things to… 2019)

Mobiilimaksaminen älylaitteella onnistuu laitteen NFC-sirun kommunikoidessa maksupäätteen lukijan kanssa, lukija tuottaa tarvittavan sähkömagneettisen energian tiedonsiirtoon ja kommunikointiin. Lähimaksun yleistyessä maksukorteissa sekä mobiilimaksumahdollisuuden tullessa älypuhelimiin, heräsi yleinen keskustelu NFC:n turvallisuudesta ja siitä, voidaanko kortilta veloittaa lähimaksuja käyttäjän

huomaamatta. Periaatteessa tämä onnistuu maksupäätelaitetta käyttämällä, mutta kiinnijäämisen mahdollisuus on aika suuri, sekä lähimaksun toimintaetäisyys pieni, varsinkin jos kortti on lompakossa ja lompakko takin tai housujen taskussa. Tekijä tarvitsisi myös jonkin maksunvälittäjäpalvelun sekä maksupäätelaitteeseen liitetyn tilin, johon maksut menevät. Mahdollinen lisäsuojautuminen lähimaksuvarkailta on RFID-lompakko, jossa on suojakalvo, joka estää sirun aktivoivan signaalin etenemisen korttiin asti.
(Klaus 2016)

Tietoturvan kannalta etuna on sirun lyhyt toimintasäde, joten virhelukuja tai rikoksen mahdollisuutta ei useimmiten ole, varsinkin koska nykyaikaiset älylaitteet ovat suojattu biometrisellä tunnistautumisella tai vähintäänkin salasanalla. Jotkin maksuvälineitä tarjoavat yritykset vaativat vahvaa tunnistautumista mobiilimaksuja tehdessä, esimerkiksi MasterCardilla on maksusovellus, jossa käyttäjä tunnistautuu kasvojen- tai sormenjälkitunnistuksen avulla palveluun tekemään maksuja. (Raes 2016)

Sirun pienen koon vuoksi NFC-tekniikkaa hyödyntäviä maksuvälineitä voidaan kehittää edelleen. Luottoyhtiö Visa on koekäyttänyt NFC-sirun sisältämiä sormuksia, joilla maksu tapahtuisi yhtä helposti kuin mobiililaitteellakin, mutta sormusta olisi helpompi kantaa mukana kuin älypuhelinta tai lompakkoa. Itseäni huolettaisi maksusormusta käyttäessä sen tietoturva, sillä sitä ei ole suojattu millään salasanalla tai biometrisellä tunnisteella. Mikäli ottaisin käyttöön maksusormuksen niin mahdollisia vahinkoja minimoidakseni asettaisin sen käyttöön alhaisen turvarajan. (Epstein 2016)

Kuva 8. Maksutapahtuman hoitaminen NFC-sirun sisältämällä sormuksella

NFC-sirun hyödyt älylaitteissa eivät jää pelkkään mobiilimaksamiseen, vaan niitä voi käyttää myös tunnistautumisen välineenä. NFC-sirun sisältävää matkapuhelinta tai älykelloa voi käyttää esimerkiksi työpaikan tai kodin älylukon avaimena.

Suomalainen iLOQ Oy on kehittänyt ensimmäisenä maailmassa älylukon, joka saa energiansa matkapuhelimen ja lukon NFC-sirujen induktiosta. Tämä ratkaisu helpottaa älylukkojen käyttöönottoa, sillä lukkojen yleinen ongelma on huolto- ja päivitystöiden kustannukset kuten paristojen vaihto ja kaapelointityöt. Perinteisten lukkojen riesana voi olla lukon kuluminen ja mahdolliset huoltotyöt, mutta erityiseksi ongelmaksi nousevat avaimet, niiden katoaminen ja riittämätön määrä. NFC-tunnistetta käyttävä älylukko on ratkaisu tähän ongelmaan, sillä lukon pääsynhallintaohjelmaa voidaan hallita pilvipalvelusta, ja esimerkiksi jakaa lukon “avain” tietyille henkilöille, esimerkiksi yrityksen työntekijöille reaaliajassa. Mahdollista on myös avata lukko järjestelmän avulla etänä tietyksi aikaa, vaikka yrityksen yleisten aukioloaikojen ajaksi.
(iLOQ kehitti puhelinta käyttävän älylukon 2016)

Järjestelmä helpottaa kulunvalvontaa, sillä jokainen NFC-tunnisteella sisään mennyt henkilö voidaan reaaliajassa tunnistaa. Avainten määrää voidaan lisätä helposti ja nopeasti järjestelmästä ilman, että tarvitsee teettää uusia avaimia uusille työntekijöille, eikä ole huolta avainten katoamisesta. Vaikka työntekijä hukkaisi tai rikkoisi mobiililaitteen, joka toimii avaimena, voidaan hänelle helposti järjestelmässä tehdä uusi avain ja deaktivoida vanha. Ongelmaksi niin yritys- kuin kuluttajakäytössäkin voi

koitua älylaitteen akun loppuminen, vaikka itse NFC:n käyttö ei akkua kulutakaan samalla volyymilla kuin esimerkiksi älylukkojärjestelmissä suosittu Bluetooth. Tätä tilannetta varten on kehitetty erillinen NFC-sirun omaava tunnistetagi, mutta omasta mielestäni tagin kantaminen mukana ja siitä jatkuva huolehtiminen heikentää tätä ”avaimettomuuden” tunnetta. (iLoqin www-sivut n.d.)

Muita NFC:n vahvuuksia tunnistautumisen välineenä on helppous jakaa NFC-tarrojen muodossa tietoa, kuten yhteystietoja tai sosiaalisen median tunnuksia. On mahdollista, että mainokset ovat tulevaisuudessa jonkinlaisia NFC-tunnisteen sisältäviä, luettavia tarroja, joissa voisi olla enemmän tietoa kuin nykyisissä paperisissa mainoslehdissä. Älylaitteella skannattavat mainokset olisivat myös ekologisempi ratkaisu kuin jaettavat, sillä suurin osa niistä menee suoraan roskiin tai viimeistään tarjousten voimassaolon umpeuduttua. Kaupat voisivat myös säästää printtauskuluissa, jos NFC-sirulla valjastetut ympäristöystävällisestä materiaalista tehdyt mainokset ja alennuskupongit syrjäyttäisivät nykyiset paperista tehdyt.
(Near Field Communicationin www-sivut 2017)

Matkapuhelinten käyttö kulkutunnisteina tulee todennäköisesti lisääntymään, sillä suurella osalla kansalaisista on jo älypuhelin, josta löytyy NFC-siru. Tämä olisi yleisen kulutuksen ja ekologisuuden kannalta hyvä asia, sillä muovisia kulkutunnistetageja tehdään vuosittain miljoonia, ja niiden tekeminen sekä hävittäminen kuluttaa luontoa. RFID-tunnisteidenkin käyttö on kuitenkin ekologisempi ratkaisu kuin muovisten viivakoodikorttien, sillä nämä kortit kuluvat käytössä huomattavasti nopeammin, ovat alttiimpia hajoamaan ennen elinkaarensa loppua ja sisältävät enemmän muovia kuin RFID-tunnistetagit.

