



RFID-etätunnistus – mahdollisuudet ja uhat

Heikki Seppä

VTT

heikki.seppa@vtt.fi

Eduskunnan tulevaisuusvaliokunnan julkaisu 9/2011

RFID-etätunnistus – mahdollisuudet ja uhat

Heikki Seppä

VTT

heikki.seppa@vtt.fi

Tulevaisuusvaliokunta
Eduskunta
Puhelin 09 4321
Faksi 09 432 2140
tuv@eduskunta.fi
www.eduskunta.fi

Kansikuva: Wäinö Aaltonen, Tulevaisuus, 1932/1969
Kuva: Vesa Lindqvist, Eduskunta

Helsinki 2011

ISBN 978-951-53-3371-1 (nid.)
ISBN 978-951-53-3372-8 (PDF)

Sisällysluettelo

Esipuhe.....	6
Rfid on tulevaisuuden avainteknologia.....	6
Tiivistelmä	8
Kirjoittajan alkusanat	8
1. Yleistä RFID:stä.....	8
1.1 Toimintaperiaate	8
1.2 Etätunnistepiirien valmistus ja ominaisuudet	9
1.3 Taajuusalueet	10
1.4 Near Field Communication (NFC)	11
1.5 Tiedonsiirtonopeus, muisti ja RFID-järjestelmä	11
2. RFID:n kehitys globaalisti	11
2.1 Historian alkutaival (1940 – 1980)	11
2.2 Kiinnostus lisääntyy (1980 – 1990)	12
2.3 Pioneerivaihe (1990 – 2000).....	12
2.4 Pioneerivaiheesta sovellutuksiin (2000 – 2010)	13
3. Kehitys Suomessa	14
4. RFID-tekniikan sovellutukset.....	16
5. RFID:n yhteiskunnallinen merkitys	17
6. RFID-tekniikkaan liittyvät uhat.....	18
7. Yhteenveto	21

Esipuhe

Rfid on tulevaisuuden avainteknologia

Näpräsin ensimmäisen kerran rfid:n parissa 1990-luvun alussa, kun saattomuistit tulivat kokoonpanolinjoille. Nykyisiin rfid-siruihin verrattuna nuo varhaiset saattomuistit olivat fyysisesti suuria ja muistiltaan pieniä, mutta ne mullistivat koko kokoonpanoteollisuuden.

Saattomuistien ansiosta kokoonpanolinja tiesi, mikä tuote milläkin paletilla oli syntymässä. Samalla linjalla voitiin valmistaa useita erilaisia tuotteita ja tuhansia eri tuoteversioita. Linja kuljetti kunkin paletin saattomuistin tietojen avulla aina seuraavaan työpisteeseen, josta löytyi oikeat osat, työvälineet ja osaava kokoonpanija.

Haasteena oli kokoonpanijoiden osaaminen, sillä jokainen päivän aikana valmistettava tuote saattoi olla erilainen. Linjalle tarvittiin järjestelmä, joka toi työpisteen tietokoneen ruudulle oikeat kokoonpano-ohjeet aina uuden paletin saapuessa.

Kokoonpanolinjojen jälkeen rfid mullisti logistiikan. Rfid-tunnisteiden ansiosta logistiikkajärjestelmät tiesivät jokaisen osan, tuotteen ja kontin sijainnin. Ensin automatisoituivat logistiikkakeskukset ja nyt robottikuljettimet ovat tulossa myös konttiterminaaleihin.

Seuraavaksi rfid on leviämässä kaikille yhteiskunnan sektoreille, mullistamassa esimerkiksi maksamisen, liikenteen ja rakentamisen. Kokoonpanossa ja logistiikassa rfid-teknologiaa hyödynnettiin sellaisenaan esineiden ja ihmisten tunnistamiseen. Todella uusia sovelluksia syntyy, kun rfid-teknologiaa sovelletaan yhdessä muiden teknologioiden kanssa.

Kun rfid-tunnisteisiin yhdistetään paikannus, viestintä, anturit ja laskentakapasiteettia, mahdollisuuksia rajoittaa vain mielikuvitus. Rfid-tunnisteiden valmistus on niin edullista, että käytännössä kaikkiin postimerkkiä arvokkaampiin esineisiin voi ja kannattaa sijoittaa oma siru. Pian esineet tietävät mitä ne ovat, missä ne ovat ja pystyvät myös kertomaan sen. Kylpyhuoneen lattian betoniin kylvetetyt rfid-sirut kertovat, onko rakenteisiin päässyt kosteutta; lihapaketti kertoo kauppiaille sisältönsä olevan pilaantunut; NFC-iPhone tekisi Applesta maailman suurimman luottokorttiyhtiön.

NFC-puhelinten viivästyminen kuvaa hyvin sitä, että rfid:n haasteena ei ole enää niinkään teknologia vaan säännösten ja standardien kehittymättömyys. NFC-teknologia on ollut valmiina jo vuosikymmenen ajan, mutta siihen ei ole standardien ja lakien puuttuessa uskallettu investoida. Suomella ja maailman ensimmäisen NFC-puhelimen markkinoille jo vuonna 2006 tuoneella Nokialla olisi ollut kaikki mahdollisuudet olla edelläkävijä. Nyt maailmalla kuitenkin odotetaan, koska Apple tuo oman NFC-puhelimensa markkinoille ja ottaa maksubisneksen haltuunsa.

Rfid:n kaltaisen strategisen teknologian sääntely on haastavaa, etenkin jos Suomi haluaa olla edelläkävijä, joka ei voi ottaa mallia muualta. Onnistunut teknologian sääntely on toisaalta mahdollisimman kevyttä, jotta se häiritsee teknologian ja sovellusten kehitystä mahdollisimman vähän. Toisaalta lainsäätäjien on osattava ennakoida uuden teknologian potentiaalisia riskejä ja mahdollisuuksia ja löytää niille toimiva tasapaino.

Rfid:n osalta huomio kiinnittyy yksityisyyden suojaan. Kun kaiken voi tunnistaa ja paikantaa, myös ihmisten elämästä tulee läpinäkyvää. Jos esimerkiksi kaupasta ostettavien tuotteiden rfid-tunnisteita

ei neutraloida kassalla, kauppakassin sisällön voi lukea kadulla kuka tahansa. Paraskin tekninen suojaus on kuitenkin vain yhtä hyvä kuin sitä käyttävät ihmiset. Rfid-tunnisteita lukemalla syntyvät tietokannat kiinnostavat paitsi mainostajia myös rikollisia.

Eduskunnan tulevaisuusvaliokunta on ainutlaatuisessa asemassa teknologian arvioinnin ja lainsäädäntötyön rajapinnalla. Tulevaisuusvaliokunnan vastuulla on ennakoida rfid:n kaltaisten yhteiskuntaa muuttavien uusien teknologioiden vaikutuksia ja ohjata niitä koskevaa lainvalmistelua. Se antaa tulevaisuusvaliokunnalle mahdollisuuden ohjata rfid:n sovellusten kehittämistä ja hyödyntämistä Suomessa ja vaikuttaa esimerkiksi myös muiden maiden lainsäädäntöön.

Jyrki J.J. Kasvi

Tiivistelmä

RFID-teknologiaa on hyödynnetty laajasti jo 1980-luvulta lähtien. Kuitenkin 2010-luvulla tapahtuva RFID:n yleistymisen matkapuhelimissa ja toisaalta kulutustavaroissa olevien tunnisteiden yleistymisen laajentaa RFID:n hyödyntämistä merkittävästi. Valitettavasti tulemme kohtaamaan myös yksilön suojaan liittyviä ongelmia. Tässä kirjoituksessa kerrotaan lyhyesti RFID-teknologian tausta, Suomen rooli, nykyiset ja tulevat sovellutukset sekä RFID-teknologian vaikutukset yhteiskunnalliseen kehitykseen. Lopuksi arvioidaan mahdollisia uhkia ja miten niihin on pyritty varautumaan.

Kirjoittajan alkusanat

Oheinen kirjoitus on syntynyt eduskunnan tulevaisuusvaliokunnan pyynnöstä. Raportti ei perustu kirjallisuuskatsaukseen, vaan kirjoittajan pitkäaikaiseen kokemukseen alalta. Olen työskennellyt RFID-teknologian alalla vuodesta 1992 ja tehnyt yhteistyötä kaikkien suomalaisten RFID-teknologiaa kehittävien yritysten kanssa. Useissa tapauksissa jo paljon aikaisemmin ennen kuin yritykset ovat varsinaisesti sitoutuneet teknologiaan. Esimerkiksi aloitimme yhteistyön UPM:n kanssa vuonna 1994 ja RFID-teknologiaan erikoistunut yritys UMB Rafsec perustettiin vasta 1997. Nokian kanssa aloitimme keskustelut RFID:n integroimisesta puhelimeen jo 1990-luvun puolessa välissä, mutta ensimmäinen NFC-puhelin ilmestyi vasta 2004. Useissa tapauksissa monet tulevaisuuden teknologiat kypsyvät yritysten tuotekehitysosastoilla joskus jopa kymmenen vuotta ennen kuin ne lopullisesti tuotteistuvat. Innovaatiot eivät synny julistuksista vaan visioista ja sitkeästä ja pitkäjänteisestä työstä niiden saavuttamiseksi. Raportissa on myös ennustuksia tulevista sovellutuksista ja osa näistä on sellaisia, joita ei ole aikaisemmin tuotu missään esille.

1. Yleistä RFID:stä

1.1 Toimintaperiaate

RFID tulee sanoista Radio Frequency Identification, mutta käytämme tässä yhteydessä myös sanaa etätunniste. Tyypillisesti RFID jaetaan passiivisiin, semipassiivisiin ja aktiivisiin etätunnistimiin, mutta koska aktiivinen RFID on usein normaalin radion tapaan toimiva etätunniste, sitä ei käsitellä tässä kirjoituksessa erikseen. RFID-sana ei historiallisista syistä kuvaa hyvin sen ominaisuuksia. Ne suunniteltiin alun perin erittäin lyhyen etäisyyden pienen tietomäärän tunnistamiseen. Radiotekniikassa RF viittaa n. 100 kHz taajuuteen, mutta nykyiset tunnisteet käyttävät paljon suurempia taajuuksia. On hyvin tärkeä ymmärtää, että nykyaikaisia RFID-tunnisteita ei pidä verrata viivakoodeihin. Parempi vertailukohta on oikeastaan radio, joka pystyy tarvittaessa tiedon keräämiseen, prosessointiin ja salaamiseen ja se voi sisältää musiikkikappaleen verran muistia. Siihen voi liittää näytön, antureita ja jopa näppäimistön.

Etätunnistus voidaan toteuttaa myös optisesti viivakoodilla (Suomessa käytetään yleisesti EAN-koodia) ja viime aikoina yleistyneellä matriisikoodauksella, joka on yleistynyt matkapuhelimissa olevien kameroiden myötävaikutuksella. Kaupat ovat ottamassa usean perinteisen viivakoodin yhdistelmän, jolla tuote voidaan yksilöidä. Nykyiset kaupan laserpohjaiset lukulaitteet pystyvät lukemaan nämä koodit, joten laajennetut viivakoodit tulevat yleistymään nopeasti. Logistiikassa ja liikenteessä käytetään myös muita optisesti helposti tunnistettavia koodeja ja tietysti autojen rekisteri-

kilpiä. On oleellista huomata, että RFID ei uhkaa viivakoodin asemaa ainakaan puhuttaessa päivittäistavaroiden merkkämisestä.

Jos RFID-tunnisteessa ei ole erillistä virtalähdettä, sitä kutsutaan passiiviseksi etätunnisteeksi. Tässä tapauksessa etätunniste ottaa tarvitsemansa energian lukijalaitteen synnyttämästä kentästä. Tällä hetkellä suurin osa etätunnisteista on passiivisia. Semipassiivinen etätunniste sisältää patterin tai ladattavan akun, joka mahdollistaa pidemmän lukuetaisyyden ja toiminnan ilman lukulaitteen tuottamaa energiaa. Semipassiivinen tunnistee ei kuitenkaan ole itsenäinen radio, joten se ei voi lähettää radioteitse tietoa ilman lukulaitetta. Semipassiivisten tunnisteen rooli lisääntyy, kun RFID-tunnisteisiin lisätään antureita. Näitä tullaan hyödyntämään logistisen ketjun laadunvalvonnassa, kiinteistöjen ja rakenteiden kunnonvalvonnassa sekä jatkossa ihmisten terveyden seuraamiseen.

Etätunniste on heijastusperiaatteeseen perustuva kommunikointimenetelmä, missä lukulaite lähettää kantoaallon tai moduloidun kantoaallon ja kuuntelee samaan aikaan tai välittömästi moduloinnin jälkeen etätunnisteen moduloimaa signaalia. Lähettimen modulaatio on aina amplitudimodulaatiota, mutta etätunnistin voi moduloida joko amplitudia tai vaihetta. On myös oleellista, että lukulaitteeseen saapuva heijastuneen signaalin taajuus on sama kuin lähetetty, joten ilmaisussa voidaan käyttää vaihelukitustekniikkaa, joka parantaa signaali-kohinasuhdetta merkittävästi. Radiotaajuuden ominaisuuksista johtuen tunnistee voidaan lukea, vaikka siihen ei ole näköyhteyttä. Kahden viimeksi mainitun ominaisuuden suhteen RFID poikkeaa optisesta tunnistuksesta.

Vaikka tunnistee voidaan lukea vain lyhyeltä etäisyydeltä, voidaan lukijan lähettämää tietoa kuulella hyvinkin kaukaa. Ne myös häiritsevät toisiaan. Tämä piirre on otettu standardeissa huomioon hiukan samaan tapaan kuin muissakin langattomissa järjestelmissä. Toisin sanoen lukulaitteen datan siirto etätunnisteelle on tästä näkökulmasta hyvin helppo kaapata. Lähetesignaali ei tietysti pidä sisällään etätunnisteen tietoja, joten tämän ominaisuuden väärinkäyttömahdollisuudet ovat vähäiset.

1.2 Etätunnisteipiirien valmistus ja ominaisuudet

Heijastusperiaatteella toimiva ”radio” voidaan toteuttaa yhdellä luokkaa 0.25 mm² kokoisella CMOS-pohjaisella piisirulla. Piisiru voidaan valmistaa ”vanhanaikaisella” 0.35 – 0.6 mm viivanleveyden omaavalla prosessilla. Näin puolijohdevalmistajat voivat käyttää vanhoja tuotantotilojaan ja laitteitaan niiden valmistamiseen. Halvimmillaan tällaisen piisirun valmistuskustannukset ovat n. 0.01 €/luokkaa. Etätunnistin edellyttää tietysti myös antennin ja tarralaminaatin, jolloin tuotantohinta on halvimmillaan n. 0.03 €. Tällä hetkellä suurina erinä markkinahinta on noin 0.05 €. Edullinen hinta ja mahdollisuus toimia ilman erillistä teholähdettä ovat syyt siihen, miksi RFID-teknologian merkitys on niin suuri ja voimakkaasti kasvava lyhyen etäisyyden kommunikoinnissa. Etätunnistimen koko on aina riippuvainen antennista eikä koskaan mikropiiristä. Suurtaajuusantenni voidaan kyllä integroida mikropiiriin, mutta lukuetaisyys jää äärimmäisen lyhyeksi. On tärkeä huomata, että pitkän lukuetaisyyden tunnistee tulee olemaan aina suuri (min. 1 cm x 3 cm) ja tässä mielessä aina havaittava. Pienimmät HF-tunnisteet ovat luokkaa 2,5 x 2,5 cm. Etätunniste voidaan tehdä erittäin ohueksi (0,1 mm), joten se voidaan haudata tuotteeseen siten, että asiakas ei sitä välttämättä huomaa. Viimeaikoina jopa ihmisten ihon alle on asennettu RFID-tunnisteita, mutta johtuen antennin pienuudesta (yleensä integroitu suoraan osaksi mikropiiriä), niiden lukeminen edellyttää lähes ihoon koskettamista.