3.4 RFID- ja NFC-sirujen turvallisuuskysymykset

Törmäyskonfliktien ohella erilaiset hyökkäykset järjestelmiin ovat yleistymässä RFID-tekniikan suosion kasvaessa. Törmäyskonfliktilla tarkoitetaan tilannetta, jossa tapahtuu tagin lukuvirhe johtuen useasta eri RFID-tagista lukijan lukuetäisyydellä. On mahdollista, että usean tagin aktivoidessa lukijaa samaan aikaan, menee lukijan lukuominaisuus häiriötilaan, ja tagit jäävät lukematta. Törmäyskonflikteja aiheuttaa

myös usean eri lukijan sijaitseminen samalla alueella. Tagien lukuvirheitä saattavat aiheuttaa myös tietyt materiaalit, kuten metallit ja nesteet. Törmäyskonfliktien ja virhelukujen toteutumiseen voi käyttäjä itse olla vaikuttamassa valitsemalla oikeanlaisen RFID-tekniikan omaan ympäristöönsä ja minimoimalla häiriöitä aiheuttavat tekijät.
(Mulkahainen 2016, 11)

Aktiivisista hyökkäyksistä puhuttaessa tarkoitetaan erilaisia tiedonkaappaus- tai häirintämetodeja, jotka kohdistetaan RFID-järjestelmään. Eavesdropping eli salakuuntelu on yksi suurimmista uhista RFID-tekniikan tietoturvalle. Salakuuntelun avulla hyökkääjä onnistuu saamaan tietoa tunnisteista, niiden sisällöstä ja käyttöajankohdasta. Uhka kohdistuu myös henkilöiden turvallisuuteen, sillä työpaikoilla, joissa käytetään RFID- tai NFC-siruja tunnistautumisen välineenä on siruihin mahdollisesti tallennettu paljon yksityistä tietoa. Hyökkääminen tapahtuu siten, että hyökkääjä kuuntelee RFID-radioliikennettä yhteensopivan lukijalaitteen kanssa, mahdollisesti tallentaen kaiken liikenteen lukijan ja tunnisteiden välillä. Kaikki RFID-tunnisteet eivät osaa erottaa ”oikeaa” lukijaa kaappaajan lukijasta, ja tietojen kaappaaminen käy helposti.

Eavesdropping-metodia muistuttava MITM-hyökkäys (Man-In-The-Middle) on toinen yleinen kuunteluhyökkäysten toteuttamistapa. Näiden kahden kuuntelumetodin avulla voidaan hyökkäystä jalostaa vielä spoofing – eli huijaushyökkäykseksi, jossa RFID-järjestelmään syötetään väärennettyä tietoa tai haittaohjelma. Sillä on mahdollista syöttää järjestelmään tunnistetiedot henkilöstä, jolla ei todellisuudessa olisi kulkulupaa kiinteistöön, tai häiritä lukuliikennettä lähettämällä lukijaan jatkuvia sulkukomentoja. Yrityksen kulku- ja tunnistejärjestelmien kaataminen on mahdollista spoofing-metodilla luodulla tunnisteella, joka sisältää viruksen tai komentoja, jotka kaatavat kaikki lukujärjestelmät. Replay-attackin eli toistohyökkäyksen avulla voidaan käyttää hyödyksi salakuuntelulla saatuja tietoja, ja saada valheellinen pääsyoikeus tilaan. Sen onnistumiseksi vaaditaan järjestelmään syötettyjä, jo hyväksyttyjä tietoja, jotka voidaan saavuttaa tunnistetietoliikennettä vakoilemalla.
(El Beggal & Azizi 2017, 196)

Aktiivisen hyökkäyksen metodiksi laskettava DOS (Denial of Service) eli palvelunestohyökkäys on nimensä mukaisesti tehty estämään järjestelmän toimintaa. Sen toteuttaminen tapahtuu RFID-systeemin radiotaajuuksia häiritsemällä, eli lähettämällä voimakkaita radiosignaaleja, jotka sekoittavat lukulaitteen ja aiheuttavat sille todennäköisesti myös fyysistä vahinkoa. Esimerkkitilanteessa palvelunestohyökkäyksen laatija häiritsee yrityksen varaston RFID-järjestelmää niin, että lukulaite menee sekaisin, ja mitkään varastosta lähtevät tai sinne saapuvat tavarat eivät kirjaudu järjestelmään. Tämä aiheuttaa merkittävästi lisätyötä ja kustannuksia. (Grunwald 2006)

Mahdollista on myös tagin ”eliminointi” niin sanotulla kill-komennolla, joka on tarkoitettu tagin omistajan käyttöön, ja sillä voidaan esimerkiksi deaktivoida varashälyttimeksi tarkoitettu RFID-tagi. Komennon väärinkäyttö onnistuu tietämällä komentoon käytettävä salasana, jonka valmistaja on määrittänyt ja toimittanut tunnisteen omistajalle. Tapahtuma on epätodennäköinen, ja vaatii yleensä salasanatiedon omistajalta, sillä uudemmat tagit käyttävät 32-bittistä salausta. (Mitrokotsa, Rieback & Tanenbaum 2008, 76)

Tiedon kaappaaminen voi mahdollistaa jopa identiteettivarkauden tekemisen, myös kulkutunnisteiden sisältämien tunnistetietojen kopioiminen mahdollistaa hyökkääjän tunkeutumisen työpaikalle fyysisesti, väärennetyllä kulkutagilla. Maksukorttien kloonaamisesta ja tietojenkaappaamisesta ei kuitenkaan tarvitse olla huolissaan, sillä korttien NFC-siruteknologia on tarkemmin standardoitua ja tiedonsiirto on uudemman sukupolven korteissa aina salattua. (Grimes 2017)

RFID-tunnisteiden standardien vähyys ja edullinen hinta, varsinkin massatuotannon maissa kuten Kiinassa, on aiheuttanut tietoturvariskien lisääntymistä tekniikan sisällä. Paljon puhuttu viivakoodien korvaaminen RFID-siruilla on riskialtista ennen standardoinnin parantumista, sillä väärennyshyökkäyksellä voidaan esimerkiksi muuttaa halutun tuotteen sirun sisältöä, tässä tapauksessa esimerkiksi hintaa hyökkääjälle mieluisemmaksi.
(Electronic Notesin www-sivut n.d.)

3.4.1 RFID-teknologian tietoturvauhilta suojautuminen

Edellä luetellut RFID-tekniikan tietoturvariskit ovat yhdistelmä turvallisuusriskejä ja yksityisyyden uhkia. Turvallisuusriskeihin kuuluvat esimerkiksi maksutapahtumien ja kulkulupien väärentäminen ja kybervandalismi. Yksityisyydelle RFID:n tietoturvauhat tarkoittavat mahdollista identiteettivarkautta ja omistajan toimien seuraamista. (Fernández-Caramés 2017, 3)
RFID-järjestelmien tietoturvaa kohentaessa täytyy ottaa huomioon tunnisteiden käyttötarkoitus, joka on helpottaa ja nopeuttaa tunnistamista. Tietoturvaparannusten ei tulisi vaikeuttaa tunnisteiden käyttöä, esimerkiksi kulkutunnisteiden kääriminen alumiinifolioon estää hyvin mahdolliset salakuuntelu- ja tiedonkaappausyritykset, mutta laskee tunnisteen helppokäyttöisyyttä erittäin merkittävästi.