Etätunniste tulee lähtökohtaisesti mieltää muistipiiriksi, jonka tietosisältö voidaan lukea ja sitä voidaan muuttaa langattomasti. Standardinmukainen mikropiiri valmistetaan siten, että siinä on aina pysyvä muisti, jota ei voi jälkepäin muuttaa. Tämä tarkoittaa sitä, että kahta samanlaista etätun-

nistetta ei periaatteessa ole. Tämän lisäksi tunnistetta hyödyntävä yritys voi kirjoittaa tunnisteseen yksikäsitteisen esim. tuotteeseen liitettävän lukitun koodin. Kiinteästi ohjelmoitavan koodin pituus on niin suuri (esim. 96 bittiä = n. 10^{29} erilaista koodia) että jokainen yksittäinen maailmassa valmistettu tuote voidaan merkitä erillisellä koodilla. Lähes aina piiri sisältää uudelleen kirjoitettavissa olevaa muistia, joka vaihtelee sovellutuksesta riippuen. Muistin lukeminen ja kirjoittaminen edellyttää aina salasanan ja tiedon kryptauksen, mutta salauksen turvallisuustaso vaihtelee hyvin paljon standardista ja sovellutuksesta riippuen. Esim. auton avaimissa käytetään turvallisuuden lisäämiseksi myös ns. vaihtuvaa salasanaa. Logistiikassa käytössä olevat EPC- (Electronic Product Coding) standardin mukaiset tunnistet edustavat salausmielessä matalinta tasoa, kun taas esim. maksamiseen tehty NFC (Near Field Communication) sisältää erittäin tehokkaan salausjärjestelmän.

1.3 Taajuusalueet

Jos taajuus on matala etätunnistimen ja lukijan väliseen etäisyyteen nähden, puhutaan ns. lähikenttätilanteesta. Päinvastaisessa tilanteessa puhumme säteilykentästä. Toinen tapa jakaa etätunnistimet eri luokkiin on tarkastella käytettyä taajuutta. Koska taajuudet ja kentänvoimakkuudet ovat viranomaistahoilta säädeltyjä, käytännössä etätunnistimet toimivat neljällä eri taajuusalueella: LF (Low Frequency) alue: 100 kHz – 250 kHz, HF (High Frequency): 13.56 MHz, UHF (Ultra High Frequency): alin 865 MHz (Eurooppa) ja suurin 950 MHz (Japani) sekä mikroaaltoalue (MW, Micro-wave Frequency): 2.54 GHz. Viimeksi mainittuja etätunnisteita ei ole maailmanlaajuisesti standardoitu ja mitä ilmeisimmin sitä ei myöskään oteta laajamittaisesti käyttöön. Tärkeimmät ja kasvavimmat teknologiat tällä hetkellä ovat passiiviset HF- ja UHF-teknologiat sekä jatkossa NFC. Sekä HF- että UHF-alueella toimivia etätunnistimia koskevat viestintäviranomaisten määrittelemät säännöt. Alan kehityksen ja yritysten kannalta standardoinnilla on kuitenkin keskeinen merkitys. HF:n ja UHF:n merkitys onkin lisääntynyt viime aikoina, koska molemmille etätunnisteille on rakennettu standardeja. Käytännössä tilanne on ollut tietysti päinvastainen. Sekä HF- että UHF-etätunnisteet ovat osoittaneet toimivuutensa ja niille on löydetty tätä kautta paljon potentiaalisia sovellutuksia. Tämä kehitys on pakottanut yritykset hakemaan näille tekniikoille yleistä hyväksyntää standardien avulla. Standardoinnissa foorumina on toiminut pääosin ISO ja näiden päälle on rakennettu UHF:lle Gen2 ja EPC (Electronic Product Coding) ja HF:lle esim. NFC (Near Field Communication). Tällä hetkellä esim. maksamiseen ollaan tuomassa uusia standardeja. On kuitenkin huomattava, että sekä uusia viranomaismääräyksiä että taajuuksia on koko ajan tulossa lisää ja standardointiprosessit ovat joiltakin osin vielä kesken. Erityisesti RFID-antureihin liittyvä standardointityö on kesken, mutta se ei kuitenkaan ole este alan kehittymisen kannalta (RFID-antureita käytetään jo esim. kylmäkuljetuksissa). Tämä johtuu siitä, että myös RFID-antureissa tiedonsiirto hoidetaan joko HF/NFC tai EPC-standardeja hyödyntäen.

Oleellista HF:n osalta (koskee myös NFC:tä) on se, että sama taajuus on kaikkialla maailmassa käytävissä kun taas UHF:llä joka maanosassa on poikkeavat taajuudet. Laajakaistainen antenni (esim. dipoli) voi toimia kohtuullisesti koko taajuusalueelle, mutta matalat metallin päällä toimivat siirtolinjatyypiset antennit ovat aina niin kapeakaistaisia, että ilman hajaviritystä niitä ei saa toimimaan kaikilla mantereilla. Ongelmaan on tulossa kuitenkin osittain ratkaisu sitä kautta, että Kiinassa otetaan käyttöön kaksi taajuutta, joista toinen lähellä Eurooppaa ja toinen USA:n taajuus- aluetta. Eurooppa on myös tuonut toisen taajuuden USA:n taajuuden sisälle. Nämä toimenpiteet tulevat helpottamaan globaalisten etätunnistimien soveltamista UHF-alueella.

1.4 Near Field Communication (NFC)

Tällä hetkellä puhutaan paljon ns. NFC-tekniikasta. Periaatteessa NFC ei ole mitään muuta kuin RFID-lukija matkapuhelimessa. NFC on kuitenkin uutta siinä mielessä, että NFC-moduli kykenee simuloimaan sekä tunnistinta että RFID-lukijaa. Esim. liputtamisessa matkapuhelin toimii nykyisen sähköisen matkalipun tavoin etätunnisteena ja voi toimia ilman matkapuhelimen akkua. Maksamisessa tilanne on hiukan samankaltainen. Myös kahden puhelimen välinen RFID-kommunikointi on mahdollinen. Vaikka NFC on suunniteltu ajatellen RFID-soveltamista matkapuhelimessa, sen käyttö laajenee myös sovellutuksiin, missä lukulaite voi olla jokin muu kuin matkapuhelin. Vaikka teknologisesti NFC on hyvin samanlainen kuin HF, on standardissa rajattu lukutehot siten, että luenta onnistuu vain 4 cm päähän. Kuten aikaisemmin mainittiin, lukulaitteen synnyttämä signaali voidaan silti kuulla jopa metrin päähän. Koska NFC on suunniteltu muiden sovellutusten lisäksi liputtamiseen ja maksamiseen, tiedon suojaamiseen on kiinnitetty erityistä huomiota.

1.5 Tiedonsiirtonopeus, muisti ja RFID-järjestelmä

Tiedonsiirtonopeus ja etätunnisteessa oleva muistin määrä ovat luonnollisesti hyvin ratkaisevia tekijöitä sovellutusten näkökulmasta. On tutkittu, että kuluttaja koskee tunnistetta luontevasti vain yhden sekunnin ajan. Logistiikassa vasteaika täytyy olla vain 1 ms-luokkaa, koska yksi lukija voi joissakin tapauksissa lukea jopa tuhat erillistä tunnistetta samaan aikaan. Logistiikassa käytetään mikropiirin yksilöimiseen liittyvän koodin lisäksi aina vähintään 96 bittinen ID-numero, joka riittää erottelemaan jokaisen maailmassa tuotetun tuotteen. Usein myös logistiikassa käytetyissä tunnisteteissa on vähintään 2 kbitin lisämuisti. Riippuen sovellutuksesta, NFC:ssä muisti vaihtelee sadoista biteistä aina miljooniin bitteihin asti. Vasta kun yhdistämme esim. UHF-tekniikan energiansyötössä ja laajakaistaisen (UWB) tiedonsiirron etätunnisteesta lukijalle, pääsemme nopeuksiin, jotka mahdollistaisivat jopa videon siirtämisen passiivisesta etätunnisteesta matkapuhelimeen. Tätä tekniikkaa hyödyntäen Nokia on tehnyt sovellutuksen, missä matkapuhelimen ohjelmisto ladataan myymälässä akun tilalle laitettavaan etätunnisteeseen ja sitä kautta matkapuhelimen muistiin. On huomattava, että yleisesti RFID-tekniikassa muisti ei ole rajoittava tekijä vaan tiedonsiirtonopeus. On myös RFID-piirejä, joissa on digitaalinen väylä. Tämä mahdollistaa hyvinkin monimutkaisen mikroprosessorin ohjaaman elektroniikkajärjestelmän kehittämisen, jonka tehonsyöttö tulee lukulaitteelta RFID-rajapinnan kautta.

2. RFID:n kehitys globaalisti

Olemme jakaneet RFID:n historiallisen kehityksen viiteen osaan: historian alkutaival (1940 – 1980), kiinnostus lisääntyy (1980 – 1990), pioneerivaihe (1990 – 2000) ja pioneerivaiheesta sovellutuksiin (2000 – 2010).

2.1 Historian alkutaival (1940 – 1980)

RFID juontaa juurensa toiseen maailmansotaan ja tutkan kehittymiseen. Tutka mahdollisti lentokoneiden havaitsemisen, mutta oman tai viholliskoneen erottaminen toisistaan ei onnistunut. Hyvin nopeasti tutkan kehittymisen jälkeen lentokoneisiin laitettiin erillinen antenni ja modulaattori koneen tyyppin tunnistamiseksi. Tätä tunnistintyyppiä kutsuttaisiin nykykielellä pitkän lukuetaisyden

semipassiiviseksi RFID-tunnisteeksi. Vuonna 1948 Harry Stockman julkaisi artikkelin ”Communication by Means of Reflected Power”, jota voidaan pitää ensimmäisenä tieteellisenä työnä RFID:stä. Neuvostoliitossa RFID:tä sovellettiin jo vuodesta 1945 vakoilukäytössä.

Seuraava merkittävä kehitysaskel oli passiivisen etätunnistimen käyttöönotto. Tätä kehitystä vauhditti merkittävästi autentikointisovellukset, joista tärkein oli eläinten merkkäämien ruokinnan automatisoimiseksi. Toinen tärkeä sovellutus oli autojen käynnistyksen esto, joka perustuu RFID-tunnisteen omaavaan avaimen ja auton lukkopesässä olevaan lukijaan. Ensimmäiset passiiviset RFID-tunnisteet olivat induktiivisia eli magneettikenttään perustuvia ja toimivat taajuusalueella 100 kHz– 250 kHz. Semipassiivisten etätunnisteiden historia voidaan katsoa alkavaksi 40-luvulta, mutta passiivisten etätunnisteiden aika alkaa vasta 80-luvulta. Tämä yksinkertaisesti siksi, että passiiviset etätunnisteet tulivat mahdolliseksi vasta CMOS-tekniikan kehityksen myötä. Eli voidaan sanoa, että vaikka passiivista RFID:tä ei keksitty 80-luvulla, se pystyttiin järkevästi realisoimaan vasta 80-luvulla. Historian alkutaival tuotti kolme merkittävää innovaatiota: heijastusperiaatteella toimivan kommunikoinnin, CMOS-pohjaisen passiivisen RFID-piirin, joukon RFID-tekniikkaa hyödynnäviä sovellutuksia, kuten auton avain. LF-taajuisia tunnistimia sovellettiin myös tuotantoautomaatioon jo hyvin varhain, mutta varsinaista läpimurtoa ei vielä kuitenkaan tapahtunut.

2.2 Kiinnostus lisääntyy (1980 – 1990)

Kun passiivinen RFID osoittautui toimivaksi teknologiaksi, CMOS-tekniikka kehittyi edelleen ja RFID vakiinnutti asemansa mm. autojen käynnistyksen estossa ja eläinten merkkääminen etätunnisteiden avulla yleistyi. RFID:n käyttö yleistyi myös tuotantoautomaatiossa. Vaikka etätunnisteita ryhdyttiin soveltamaan yhä enenevässä määrin, kehitys oli kohtuullisen hidasta. Tärkein syy oli tekninen: LF-taajuiset RFID-tunnisteet edellyttivät usean kierroksen omaavan lankakäämin ja tästä johtuen etätunnisteet olivat hyvin kalliita. Lukuetaisyys jäi myös hyvin lyhyeksi, joten sitä ei voinut soveltaa kuin rajatussa määrässä sovellutuksia.

Voidaankin sanoa, että 80-luku oli orastavan RFID-tekniikan kokeiluvuosikymmen, jonka aikana huomattiin tekniikan rajoitukset ja sen liian korkea hinta. Kuitenkin tietyissä erityissovellutuksissa se löi itsensä lopullisesti läpi ja tätä kautta synnytti paineen uuden (HF) tekniikan kehittämiseksi. Innovaatiomielessä 80-luku oli vaatimaton, mutta se oli välttämätön pioneerivaihe, joka herätti kiinnostuksen tekniikkaan ja kokeilujen kautta näytti tietä eteenpäin.

2.3 Pioneerivaihe (1990 – 2000)

Koska LF-tekniikka oli kallis ja standardeja ei ollut, syntyi paine kehittää HF-tekniikka. Tiedettiin, että taajuutta nostamalla voidaan lankakäämi korvata muutaman kierroksen omaavalla etsaamalla valmistetulla antennilla. Jo 80-luvun lopussa oli kehitetty 8 MHz:n taajuudella toimivia LC-resonanssiin perustuvia ”varasantureita”. Näiden tuotantoa varten oli kehitetty rullalta rullalle toimivia etsauksen perustuvia prosesseja. Yhdistämällä ”varasantureiden” antennituotantotekniikka ja RFID-mikropiiri, etätunnistimien hintaa voitiin merkittävästi alentaa. Näin tehty tarramainen etätunniste voidaan helposti kiinnittää esim. pakkausten pintaan. Se mahdollistaisi myös ohuet ja edulliset sähköiset liput, kulkukortit jne. Uudeksi RFID-taajuudeksi vakiintui 13.56 MHz HF:n käyttöönotto ei vain alentanut etätunnistimien hintaa, vaan lukuetaisyys voitiin kasvattaa noin 10 cm:stä 50 cm:iin asti. Porttimaisella rakenteella päästiin jopa 1 m:n lukuetaisyyteen. HF-taajuutta käytetään kaikkialla maailmassa ja sen ympärille on syntynyt useita ISO-standardeja.