Salakuuntelun ja muiden tietoturvariskien yleistyessä RFID-tekniikan piiriin on kehitetty salaustekniikoita. On olemassa tunnistetageja, jotka käyttävät niin sanottua ”rolling code” eli vierityskoodi-metodia. Metodissa tagin tunnistetiedot vaihtuvat jokaisen lukukerran jälkeen pyrkien näin estämään esimerkiksi kulkutunnisteen pääsytietojen kaappaamista Eavesdropping-metodilla. Vierityskoodi-tekniikka on käyttäjän kannalta helppo ratkaisu, sillä se ei muuta tagin fyysistä käyttöä mitenkään. Sitä vastoin tunnistejärjestelmän hallitsijalle ongelmallisempi, sillä yksilöllisten tunnistetietojen vaihtuessa joka lukukerran jälkeen, ei voida enää yksilöidä jokaista sirua käyttäjäänsä.

Kehittyneemmät suojaustekniikat käyttävät ”challenge-response”-salaustekniikkaa, jossa kysyvä osapuoli, tässä tapauksessa RFID-lukija lähettää ”haasteen”, johon vastaaja, eli RFID-tunniste vastaa ”response”-viestillä. Tunnisteen vastaus generoituu salaustekniikan avulla, eikä tunnistetietoja voi kaapata salakuuntelumetodilla, sillä lukijan ja tunnisteen välinen tietoliikenne on kryptattu, kaappaaja saa käsiinsä vain tapahtumaa varten yksilöidyn numerosarjan. Tunnisteen lähettämä vastaus vaihtuu joka lukukerta, tämä vaikeuttaa edelleen tagin ja lukijan välisen tietoliikenteen kaappaamista. (Rouse 2018)
Ongelmaksi nousee tämänkaltaisilla suojaustekniikoilla varustettujen RFID-sirujen hinta, sillä ne ovat huomattavasti kalliimpia kuin massatuotannolla tehdyt, standardoimattomat ja suojaamattomat vaihtoehdot. RFID-tageilla on pienen kokonsa

ja yksinkertaisen toimintametodinsa vuoksi erittäin vähän laskentatehoa, joka vaikeuttaa kompleksisten salaustekniikoiden käyttöönottoa siruteknologiassa. Salaustekniikat vaativat huomattavan paljon enemmän laskentatehoa mitä varsinkaan halvemmilla tunnistetageilla on tarjota. Lisäksi niitä on vaikea ottaa käyttöön vanhoissa RFID-järjestelmissä, sillä tekniset vaatimukset lukijoiden osalta eivät riitä salaustekniikoiden käyttöönottoon. RFID-pohjaista järjestelmää käyttöönotettaessa tulee ottaa kustannuksissa huomioon myös tietoturva. Vaikka turvallisemman järjestelmän hankintahinta olisi korkeampi, turvallisempi käyttöympäristö saattaa säästää käyttäjän vielä isommalta laskulta, jos sillä onnistutaan välttämään tietomurrot ja vandalismi.
(RFID Handbook: Applications… 2008, 478)

RFID-järjestelmän tietoturvauhista puhuttaessa tulee ottaa huomioon myös NFC-sirujen tietoturva. Maksukorttien lähimaksuominaisuuden ja mobiilimaksamisen suosion kasvaessa on noussut huoli maksutapahtumien kaappaamisesta ja korttien väärinkäytöstä. NFC-tekniikalla varustetut kortit ja mobiililaitteet ovat kuitenkin huomattavasti paremmin salattuja kuin RFID-sirut, pääasiallisesti NFC:n laajemman standardoinnin vuoksi. Maksukortit käyttävät lähimaksussa edellä mainittua vierityskoodi-tekniikkaa, jossa korttiin sulautettu mikroprosessori vaihtaa tunnistekoodia jokaisella lukukerralla, tehden sen jäljittelemisen erittäin hankalaksi. Hyökkääjän kaapatessa maksutapahtuman tiedot, saa hän haltuunsa vain sitä maksutapahtumaa varten yksilöidyn salauskoodin, jota on hyvin hankala saada auki. Vaikka varas onnistuisi lukemaan esimerkiksi puhelimen sovelluksesta maksukortin tiedot, jäisi hänelle käteen ainoastaan kortin numero ja haltijan nimi, maksutapahtumien suorittamiseksi hän tarvitsisi siis vielä kortin takana olevan kolminumeroisen turvanumeron haltuunsa. Suoraan kortista edellä mainittujen tietojen lukeminen onnistuu erillisellä lukijalla, mutta varkaan täytyy päästä kortin lähelle, ja tältä ongelmalta on helppo suojautua RFID-lompakolla tai käärimällä maksukortti folioon, sillä se estää radiomagneettisten säteiden kulun.
(Erenhouse 2018)

Kortin sirulla tehtävä maksutapahtuma toteutuu vain, jos kortissa olevan sirun prosessoima henkilökohtainen identifiointikoodi eli tässä tapauksessa henkilökohtainen tunnusluku kirjoitetaan lukijaan.

Lähimaksussa tunnuslukua ei tarvita, mutta lukijan ja tunnisteen välinen tapahtumatunnistekoodi vaihtuu joka maksutapahtuman jälkeen, ja ennalta määrätyn maksutapahtumien määrän jälkeen lukija vaatii kortilta tunnuslukua myös lähimaksua käytettäessä varmistaakseen oikean omistajan. Lähimaksulla tehtävien ostosten summa on rajattu muutamaan kymppiin siksi, että kortin varkaustilanteessa sillä ei pysty aiheuttamaan oikealle omistajalle merkittävää taloudellista vahinkoa aikaiseksi, ei siksi, että sen tietoturva olisi alhaisempi kuin tunnusluvulla maksamisen. (Brecht 2019)

NFC-tekniikkaa uhkaavat toki samat tietojenkalastelumetodit kuin RFID-sirujakin, mutta niiden turvallisuuteen on kiinnitetty huomattavasti enemmän huomiota kuin pääasiallisesti tunnistekäyttöön käytettävien RFID-sirujen turvallisuuteen. Yleisempää kuin suora tietojen kalastelu on NFC-maksuliikenteen häirintä törmäyskonfliktien avulla. Väärennettyjen maksupyyntöjen lähettämisen voi eliminoida ottamalla maksulaitteella NFC:n käyttöön vasta kun maksua ollaan suorittamassa ja tarkistamalla aina maksun saajan ja summan tarkasti. Kaappauksen suorittamiseen NFC-sirua käyttäen tarvitsee hyökkääjän päästä tarpeeksi lähelle uhrin maksulaitetta, muutaman senttimetrin päähän. On hyvin epätodennäköistä, ettei uhri huomaisi, jos tällaista joku yrittäisi. (Heikkinen 2013, 38)