Kun HF otettiin käyttöön, kuviteltiin sen mahdollistavan tunnistamisen, lippujen ja kulunvalvonnan lisäksi myös tekniikan logistiikan sovellutuksiin. Tämä ei kuitenkaan lähtenyt etenemään toivotulla tavalla. Vaikka RFID-tekniikka oli HF:n osalta standardoitu, muistista ja numeroinnista ei kuitenkaan ollut globaalia sopimusta. Kuviteltiin, että jos HF:n muistiavaruudesta päästäisiin sopimukseen, HF:n ja sitä kautta RFID:n käyttö laajenisi. Eli jälleen syytettiin standardoinnin puutetta epäonnistumisesta. Tämä saikin aikaan sen, että amerikkalaisen teollisuuden aktivoimana MIT (Massachusetts Institute of Technology) perusti AutoID Centerin vuonna 1998. Tehtäväksi asetettiin globaalin numerointijärjestelmän synnyttäminen. Tästä sai alkunsa kaikkien alalla toimivien tuntema lyhenne EPC (Electronic Product Coding). Suomesta UBM Rafsec on ollut alusta lähtien mukana määrittelemässä EPC-standardia.

Digitaalisten matkapuhelimien yleistymisen kautta syntyi mahdollisuus integroida RFID-lukija matkapuhelimeen. Oli helppo nähdä ne valtavat mahdollisuudet, joita RFID ja matkapuhelimen sulautuminen mahdollistaisivat. On kuitenkin aivan eri asia tuoda matkapuhelimeen RFID-lukija kuin tuoda siihen kamera, FM-radio, nettipalvelut jne., koska nämä sovellutukset eivät edellyttäneet uuden ekosysteemin rakentamista. Ajatus puhelimen ja RFID:n yhdistämisestä fyysisen käyttöliittymän välineeksi on todennäköisesti syntynyt ensimmäisenä Suomessa, mutta japanilaiset realisoivat NFC:tä vaatimattomamman ratkaisun nimeltään Felica hiukan aikaisemmin 2002 – 2003.

Ehkä merkittävin 90-luvun tulos oli HF:n syntyminen ja siihen liittyen etsäamalla tehtyjen antennien tuotanto tehokkaasti rullalta rullalle. 1990-luku synnytti myös pitkän lukuetaisyyden UHF-tekniikan, mutta sen taloudellinen merkitys jäi vähäiseksi. UHF-antennit valmistettiin jo tuolloin samalla tekniikalla kuin HF-antennit. Matkapuhelimien yleistymisen ja RFID-tekniikan kehitys synnytti 90-luvulla vision näiden tekniikoiden yhdistämisestä.

2.4 Pioneerivaiheesta sovellutuksiin (2000 – 2010)

HF oli kypsä ja standardoitu teknologia. UHF oli osoitettu toimivan logistiikan sovellutuksissa. AutoID Center ryhtyi HF:n sijaan standardoimaan UHF-tekniikkaa logistiikkasovellutuksiin. Koska pyrittiin erittäin halpaan ratkaisuun, standardoinnin keskeinen tavoite oli minimoida muistin määrä ja lopuksi päädyttiin 96 bittiseen standardiin, joka katsottiin riittävän jokaisen maailmassa myytävän lavan, pakettin ja tuotteen merkkäämiseen. Toinen tärkeä tavoite oli se, että yksi lukulaite pystyy lukemaan useita tunnisteita (jopa tuhat) samaan aikaan. Pääpaino ei ollut lisämuistissa eikä tiedon salauksessa. Tämä oli ymmärrettävää, koska tavoitteena oli halpa ja kertakäyttöinen tunnistelogiikka sovellutuksiin.

AutoID Centerin työn lisäksi toinen merkittävä seikka oli, että amerikkalainen kauppaketju Wal-Mart aloitti laajamittaiset RFID-testit 2002 – 2004. Tämän jälkeen Wal-Mart ilmoitti haluavansa kaikkiin heille toimitettaviin lähetyksiin UHF RFID-tunnisteet ja vähän myöhemmin EPC julkistettiin. Nämä kaksi tapahtumaa synnyttivät todellisen buumin: RFID-teollisuus ryhtyi liputtamaan UHF:n puolesta ja ympäri maailmaa käynnistyi useita pilotteja. EPC-standardin mukaisia etätunnistimia ryhdyttiin laajamittaisesti tutkimaan erilaisissa logistisissa ongelmissa ja sekä auto- että lentokoneteollisuus käynnisti useita pilotteja kuljetusalustojen, laitteiden osien jne. merkkäämiseksi. Standardin tuleminen oli toisaalta myös ongelma, koska useat yritykset jäädyttivät useita RFID-pilotteja ja jäivät odottelemaan EPC-standardin mukaisia edullisia etätunnisteita. Vasta 2006 – 2007 EPC-standardia ryhdyttiin käyttämään laajamittaisesti.

2000-luvulle tultaessa HF oli jo vakiinnuttanut asemansa esim. kulunvalvonnassa ja matkalipuissa. Myös kirjastot ryhtyivät soveltamaan HF-tekniikkaa. UHF:n aseman vahvistuminen vaikutti hid-

tavasti HF:n soveltamiseen logistiikassa. Nokia päätti 2000 – 2001 tuoda puhelimeen HF-tekniikkaan perustuvan lukijan matkapuhelimiin. NFC Forum perustettiin vuonna 2004 Nokian aktiviteetin tuloksena. NFC:ssä yhdistettiin eri standardeja ja siinä huomioitiin alusta alkaen tiedon salaus, jotta sitä voitaisiin käyttää myös maksamisessa. Tällä tasoitettiin tietä sille, että matkapuhelin voisi myöhemmin korvata pankkikortin maksamisvälineenä. Japani oli noin 2 vuotta Suomea edellä. Teleoperaattori DoCoMo:n ja Sonyn johdolla julkistettiin Felica-tekniologia. Felica ei tue kaikkia NFC:n piirteitä ja voidaankin sanoa, että NFC on edistyneempi. Syy, miksi Japanissa kaupallistuminen tapahtui Eurooppaa nopeammin, liittyy lähinnä siihen, että toisin kuin Euroopassa, Japanissa operaattoreiden valta valmistajiin nähden on suurempi.

1990-luvulla opittiin valmistamaan kohtuullisen edullisesti sekä HF- että UHF-antenneja etsaamalla rullalta rullalle. Etsaaminen pyrittiin korvaamaan joko metallin kasvattamisella tai painamalla, jotta päästäisiin eroon alumiinin aiheuttamasta jäteongelmasta. 2000-luvulla tehtiinkin jo aimo harppaus, kun metallipartikkeleita valmistavat yritykset keksivät pallomaisten partikkeleiden ohessa valmistaa hiutalemaisia hopeahiukkasia, jotka painovaiheessa ja prässäyksessä johtivat kohtuullisen hyvään lopputulokseen. Näin valmistetun hopean johtavuus jää n. 20 – 40 kertaa ideaalista hopeaa huonommaksi, mutta on täysin riittävä UHF-antennin tuottamiseen. Etsaamiseen liittyvään jäteongelmaan keksittiin ratkaisu, kun alumiinioksidia sisältävälle jätteelle löytyi hyötykäyttöä. Käytännössä etsaaminen on tällä hetkellä edullisin tapa antennien tuottamiseksi, mutta kun nykyisen tarralaminaatin sijaan etätunnisteen antenni ”painetaan” suoraan pakkauksen pintaan, painotekniikoiden merkitys tulee korostumaan.

2000-luku on RFID-historian merkittävin vuosikymmen. Passiivinen HF ja UHF vakiinnuttivat asemansa. HF synnytti NFC- ja UHF EPC-standardit. 2000-luku jätti jälkeensä tietysti paineen näiden teknologioiden konvergenssista. Laitetaanko jatkossa tuotteisiin piiri, joka tukee sekä HF/NFC-että UHF/EPC -standardeja, vai sisältääkö lukulaite molemmat lukijat? Pitäisikö muistiavaruus ja sen käyttö standardoida riippumatta käytetystä taajuudesta? Molempien ympärille on rakennettu anturirajapintoja ja antureita, mutta standardit puuttuvat. Miten UHF-antenni, joka toimii metallin päällä, voidaan valmistaa alle 0.1 €n kustannuksella? Nämä ja monet kysymykset saavat lopullisen ratkaisunsa vasta 2010-luvulla.