Älypuhelimen mobiilimaksamisominaisuutta hyödyntävä Apple Pay linkittää käyttäjän maksutiedot Apple-tunnukseen, sen sijaan, että luottokorttitietoja tallennettaisiin itse puhelimeen. Tämä ja sormenjälkitunnistuksen tai kasvojentunnistuksen käyttö maksutapahtuman todentamisessa antaa ylimääräisen turvallisuuskerroksen maksutapahtumalle. Apple Payn tapauksessa maksutapahtuman datan kaappauksesta ei olisi hyökkääjälle mitään hyötyä, sillä datan hyväksikäyttämiseksi hänen tarvitsisi saada uhrin Apple-tilin tiedot, josta käytetyn maksuvälineen tiedot löytyvät.
(Giese 2018, 5)

Suurin riski NFC-tekniikan tietoturvalle on käyttäjän huolimattomuus: jos NFC:tä ei aktiivisesti käytä, kannattaa se kytkeä puhelimen asetuksista pois päältä. Tällä välttää mahdolliset huijausyritykset, kuten väärennetyt maksupyynnöt. Mobiililaitteessa, jossa käyttää mobiilimaksua, tulee olla biometrinen salaus, kuten sormenjälki- tai

kasvojentunnistus. Tiedossani olevat mobiilimaksusovellukset kuten Pivo ja Android Pay vaativat salasanan tai sormenjälkitunnistautumisen maksutapahtuman yhteydessä. Mahdollisin kuviteltavissa oleva tietoturvariski NFC-siruilla varustetuille mobiililaitteille on skenaario, jossa suojaamaton laite varastetaan ja se sisältää omistajansa maksutiedot. On hyvä muistaa myös päivittää mobiililaitteen käyttöjärjestelmä ja maksusovellukset ajan tasalle, sillä vanhat sovellusversiot altistavat tietoturvahyökkäyksille.

Kuva 9. Mobiilimaksutapahtuma Apple Pay-sovelluksella, sormenjälkitunnistautumisen käyttö maksutapahtuman vahvistamiseksi havainnollistettu

4 RFID-TEKNIIKAN TULEVAISUUS

Opinnäytetyön kirjoittamisen aikaan tehty RFID-alan tutkimus osoittaa tulevaisuuden olevan sirutekniikan osalta valoisa. IDTechEx:in tekemästä tutkimuksesta selviää, että vuonna 2019 RFID-alan arvo on noin 11,6 miljardia dollaria. Laskelma sisältää tunnisteet, lukijat, ohjelmistot sekä palvelut. Ennustuksen mukaan arvo tulee kasvamaan 15,2 miljardiin dollariin vuoteen 2024 mennessä. Raportti paljastaa, että passiivisten tunnisteiden myynti on kasvanut 13 prosenttia verrattuna vuoteen 2018,

nopeiten kasvanut sirutekniikka on ultrakorkean taajuuden sirut. Tämä selittyy pitkälti RAIN-RFID-tekniikan yleistyessä, siinä UHF-taajuudella varustetut sirut yhdistetään internetiin, jolloin RFID-dataa voidaan käsitellä, varastoida ja jakaa internetin välityksellä.
Maksuvälineissä käytettävä NFC-tekniikka jatkaa kasvuaan, mutta maksujen ulkopuolella NFC:n kasvu on kovin hidasta, johtuen siitä, että niitä ei myydä samanlaisissa volyymeissä isoille yrityksille kuin radiotaajuuksellista etätunnistusta käyttäviä siruja.
(Over 20 Billion… 2019)

Passien, mobiilimaksamisen ja NFC-tagin sisältämien maksukorttien myötä elämämme on muuttunut aiempaa sirutetummaksi, ja RFID-tekniikkaan törmää nykyään joka paikassa. RFID:n standardoinnin parantuessa ja tagien hinnan laskiessa edelleen voivat tunnisteet korvata jopa viivakoodit kaupoissa, ja helpottaa teollisuuden automatisointia entistä enemmän. Tällä voidaan saavuttaa rahallista ja ajallista säästöä sekä vähentää turhan, monotonisen työn tekemistä.
Seuraavissa alaluvuissa käsitellään innovaatioita RFID-tekniikan saralla, jotka ovat vähemmän tuttuja, mutta selvästi yleistymässä olevia käyttökohteita tunnistussiruille.

4.1 Ihonalaiset tunnistesirut

Eläimillä laajasti käytettyjä ihonalaisia RFID-tekniikkaa hyödyntäviä mikrosiruja on myös implantoitu ihmisten käyttöön. Ihon alle, yleensä kämmeneen, etusormen ja peukalon väliin asennettu siru voi olla RFID- tai NFC-siru. Yleisimmät käyttötarkoitukset ihonalaisella RFID-sirulla ovat kulkutunnisteena käyttö, siru korvaa perinteisen kulkutagin esimerkiksi työpaikalle tai harrastuksiin mentäessä. Matkakortin voi korvata sirulla, siihen saa tallennettua myös esimerkiksi salasanoja, joten tietokoneen lukituksen avaaminen voi tapahtua ihonalaista sirua käyttäen. NFC-sirutekniikkaa hyödyntävät implantit ovat tarkoitettu tietojen tallentamiseen, omistaja voi tallentaa vaikkapa käyntikorttinsa implanttiin, ja se voidaan lukea suoraan hänen kädestään. Tämä voi olla tulevaisuudessa yksi keino vähentää turhaa ympäristön kuormittamista, kun muoviset kortit ja paperiset, usein erittäin lyhytikäiset käyntikortit voitaisiin korvata tulevaisuuden ratkaisulla. (Schwartz 2019)

Ruotsissa Epicenter-niminen yritys on tarjonnut työntekijöilleen sirun implantoimista käteen, ja yli 150 työntekijää on ottanut sellaisen. Työntekijät voivat avata ovia, käyttää printtereitä ja maksaa lounaansa sirun avulla.
Nähtäväksi jää, milloin Suomessa jokin yritys uskaltautuu kokeilemaan vastaavaa. (Lehti 2018)

Yleisenä pelkona ihmisiin implantoiduissa siruissa on uhka siitä, että sirun valmistaja tai muu taho seuraa sirun ottajan toimintaa sen avulla. NFC-tekniikalla varustetuissa siruissa tämä on käytännössä ottaen mahdotonta, sillä sirujen toimintasäde on muutaman senttimetrin luokkaa. Ihmisiin implantoitavat sirut ovat kooltaan noin riisinjyvän kokoisia, joten niissä ei voi olla kovinkaan isoa antennia. Tämä tarkoittaa suoraviivaisesti sitä, että RFID-teknologialla varustettu siru on yksityisyydensuojaltaan hyvää tasoa. Suunnitteilla on myös mikrosiruja, joissa olisi pieni valo, joka vilkkuisi ihon läpi, jos sirua yritetään luvattomasti lukea.
(Savage 2018)
Pelot ja ennakkoluulot eivät kuitenkaan ole pelkästään nopean digitalisoitumisen shokista johtuvia, sillä tietokonevirus on onnistuttu tartuttamaan ihmiseen implantoituun mikrosiruun, josta käyttäjä olisi sitä voinut tietämättään levittää muiden laitteisiin. RFID-teknologiaa on suunniteltu ihmiskäyttöä varten vasta lyhyen aikaa, joten sirua ottaessa tulee ottaa huomioon mahdolliset tietoturvariskit ja varmistaa, että siru on läpäissyt stressitestit ihmiskäyttöä varten. (Readingin Yliopiston www-sivut 2010)

Käteen implantoitavien sirujen tietoturvan ollessa vielä alkeellisella tasolla, NFC-teknologiaa hyödyntävät sirut maksuvälineinä eivät ole toistaiseksi saaneet jalansijaa. Joitain kryptovaluutalla tehtyjä maksutapahtumia on onnistuttu tekemään. Implantti-asiantuntijoiden haaveet RFID- ja NFC-implanttien mahdollisuuksista ja käyttökohteista ovat korkealla: uskotaan, että siruilla voitaisiin tulevaisuudessa korvata esimerkiksi nykyisiä tunnistautumisen välineitä, ja seurata ihmisten terveydentilaa. Sirusta voisi olla apua, jos vaikka dementiaosastolla hoidettavana oleva potilas karkaa. Sairautensa vuoksi hän ei osaa kertoa nimeään ja yhteystietojaan, mutta ne voitaisiin helposti lukea siruimplantista älypuhelimella. Tekniikka kehittyy ja toivottavasti tulevaisuudessa saadaan entistä paremmalla tietoturvalla varustettuja

RFID- ja NFC-siruja ihmiskäyttöön. Mikrosiru voisi olla oiva väline helpottamaan arkea ihmisille, jotka haluavat kokeilla jotain uutta digitalisaation aikakaudella. (McClelland 2018)

Kuva 9. Ihon alle asennettavan mikrosirun koko ja yleisin paikka implantille havainnollistettuna.

4.2 RFID-teknologia ja IoT

IoT eli esineiden internet on eräänlainen verkkoinfrastruktuuri, joka käsittää kaikki verkkoon kytketyt esineet, laitteet ja ajoneuvot. Nämä verkkoon kytketyt laitteet aistivat ympäristöään erilaisilla antureilla ja sensoreilla, ja viestivät verkkoyhteyden välityksellä keskenään. (Jyväskylän yliopiston www-sivut 2017) Arkisin esimerkki IoT-laitteesta on aktiivisuusranneke, joka seuraa käyttäjänsä liikkumista ja muita toimintoja. Käyttäjän asettaman tavoitteen mukaan ranneke ilmoittaa, onko liikuttu tarpeeksi. Asioiden internetin tarkoitus on helpottaa ja nopeuttaa prosesseja reaaliaikaisesti kerätyn datan avulla. Esimerkiksi etäluettavat sähkö- ja vesimittarit ovat osa IoT:tä. Tämänkaltaisten innovaatioiden avulla voidaan säästää kustannuksissa, ja reaaliaikaisen seurannan avulla myös puuttua nopeammin vikatilanteisiin. (Manninen 2018)

RFID-teknologia liittyy esineiden internettiin merkittävästi, sillä monet IoT:hen kytketyt laitteet käyttävät sensoreinaan RFID-teknologiaa hyödyntäviä siruja. (Thrasher 2014)

Googlella on monia tuotteita, jotka kytketään Asioiden Internetiin, kuten älykäs ovikello, avaimeton älylukko ja älykäs termostaatti. Google Nest-termostaatissa on RFID-siru, joka mittaa reaaliajassa lämpötilaa ja jonka avulla laite oppii säätämään lämpötilaa oikeaksi tiettyinä ajankohtina. Termostaattiin kytketystä älypuhelinsovelluksesta voi nähdä reaaliajassa lämpötilan sekä kuinka paljon energiaa on kulutettu. Se on siis myös ekologinen ratkaisu, sillä laitteen ollessa kytkettynä WLAN-verkkoon, voi käyttäjä seurata ja säätää kotinsa lämpötilaa etänä. Järjestelmä osaa myös hälyttää, jos lämpötila jostain syystä laskee liian alas tai ylös.
(Google-storen www-sivut n.d.)

Tulevaisuuden IoT-ratkaisuja ovat ei-elektronisten laitteiden saattaminen IoT:n piiriin asentamalla niihin RFID-teknologialla varustettuja siruja. Älytekniikan tullessa tavallisimpiin arjen ratkaisuihin, kuten esimerkiksi lääkepurkkeihin, voitaisiin sen avulla seurata, onko potilas ottanut oikean määrän lääkettä. Niillä voisi mitata esineiden todellista käyttöikää ja vähentää turhaa kulutusta. Jotkin käytössä kuluvat esineet, kuten esimerkiksi hehkulamput, voisivat käyttöikänsä lopun lähestyessä ilmoittaa käyttäjälle, että on suositeltavaa mennä ostamaan korvaava lamppu.
(Mraz 2019)

IoT:n kasvu on sysännyt RFID-teknologian suosiota edelleen ylöspäin, ja IoT-laitteet tulevat yleistymään myös kotitalouksissa lähivuosina. Ainoaksi jarruttavaksi tekijäksi ja isoimmaksi ongelmaksi tämän infrastruktuurin laajemmassa käyttöönotossa on sen mahdolliset tietoturvaongelmat: kuten aikaisemmissa luvuissa mainittiin, on RFID:n tietoturva osittain erittäinkin haavoittuvainen. Ratkaisuna tähän voisi olla IoT-laitteisiin asennettavien sirujen standardisointi ja yhteiset määräykset tietoturvan tasosta, sillä pelottavaksi skenaarioksi nousee mahdollinen terveydentilaa seuraavien laitteiden hakkerointi ja vandalisointi.

5 JOHTOPÄÄTÖKSET JA POHDINTA

Opinnäytetyössä pohdittiin, kuinka tunnistautumistavat ovat kehittyneet ajan saatossa, ja miten juuri RFID-teknologialla varustettuja tunnistautumisen välineitä käytetään. RFID:n tekniikka selitettiin tarkasti työssä, sillä haluttiin, että lukija ymmärtää sirujen toiminnan perinpohjaisesti. Tämä auttaa myöhemmissä luvuissa esiteltyjen, monimutkaisempien asioiden ymmärtämisessä. Luvussa kolme perehdyttiin tarkemmin RFID-teknologian käyttöön tunnistautumisen kentällä käytännön esimerkein. Tulevaisuuden aspekti otettiin koko ajan huomioon, ja työhön sisältyy myös tekijän omia pohdintoja tulevaisuuden sovelluksille ja mahdollisuuksille varsinkin luvussa neljä. Tietoturvan osuus nousee korostetusti esille, sillä yksi merkittävimmistä kyseenalaistuksen aiheista RFID-tekniikalle on sen luotettavuus.