3. Kehitys Suomessa

Vuonna 1989 perustettiin Idesco Oy Rautaruukki Oy:n toimesta. Yrityksen lähtökohta oli RFID-tekniologia ja sen sovellutukset. Tuolloin LF RFID (LF = Low Frequency) oli jo vakiinnuttanut asemansa muutamissa sovellutuksissa ja oli osoittanut toimivuutensa. Suomessa 1980-luvun puolivälissä saattomuisti (tätä nimikettä käytettiin 1980-luvulla) tuli kaupallisesti saatavaksi ja tuolloin sovellutusalueena olivat teollisuuden kuljetinjärjestelmät. Selviä mahdollisia sovellutuksia olivat eläinten ja metalliesineiden merkkäminen (poranterät), matkaliput, kulunvalvonta jne. Idescon aloite johtikin oululaiseen RFID-keskittymään. Pian Idescon perustamisen jälkeen Buscom Oy ryhtyi kaupallistamaan RFID-tekniikkaa matkalipuissa ja Oulu olikin ensimmäinen kaupunki maailmassa, missä RFID:tä sovellettiin julkisessa liikenteessä. Toisaalta Securitas Oy lähti kaupallistamaan etätunnistimia kulunvalvonnassa. Oleellista tässä vaiheessa oli se, että etätunnistimien tekniologia lisensoitiin ulkomailta ja sillä nähtiin ilmeisiä lyhyen aikavälin sovellutusmahdollisuuksia.

UPM Raflatac kiinnostui RFID teknologiasta noin 1994 ja lähti kehittämään rullalta rullalle tuotantolinjaa. Vuonna 1996 UPM perusti RFID-tuotantoon suuntautuvan yrityksen nimeltään UPM Rafsec, joka 2000-luvun puolenvälän jälkeen sulautettiin uudestaan osaksi UPM Raflatacin liiketoimin-

taa. Suomen kannalta UPM:n sitoutuminen RFID-tekniikkaan on ollut koko alan kannalta ratkaisevan tärkeää. Suurena yrityksenä UPM toi alalle uskottavuutta ja monet muut suomalaiset yritykset lähtivät kartoittamaan RFID-tekniikan merkitystä omassa liiketoiminnassaan. Voidaankin sanoa, että yrityksistä Idesco toi RFID-tekniikan Suomeen, mutta UPM Rafsecin toimesta siitä tuli pysyvä osa suomalaista teollisuutta. Ainoana tutkimuslaitoksena VTT on ollut mukana lähes kaikkien suomalaisten RFID-yritysten tuotekehityksessä alusta lähtien.

Jo 1990-luvun puolessa välin Nokia oli hyvin tietoinen VTT:n aktiivisuudesta alalla. 1990-luvun lopulla he ryhtyivät kartoittamaan RFID:n mahdollisuuksia puhelimen yhteydessä ja vuonna 2001 he tekivät päätöksen tuoda markkinoille RFID-puhelin, joka julkaistiin vuonna 2004. Tuolloin RFID-piiri ja -antenni oli asetettu matkapuhelimen kuoreen. Vuonna 2005 he julkaisivat puhelimen, missä piiri oli integroitu puhelimen alustaan, mutta ohjelmisto oli rakennettu Symbian päälle. Nokian aloitteesta vuonna 2005 perustettiin NFC foorumi, jonka tarkoituksena oli standardoida RFID-teknologia matkapuhelinympäristössä. Nämä alkuajan puhelimet oli tehty lähinnä pilottiprojekteja varten, joita Nokia on tehnyt yli sata ympäri maailmaa – viime aikoina hyvin vähän Suomessa. Nyt kun lähes kaikki maailman matkapuhelinyhtiöt ovat julkaisseet NFC-puhelimet, ovat amerikkalaiset operaattorit olleet erittäin aktiivisia palveluiden kehittämisessä ja niistä tiedottamisessa. Yhdysvaltojen sisällä on myös syntynyt riita siitä, tuleeko jatkossa puhelimiin perinteisen sim-kortin lisäksi toinen sim-kortti maksamiseen ja muihin palveluihin. Vastakkain ovat toisaalta Google (kaksi sim-korttia) ja toisaalta amerikkalaiset operaattorit (yksi sim-kortti). On todennäköistä, että yhden kortin ratkaisu voittaa, koska se on korttien jakelukustannusten ja puhelimien tuotantokustannusten kannalta edullisempi vaihtoehto. Myös kuluttajan kannalta on helpompi, että yksi kortti riittää ja siihen voidaan ladata kaikki asiakkaan haluamat palvelut.

Noin vuonna 1987 – 2000 VTT kehitti yhdessä Atmelin kanssa maailman ensimmäisen pitkän luetäisyyden RFID-piirin. Nykyisillä sallituilla tehoilla etäisyys vastaa noin 6 metriä. Suomesta projektiin osallistuivat alusta alkaen Idesco Oy ja myöhemmin hankkeeseen liittyi UPM Rafsec. Projektin merkitys kansainvälisestäkin katsottuna oli se, että ensimmäistä kertaa osoitettiin, että UHF-taajuuksilla voidaan päästä luetäisyyteen, joka on riittävä logistiikkasovellutuksia silmälläpitäen. Logistiikkaan suunniteltu EPC- (Electronic Product Coding) standardi perustuu UHF-tekniikkaan ja se julkistettiin vuonna 2004.

2000-luvulla Suomeen syntyi useita uusia yrityksiä RFID:n teknologian ympärille. Myös monet jo olemassa olevat yritykset ottivat tuotevalikoimaansa RFID-teknologian. Esimerkkinä voidaan mainita NordicID, joka on tällä hetkellä Euroopan suurin käsipäätteiden toimittaja. 2007 perustettu Confidex on maailman johtava korkealaatuisten etäluettavien matkalippujen ja RFID-tunnisteratkaisujen ja -palveluiden tarjoaja. Se on myös tällä hetkellä Suomen kasvavin yritys ja Euroopassakin sijalla kuusi. UBM on ollut jo pitkään maailman suurin etätunnistimien tuottaja ja Savcor (Suomessa perustettu yritys, joka on pörssinoteerattu Australiassa) on maailman suurin RFID-antennien tuottaja. Mukana oli vanhoja yrityksiä kuten Finn ID ja merkittävänä uutena pelaajana mukaan tuli mm. Electrobit Oy. Useat suomalaiset Nokian alihankkijat vedettiin NFC:n myötä mukaan RFID-liiketoimintaan. Sascen (aikaisemmin tunnettiin nimellä Botnia Hightech) teki sulautettuja ohjelmistoja NFC-moduleille ja Perlos integroi antennin Nokian ensimmäisiin NFC-puhelimiin.

UPM Rafsec, Tyco ADT (USA) ja suomalainen Salpomec aloittivat yhteistyön n. 2007 järjestelmien kehittämiseksi vaateteollisuudelle. Vaateteollisuus on viime vuosina ollut ylivoimaisesti kasvavin yksittäisissä tuotteissa käytettävien tunnistimien hyödyntämisessä. Stora Enso on myös viime aikoina aktivoitunut RFID-tekniikassa ja he ovat tuoneet sitä mm. lääkepakkauksiin. He ovat myös tuoneet markkinoille painettua elektroniikkaa ja RFID-tekniikkaa hyödyntäviä ratkaisuja, missä

lääkepakkauksen mukana olevalla kyselykaavakkeella potilas voi kertoa tuntemuksiaan lääkkeen vaikutuksesta ja lääkäri kerää nämä tiedot vastaanotolla RFID-lukijalla.