Ennen opinnäytetyöprosessia tietotasoni RFID-tekniikasta oli hyvin vähäinen, mutta perehtyminen aiheeseen on ollut hyvin opettavaista. Johtopäätöksenä voidaan todeta, että RFID-pohjaiset järjestelmät ovat nykyisessä käyttökohteessaan tunnistautumisen välineenä oikealla paikallaan. Lisämahdollisuuksia teollisuuden ja sairaanhoidon käyttöön ratkaisuja kehittämällä kuitenkin vielä on: esimerkiksi Suomessa moni teollisuuden alan yritys nojaa vielä perinteisempiin viivakoodeihin ja ihmistyöhön. Kustannus- ja aikasäästöjä voitaisiin saavuttaa ottamalla RFID-pohjainen tunnistautumisjärjestelmä käyttöön. IoT:n ja RFID:n liitto on hyvin todennäköinen, ja se kasvattanee sirujen myyntiä edelleen. Näen kuitenkin välttämättömänä RFID:n nykyistä paremman standardoinnin, jotta tietoturva paranisi ja tietomurtoja voitaisiin torjua nykyistä tehokkaammin.

RFID-pohjainen NFC on vakiinnuttanut asemansa maksuvälinemarkkinoilla, ja NFC:n avulla tehtävät mobiilimaksut yleistyvät edelleen. Tietoturvaltaan NFC on hyvin vahva, ja saattaa levitä mobiilimaksamisen suosion kasvun myötä vielä pienempiin ja helpommin mukana kannettaviin välineisiin. Esimerkkinä tästä jo prototyyppinä esitetty maksusormus tai käteen implantoitu NFC-siru. Kehitys menee kovaa vauhtia eteenpäin, ja siruteknologia tulee vakiinnuttamaan jalansijansa teollisuudessa ja yksityisten ihmisten arjessa entistä monimuotoisemmin tulevina vuosina.

LÄHTEET

7 things to know about accepting NFC mobile payments. 2019. FIS Global. 8.7.2019. Viitattu 30.1.2020. https://www.fisglobal.com/en/insights/merchant-solutions-worldpay/article/nfc-payment-acceptance-for-smbs

A Brief History of Passports: From Laissez-Passer to Biometric Passports. 2018. Gelin, P. Viitattu 15.12.2019. https://shorexcapital.com/a-short-history-of-the-passport/

Advance Mobile Groupin www-sivut. Viitattu 12.12.2019. https://www.advancedmobilegroup.com/

Advance Mobile Groupin www-sivut. Viitattu 15.12.2019. https://www.advancedmobilegroup.com/

AtlasRFIDstoren www-sivut. Viitattu 4.1.2020. https://www.atlasrfidstore.com/

Autopassin www-sivut. Viitattu 12.12.2019. https://www.autopass.no/en/

Bibi F. 2019. Active RFID VS. Passive RFID: Which differences? Viitattu 27.12.2019. https://elainnovation.com/active-rfid-vs-passive-rfid-which-differences.html

BlueBiten www-sivut. Viitattu 3.3.2020. https://www.bluebite.com/nfc/rfid-vs-nfc

Bonsor K. & Wesley F. 2007. How RFID Works. Viitattu 26.12.2019. https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/rfid8.htm

Brecht. ‘Concerns Related to…’ InfoSecInstitute-blogi. 8.9.2019. Viitattu 8.2.2020. https://resources.infosecinstitute.com/nfc-technology-payments-concerns/#gref

Chandler. 2012. What's an NFC tag? Viitattu 9.1.2020. https://electronics.howstuffworks.com/nfc-tag1.htm

Digi- ja Väestötietoviraston www-sivut. Viitattu 30.1.2020. https://dvv.fi/kansalaisvarmenne-ja-sahkoinen-henkilollisyys

Dima. 2018. Passive RFID using UHF delivers long-range benefits in the IoT. Viitattu 9.1.2020. https://www.avnet.com/wps/portal/silica/resources/article/passive-rfid-using-uhf-delivers-long-range-benefits-in-the-iot/

Dua. ‘Applications for Active and Passive RFID’ rfid4u-blogi. 27.09.2016. Viitattu 26.12.2019. https://rfid4u.com/applications-for-active-and-passive-rfid/

Dua. ‘Comparison of RFID, NFC and Barcode for Inventory Tracking – Part 1 – RFID’ rfid4u-blogi. 07.09.2019. Viitattu 9.1.2020. https://rfid4u.com/comparison-of-rfid-nfc-and-barcode-for-inventory-tracking-part-1-rfid/

El Beggal & Azizi. 2017. Review on security issues in RFID systems. Viitattu 2.2.2020. https://www.researchgate.net/publication/322726986_Review_on_security_issues_in_RFID_systems

Electronic Notesin www-sivut. Viitattu 5.2.2020. https://www.electronics-notes.com/

ElectronicSpecifierin www-sivut. Viitattu 3.1.2020. https://www.electronicspecifier.com/

Epstein, M. 2016. A new Olympic ring…Viitattu 1.2.2020. https://www.digitaltrends.com/wearables/visa-payment-ring-rio-2016/

Erenhouse. 'Dispelling the Myths…' Beyond The Transaction-blogi. 17.1.2018 Viitattu 7.2.2020. https://newsroom.mastercard.com/2018/01/17/dispelling-the-myths-the-reality-about-contactless-security-2/

Euroopan Unionin www-sivut. Viitattu 11.1.2020. https://ec.europa.eu/food/animals/identification_en

Evifinin www-sivut. Viitattu 30.1.2020. https://www.evifin.fi/

Fernández-Caramés, T. 2017. A Methodology for… Viitattu 5.2.2020. https://www.intechopen.com/books/radio-frequency-identification/a-methodology-for-evaluating-security-in-commercial-rfid-systems

GaoRFID:n www-sivut. Viitattu 27.12.2019. https://gaorfid.com/rfid-101-active-passive-differences/

Garska. 'Two-Factor Authentication (2FA) Explained: RFID Access Control' IdentityAutomation-blogi. 11.9.2018. Viitattu 16.12.2019. https://blog.identityautomation.com/

Google Storen www-sivut. Viitattu 19.2.2020. https://store.google.com/us/product/nest_learning_thermostat_3rd_gen?hl=en-US

Grimes, R. 2017. Why you don't… CSO-verkkolehden artikkeli. 22.11.2017. Viitattu 5.2.2020. https://www.csoonline.com/article/3199009/why-you-dont-need-an-rfid-blocking-wallet.html

Grunwald. 2006. New Attacks Against RFID-Systems. Viitattu 2.2.2020. https://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Grunwald.pdf

Heikkinen, S. 2013. Korttimaksamisen turvallisuus. Seminaariraportti, Tietoliikenteen turvallisuus (TLT-3601). Viitattu 8.2.2020. http://www.cs.tut.fi/kurssit/TLT-3600/maksturv-sem.pdf

Heyden, D. 2008. RFID Applications. Viitattu 25.1.2020. https://www.fibre2fashion.com/industry-article/3271/rfid-applications

IdTechExin www-sivut. Viitattu 16.12.2019. https://www.idtechex.com/

iLOQ kehitti puhelinta käyttävän älylukon. 2016. Oulu-lehti. 15.3.2016. Viitattu 1.2.2020. https://www.oululehti.fi/uutiset/iloq-kehitti-puhelinta-kayttavan-alylukon-6.386.3487370.c550861c75

iLoqin www-sivut. Viitattu 1.2.2020. https://www.iloq.com/nfc/faq/

Impinjin www-sivut. Viitattu 3.1.2020. https://www.impinj.com/about-rfid/types-of-rfid-systems/

ISO 11784:1996. Radio frequency identification of animals.1996. International Organization of Standardization. Viitattu 11.1.2020. https://www.iso.org/obp/ui/#iso:std:iso:11784:ed-2:v1:en

ISO 14223-1:2011. Radiofrequency identification of animals — Advanced transponders — Part 1: Air interface. 2011. International Organization of Standardization. Viitattu 15.1.2020. https://www.iso.org/obp/ui/#iso:std:iso:14223:-1:ed-2:v1:en

ISO/IEC 14443-1:2018. Cards and security devices for personal identification - Contactless proximity objects - Part 1: Physical characteristics. 2018. International Organization of Standardization. Viitattu 15.1.2020. https://www.iso.org/obp/ui/#iso:std:iso-iec:14443:-1:ed-4:v1:en

ISO/IEC 14443-2:2016. Identification cards - Contactless integrated circuit cards - Proximity cards - Part 2: Radio frequency power and signal interface. 2016. International Organization of Standardization. Viitattu 20.1.2020. https://www.iso.org/obp/ui/#iso:std:iso-iec:14443:-2:ed-3:v1:en

ISO/IEC 14443-3:2018. Cards and security devices for personal identification - Contactless proximity objects - Part 3: Initialization and anticollision. 2018. International Organization of Standardization. Viitattu 20.1.2020. https://www.iso.org/obp/ui/#iso:std:iso-iec:14443:-3:ed-4:v1:en

ISO/IEC 15693-1:2018. Cards and security devices for personal identification - Contactless vicinity objects - Part 1: Physical characteristics. 2018. International Organization of Standardization. Viitattu 21.1.2020. https://www.iso.org/obp/ui/#iso:std:iso-iec:15693:-1:ed-3:v1:en

ISO/IEC 15693-2:2019. Cards and security devices for personal identification - Contactless vicinity objects - Part 2: Air interface and initialization. 2019. International Organization of Standardization. Viitattu 21.1.2020. https://www.iso.org/obp/ui/#iso:std:iso-iec:15693:-2:ed-3:v1:en

ISO/IEC 15693-3:2019. Cards and security devices for personal identification - Contactless vicinity objects - Part 3: Anticollision and transmission protocol. 2019. International Organization of Standardization. Viitattu 21.1.2020. https://www.iso.org/obp/ui/#iso:std:iso-iec:15693:-3:ed-3:v1:en

ISO:n www-sivut. Viitattu 11.1.2020. https://www.iso.org/home.html

Jokinen. ‘Digitalisoidut tekstiilit’ Lindström Groupin blogi. 9.4.2019. Viitattu 11.1.2020. https://lindstromgroup.com/fi/blog/digitalisoidut-tekstiilit/

Jyväskylän yliopiston www-sivut. Viitattu 18.2.2020. https://peda.net/jyu/it/do/kkv

Kärkkäinen, H. 2019. Kännykällä kirjautuminen helpottuu – jatkossa riittää sormenjälki. Ilta-Sanomat 4.11.2019. Viitattu 30.1.2020. https://www.is.fi/digitoday/mobiili/art-2000006295954.html

Klaus. 'Kysymyksiä ja vastauksia…' Nixu Cybersecurity-blogi. 17.3.2016. Viitattu 30.1.2020. https://www.nixu.com/fi/blog/Kysymyksia-ja-vastauksia-lahimaksukorteista-NFC-korttien-turvallisuus-vuonna-2016

Koskinen, L. 2007. RFID-tekniikka ja sen sovellukset. AMK-opinnäytetyö. Tampereen ammattikorkeakoulu. Viitattu 30.12.2019. https://www.theseus.fi/bitstream/handle/10024/10286/Koskinen.Lari.pdf?sequence=2

Kuva 1. https://i.stack.imgur.com/wK2OK.jpg

Kuva 10. https://itknowledgeexchange.techtarget.com/inspect-a-gadget/wp-content/blogs.dir/307/files/2018/01/bichip-pic-768x384.jpg

Kuva 2. http://www.veryfields.net/wp-content/uploads/2011/05/A927E_Sensor.jpg

Kuva 3. https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRI4jI18fiLqTieQ_Kl4VBg2HkRTj_qKKiR5uu7_mQnGU7hL4bJBw&s

Kuva 4. https://www.shopnfc.com/708-large_default/nfc-stickers-with-social-logos-ntag213.jpg

Kuva 5. https://www.pngkey.com/maxpic/u2t4u2r5t4e6y3u2/

Kuva 6. https://www.raja.fi/download/5d77c1f6a4dabc6310754cb39353114284f89451.jpg

Kuva 7. https://yle.fi/aihe/artikkeli/2019/03/06/digitreenit-mobiilivarmenne-on-nappara-vaihtoehto-pankkitunnuksille-mutta-yhta

Kuva 8. https://www.techworm.net/2016/06/soon-can-use-nfc-enabled-visa-ring-make-payments.html

Kuva 9. https://s.appleinsider.ru/2019/12/applepayserv.jpg

Lantto, R. 2017. Älypakkaukset yleistyvät monella rintamalla. Viitattu 27.12.2019. http://digitext.fi/alypakkaukset-yleistyvat-monella-rintamalla/

Laukkanen L. 2019. UHF RFID. Kandidaatintyö. Tampereen yliopisto. Viitattu 9.1.2020. http://urn.fi/URN:NBN:fi:tuni-201907052483

Lehti, A. 2018. Käteen asennettavat sirut kasvattavat suosiotaan Suomessa. Tivi. Viitattu 12.2.2020. https://www.tivi.fi/uutiset/kateen-asennettavat-sirut-kasvattavat-suosiotaan-suomessa-kl-korvaavat-muun-muassa-avaimia-turvakoodeja-ja-kayntikortteja/a8cde431-e47b-3169-92fc-0bbf0090590b

Manninen, O. 2018. Kaupunkipyöräkin on esineiden internetiä. OP-media. Viitattu 19.2.2020. https://op.media/teemat/teknologia/kaupunkipyorakin-on-esineiden-internetia-91f62b0823294a61900fa732594e083c

MaxMicrochipin www-sivut. Viitattu 15.1.2020. http://maxmicrochip.com/ISO_types.htm

McClelland, D. 2018. Cash in hand… Computer Weekly. Viitattu 18.2.2020. https://www.computerweekly.com/blog/Inspect-a-Gadget/Cash-in-hand-This-cryptocurrency-body-implant-will-secure-your-cyber-cash-stash

Miller. 'RFID Frequencies: Low, High, and Ultra High; What They are and why it Matters' Computype-blogi. 20.11.2019. Viitattu 3.1.2020. https://www.computype.com/blog/rfid-frequencies-low-high-and-ultra-high