Toisaalta RFID:stä on lähinnä VTT:n aktivoimana tiedotettu sadoissa seminaareissa ja yritysten strategiapäivillä jo 1990-luvun puolestavälistä asti, joten suomalainen elinkeinoelämä on hyvin tietoinen RFID-tekniikan mahdollisuuksista. Vuonna 2004 Vantaan kaupungin projektirahoituksella perustettiin RFID lab, jonka pohjalta muodostettiin 2009 RFID Lab Finland ry. Nykyään yhdistykseen kuuluu 45 jäsenyritystä kattaen lähes kaikki Suomessa RFID-tekniikkaa, -ohjelmistoja sekä -palveluita tarjoavat yritykset. Yhdistyksellä on erittäin suuri merkitys, koska se verkottaa yhteen alalla toimivat yritykset ja edesauttaa yrityksiä vastaamaan kotimaisiin ja kansainvälisiin tarjouspyyntöihin. Yhdistyksen tiloissa Technopoliksessa Vantaalla on myös näyttelytila, missä asiakkaat voivat tutustua erilaisiin RFID-ratkaisuihin. Koska RFID Labin yhtenä toteuttajajäsenistä toimii Metropolia ammattikorkeakoulu, se mahdollistaa tilan käytön myös opetustarkoituksissa. Kokonaisuudessaan voidaan sanoa, että Suomen kilpailuasema laajentuvilla RFID-markkinoilla on erittäin hyvä. Voi jopa sanoa, että Suomi on johtava maa maailmassa ainakin mitä tulee tekniikan osamiseen ja kehittämiseen.

Nyt kun HF-, ja UHF-tekniikat ovat kypsiä ja NFC:n laajamittainen kaupallistuminen alkaa, tärkein haaste Suomessa on löytää näitä teknologioita hyödyntäviä sovellutuksia ja kaupallistaa ne kansainvälisille markkinoille. On arvioitu, että liikevaihdolla mitattuna varsinaiseen RFID-tekniikkaan (lukulaitteet, etätunnisteet, ohjelmistot) liittyvä liiketoiminta on alle kymmenen prosenttia koko RFID:n mahdollistamasta liiketoiminnasta. Ratkaiseva kysymys onkin, mikä rooli Suomella tulee olemaan uusissa palvelukonsepteissa (terveyspalvelut, kaupan palvelut jne.), joita voidaan rakentaa RFID-tekniikka-alustan päälle. On huomionarvoista, että Kesko Oy on tuomassa kauppoihinsa NFC-yhteensopivat kassapäätteet, joista ensimmäiset on jo asennettu.

4. RFID-tekniikan sovellutukset

Tällä hetkellä RFID:tä käytetään laajasti jo seuraavilla aloilla:

Lentokoneiden tutkavalvonnassa, tuotantoautomaatiossa, inventaariossa, logistiikassa, kulunvalvonnassa, eläinten merkkämisessä, auton avaimissa, kirjastoissa, liputtaminen (linja-autot ja metrot), uimahalleissa, vaatteiden merkitsemisessä, matkalaukuissa (lentäminen), passeissa ja henkilökorteissa (esim. Kiinassa).

Pienempinä sovellutusaloina voidaan mainita:

Pesulat, parkkeeraus, vuokra-autojen tunnistaminen, sairaaloiden potilas- ja henkilökunnan -tunnistaminen, kiinteistöjen huoltotoiminnot, matkalaukut lentoliikenteessä ja lääkkeiden alkuperäistunnistus.

Pilotointien pohjalta on jo lähes varmaa, että sitä tullaan käyttämään:

Puhelimissa ja sitä kautta maksamisessa ja liputtamisessa (käteinen, pankkikortti, luottokortti, etukortti, matkalippu ja muut maksukortit) sekä avaimissa, palveluiden aktivoimisessa sekä (Wlan- ja Bluetooth -yhteyden avaamisessa), lentokoneissa (pelastusliivit, lentokoneiden kriittiset komponentit), lentoliikenteessä (matkalippu), antureissa (kiinteistöjen seinien ja betonivalun kosteus, rakenteiden valvonta silloissa, rakennuksissa, lentokoneissa), kuljetusten laadunvalvonnassa (esim. kylmäkuljetukset), kulkuneuvojen osien merkinnässä, kulunvalvonnassa (pitkä lukuikäisyys), lääkepakkauksissa, kyselykaavakkeissa (esim. lääkepakkauksen yhteydessä), tieliikenteessä (tullit, ruuhkamaksut, kaistavalvonta, varastettujen autojen seuranta ja nopeusvalvon-

ta) ja matkapuhelinten ohjelmistojen lataamisessa (Nokia ottamassa tämän kohta käyttöön). Tavaroiden internetiä tukevia kilpailevia palvelusivustoja (vrt. Google) tulee ilmestymään useita. Sivustojen idea on kytkeä tuotteen ID-numero ja matkapuhelimen paikkatiedot paikkalisiin tähän tuotteeseen erikoistuneisiin palvelujen tarjoajiin.

Jatkossa hyvin todennäköisesti sitä sovelletaan:

Tuoteinformaatio (kauppojen hintalapun yhteydessä), kauppojen ja tuotteiden löytäminen, myyjien kutsuminen, aseet, ammuksiset, yksittäiset kuluttajatuotteet (kodin elektroniikka, kodinkoneet, kalusteet, vaatteet), rakennustarvikkeet, erilaisten palvelujen aktivointi (turistipalvelut, musiikin lataaminen), käyttöliittymä kiinteistön energianhallinnassa, sähköautojen lataus jne. NFC:tä tullaan laajasti soveltamaan myös terveysterveyden- ja hyvinvointisektorilla.

Olen rajannut pois ne sovellutukset, missä RFID-piirin ympärille rakennetaan kokonainen elektroniikkajärjestelmä. Tämä siksi, että mahdollisten sovellutusten määrä on niin suuri, että vielä on ennen aikaista sanoa, mitkä niistä lyövät itsensä läpi ja uusia ideoita hyödyntää RFID:tä tulee koko ajan lisää. Koska puhelimesta oleva NFC-rajapinta on avoin ja puhelinten käyttöliittymät ovat nyt yksinkertaistumassa (erityisesti Android), periaatteessa kuka tahansa voi jatkossa tehdä näiden päälle oman sovelluksensa. Tulemme pian näkemään, että internetistä on saatavissa mitä erilaisimpia maksullisia ja ilmaisia matkapuhelimeen ladattavia NFC:hen liittyviä ohjelmistoja ja niihin liittyviä palveluita. Jo nyt voi ostaa kohtuullisella hinnalla sekä HF/NFC- että EPC/UHF-tunnisteita netin kautta sadan kappaleen erissä. Tulemme näkemään hieman samanlaisen ilmiön kuin internetissä ja iPhoneissa on jo nyt tapahtunut; tekniikasta ja ohjelmoinnista kiinnostuneet nuoret tekevät itseään kiinnostavia sovellutuksia ja osa näistä päätyy julkiseen jakeluun. On tietysti hyvin aikaista ennakoita, minkälaisia sovellutuksia tästä kehityksestä seuraa.

Osasta NFC-tekniikkaan liittyvistä jo jonkin aikaa sitten tunnistetuista sovellutuksista kerrotaan yksityiskohtaisemmin liikenne- ja viestintäministeriön raportissa ”Near Field Communications (NFC-työryhmän loppuraportti)”, julkaisu 4/2011.