Mitrokotsa, A, Rieback, R & Tanenbaum, T. 2008. Classification of RFID Attacks. Viitattu 2.2.2020. https://www.cs.vu.nl/~ast/Publications/Papers/iwrt-2008.pdf

Mobiilimaksuinfon www-sivut. Viitattu 30.1.2020. http://mobiilimaksuinfo.fi/

Mobiilivarmenteen www-sivut. Viitattu 30.1.2020. https://mobiilivarmenne.fi/

Morimoto, R. 2018. Enterprise IoT: Business uses for RFID technology. Viitattu 16.12.2019. https://www.networkworld.com/

Mraz, S. 2019. Everything Could Be… MachineDesign. Viitattu 20.2.2020. https://www.machinedesign.com/automation-iiot/article/21837738/everything-could-be-part-of-the-iot-with-a-new-rfid-system

Muikkula, V. 2017. Ajan kulku näkyy… Yle Uutiset 1.12.2017. Viitattu 25.1.2020. https://yle.fi/uutiset/3-9952035

Mulkahainen, M. 2016. Radiotaajuisen etätunnistuksen tietoturvaongelmat esineiden Internetissä. Kandidaatintyö. Jyväskylän yliopisto. Viitattu 2.2.2020. http://urn.fi/URN:NBN:fi:jyu-201604052010

Near Field Communicationin www-sivut. Viitattu 1.2.2020. http://nearfieldcommunication.org/

NFC-Forumin www-sivut. Viitattu 6.1.2020. https://nfc-forum.org/what-is-nfc/about-the-technology/

Over 20 Billion RFID Tags to be Sold in 2019. 2019. Everything RF News. Viitattu 12.2.2020. https://www.everythingrf.com/News/details/9193-Over-20-Billion-RFID-Tags-to-be-Sold-in-2019

Poliisin www-sivut. Viitattu 25.1.2020. https://www.poliisi.fi/passi/suomen_passien_ominaisuudet

Radiotaajuinen tunnistus eli RFID teollisuuden sovelluksissa. N.D. Sarlin. Viitattu 6.1.2020. https://www.sarlin.com/assets/Tuotteet/liitteet/Radiotaajuinen-tunnistus-eli-RFID-teollisuuden-sovelluksissa.pdf

Raes, C. 2016. Mastercard makes fingerprint and ‘selfie’ payment technology a reality. Viitattu 1.2.2020. https://newsroom.mastercard.com/eu/press-releases/mastercard-makes-fingerprint-and-selfie-payment-technology-a-reality/

Ray, B. 2018. The Complete Active RFID Overview. Viitattu 27.12.2019. https://www.airfinder.com/blog/active-rfid

Readingin yliopiston www-sivut. Viitattu 18.2.2020. http://www.reading.ac.uk/

Resource Labelin www-sivut. Viitattu 6.1.2020. https://www.resourcelabel.com/comparing-different-types-of-rfid-tags/

RFID and the Differences in Passive, Semi-Passive, and Active Tags. 2019. Miller J. Viitattu 3.3.2020. https://www.computype.com/blog/rfid-and-the-difference-in-passive-semi-passive-and-active-tags

RFID Cardin www-sivut. Viitattu 20.1.2020. https://www.rfidcard.com/iso-iec-15693-rfid-cards-standard/

RFID Handbook: Applications… 2008. Syed, A & Mohammad, I. Viitattu 5.2.2020. https://books.google.fi/books/about/RFID_Handbook.html?id=q4aCyZnq0cwC&redir_esc=y

RFIDInEuropen www-sivut. Viitattu 30.12.2019. http://www.rfidineurope.eu/

RFID-Journalin www-sivut. Viitattu 16.12.2019. https://www.rfidjournal.com/

Rouse. ‘challenge-response authentication’ Search Security-blogi. 31.10.2018. Viitattu 5.2.2020. https://searchsecurity.techtarget.com/definition/challenge-response-system

Saeng, S. 2019. The history of RFID technology over the past 80 years. Viitattu 10.12.2019. https://www.medium.com

Savage, M. 2018. Thousands Of Swedes Are Inserting Microchips Under Their Skin. NPR. Viitattu 18.2.2020. https://www.npr.org/2018/10/22/658808705/thousands-of-swedes-are-inserting-microchips-under-their-skin?t=1582622519693&t=1583411768027

Schwartz, O. 2019. The rise of microchipping: are we ready for technology to get under the skin? The Guardian. Viitattu 12.2.2020. https://www.theguardian.com/technology/2019/nov/08/the-rise-of-microchipping-are-we-ready-for-technology-to-get-under-the-skin

Security Analysis of… 2018. Giese, D. Liu, K. Sun, M. Syed, T. & Zhang, L. Viitattu 9.2.2020. https://courses.csail.mit.edu/6.857/2018/project/Giese-Liu-Sun-Syed-Zhang-NFC.pdf

Simonaho, M. 2013. Mobiililaitteiden käyttö maksuvälineenä ja tunnistautumisessa. AMK-opinnäytetyö. Kemi-Tornion ammattikorkeakoulu. Viitattu 30.1.2020. http://urn.fi/URN:NBN:fi:amk-201304224789

Smiley, S. 2014. UHF RFID Frequency Regulations. Viitattu 30.12.2019. https://blog.atlasrfidstore.com/uhf-rfid-frequency-regulations

Smiley, S. 2017. RFID vs. EAS. Viitattu 3.3.2020. https://blog.atlasrfidstore.com/

Smiley. 'Low Frequency RFID and Animal Identification' RFID Insiderin blogi. 15.12.2015. Viitattu 25.1.2020. https://blog.atlasrfidstore.com/low-frequency-rfid-and-animal-identification

Smiley. 'RF Physics: How Does Energy Flow in an RFID System?' AltasRFIDstore-blogi. 5.2.2016. Viitattu 20.12.2019. https://blog.atlasrfidstore.com/rf-physics?utm_source=RFID-Beginners-Guide&utm_medium=eBook&utm_campaign=Content&utm_content=energy-flow

Technovelgyn www-sivut. Viitattu 20.12.2019. http://www.technovelgy.com/

Thrasher. 'A Primer On The Internet of Things & RFID'. AtlasRFIDStore-blogi. 15.1.2014. Viitattu 19.2.2020. https://blog.atlasrfidstore.com/internet-of-things-and-rfid

Toptunnisteen www-sivut. Viitattu 10.12.2019. https://toptunniste.fi/

TraceID:n www-sivut. Viitattu 11.1.2020. http://trace-id.com/en/protocols-and-standards-of-uhf-rfid/

Triggs. 'All you need to know about NFC Tags' Android Authority-blogi. 29.6.2018. Viitattu 4.1.2020. https://www.androidauthority.com/nfc-tags-explained-271872/

Ward, D. 2009. A Brief History of RFID. Viitattu 12.12.2019. http://www.u.arizona.edu/~obaca/rfid/history.html

Wehr, J. 2003. Is the debate still relevant? An in-depth look at ISO 14443 and its competing interface types. Viitattu 15.1.2020. https://www.secureidnews.com/news-item/is-the-debate-still-relevant-an-in-depth-look-at-iso-14443-and-its-competing-interface-types/