5. RFID:n yhteiskunnallinen merkitys

RFID-ala kasvaa tällä hetkellä enemmän kuin mikään muu teknologia-ala maailmassa. Nyt on jo käytössä useita miljardeja tunnisteita, joista osa on kertakäyttöisiä (esim. logistiikka) ja useita vuosia käytettäviä (esim. matkalippu). Jos huomioidaan sekä teknologia että siihen oleellisesti liittyvät tietojärjestelmät on RFID:n kansantaloudellinen merkitys jo nyt suuri. RFID on kaiken kaikkiaan tämän hetken suurin teknologiamurros ja sitä voidaan verrata hyvin matkapuhelimen ja internetin merkitykseen. Sovellutusten laajuus huomioiden se tulee vaikuttamaan tuotantoon, logistiikkaan, kauppaan, palveluihin ja tietysti viime kädessä kuluttajiin.

Tuotantoautomaatiossa ja logistiikassa RFID mahdollistaa tuottavuuden kasvattamisen. Kokoonpanoteollisuus (esim. autoteollisuus) katsoo, että RFID:n tuominen ”just on time” -tuotantoon, mahdollistaa kokoonpanoajan puolittamisen. Lentokoneteollisuudessa ei ole kysymys vain tuotannon tehokkuudesta, vaan osat tullaan merkkäämään (lentokoneteollisuus on tuomassa oman RFID-standardin) myös turvallisuuden takia. RFID:n käyttö vähentää varastointikustannuksia, kuljetuksiin liittyvää hävikkiä, nopeuttaa inventaariota, mahdollistaa kuljetuksen seurannan antureilla (lämpötila, kosteus, värinä, jne.). Standardoitu tunnisteen käyttöönotto esim. logistiikassa helpottaa siirtymistä vertikaalisesta liiketoimintamallista horisontaaliseen malliin, joka lisää merkittävästi kilpailua ja antaa yrityksille mahdollisuuden erikoistua ydintoimintoihinsa, joka puolestaan lisää tuottavuutta.

Tuotepakkauksissa tai yksittäisissä tuotteissa olevat tunnisteet ovat tehokas keino estää tuoteväärrennöksiä. Tämä tapahtuu sekä tarraan laitettavien salasanojen perusteella että yksinkertaisesti siten, että koko tuotteen logistista ketjua voidaan seurata. Tällä on suuri merkitys esim. lääkkeitä puhuttaessa. Lääkepurkissa olevaa tarraa voi myös kuluttaja hyödyntää tietojen saamiseksi lääkkeitä (viimeinen käyttöpäivämäärä - voidaan ilmoittaa jäljellä oleva aika vertaamalla tietoa matkapuhelimen kalenteriin).

Yksinkertaisin tapa kuvata NFC:n merkitystä kuluttajalle on se, että standardi on rakennettu siten, että kaikki tällä hetkellä kukkarossa olevat kortit ja liput (matkaliput, pankkikortit, luottokortit, asiakaskortit, teatteri-, konsertti- jne. -liput ja maksukuitit) voidaan laittaa matkapuhelimeen. Tämän lisäksi auton, kodin ja työpaikan avaimet voidaan sisällyttää matkapuhelimeen (BMW julkisti 2011 alussa ensimmäisen NFC-lukitusta hyödyntävän automerkin). Puhelimessa olevat kortit toimivat myös vaikka puhelimen akku on tyhjä, koska päätelaite antaa tarvittaessa energian puhelimesta olevalle NFC-piirisarjalle. Kuluttajan näkökulmasta NFC:tä voidaan pitää myös fyysisenä käyttöliittymänä palveluiden aktivoimiseen kosketuksen avulla. Tämä tarkoittaa sitä, että sen käyttö ei tarvitse useissa tapauksessa ollenkaan matkapuhelimen näppäimistön käyttöä. Vanhusväestö voi aktivoida palvelupyynnön (sairaanhoito, siivousapu, poliisi, palokunta, jne.) koskettamalla etätunnistetta, johon on selkeästi painettu palveluun liittyvä kuva. Kaupassa kuluttaja saa tuotetiedot matkapuhelimeensa, jonka näytöstä myös iäkkäät saavat helpommin yksilöityjä tietoja (esim. tuotteen mahdollisesti allergiaa aiheuttavat aineosat). Jos vanhuksen terveydentilaa seurataan NFC-rajapinnan omaavalla laitteella (pikatesti, monitori tai ihon päälle laitettavat anturit), saadaan tiedot esim. lääkärille koskettamalla kohdetta matkapuhelimella. Tämäntyyppisten sovellutusten näkökulmasta NFC:tä voidaan pitää fyysisenä käyttöliittymänä, joka helpottaa arjessa pärjäämistä.

Jos ja kun tuotetiedot kaupassa ovat saatavissa tuotteen hintalappua koskettamalla, saadaan tuotteesta myös valmistuspaikka, elintarvikkeissa jopa tuottaja (tila), hiilidioksidijalanjälki, jne. Tuotteiden hintavertailu helpottuu, koska asiakas voi kosketettuaan etätunnistetta saada kyseiseen tuotteeseen liittyviä tietoja esim. hinnasta muissa kaupoissa. Kaupassa kuluttaja voi koskettamalla tunnistetta kerätä ostettujen tavaroiden listan matkapuhelimeen ja maksaa ostamansa tuotteen ilman kassahenkilökuntaa. Ostoksia voidaan myös verrata matkapuhelimessa olevaan ostolistaan. Toisin sanoen kuluttaja saa helposti tietoa tuotteesta, joka tietysti puolestaan vaikuttaa merkittävästi kuluttajan käyttäytymiseen.

RFID mahdollistaa sillan fyysisen maailman ja digitaalisen maailman välille. Se on tavallaan jatke toisaalta teolliselle – ja toisaalta informaationvallankumoukselle. Koska informaatiotekniikka on synnyttänyt hyvin pitkälle fyysisestä maailmasta riippumattoman virtuaalisen maailman, RFID mahdollistaa näiden riippumattomien maailmojen yhteensovittamisen. RFID:n todellinen merkitys nähdään vasta noin kymmenen vuoden kuluttua. Tämä johtuu siitä, että vasta kun NFC-puhelimet saavuttavat länsimaissa kymmenien prosenttien osuuden kaikista matkapuhelimista, yrityksille tulee kannattavaksi kehittää tälle pohjalle taloudellisesti kannattavia sovellutuksia. On arvioitu, että vuonna 2015 käytössä on 750 milj. NFC-ominaisuuden omaavaa puhelinta ja sitä käytetään yleisesti ainakin liputtamisessa ja maksamisessa.

6. RFID-teknologiaan liittyvät uhat

RFID:tä on käytetty yleisesti jo lähes 30 vuotta. Tänä aikana on sattunut vain muutamia väärinkäytöksiä. Esimerkiksi autojen varastaminen on RFID:n myötä käynyt lähes mahdottomaksi ja kirjastoista varastaminen on vaikeutunut. Myös kulunvalvonnassa käytetty järjestelmä on toiminut hyvin

– kortteja ei ole pystytty väärentämään. Väärinkäytöksistä ehkä kuuluisin esimerkki on passissa olevien tietojen lukeminen omistajan sitä huomaamatta. Tästä on vaikea syyttää tekniikkaa, koska näissä passeissa ei käytetty parasta mahdollista suojaustekniikkaa. Toinen virhe oli se, että lentokentille asennettiin porttityyppisiä lukulaitteita, jotka antoivat passille energian, jolloin toinen pienikokoinen lukulaite pystyi lukemaan passin tiedot huomaamattomasti. On ollut yksittäistapauksia, missä ravintolassa on seurattu ihmisten liikkeitä tai kadulla vanhemmat ovat seuranneet lapsiaan. Kaiken kaikkiaan väärinkäytösten määrä on tähän asti ollut hämmästyttävän vähäinen verrattuna siihen, kuinka paljon tunnisteita on jo käytetty. Tämä ei tietysti tarkoita sitä, että ongelmia jatkossa ei voisi ilmetä.

Nykyisten sovellutusten laajentuessa RFID-teknologia ei lisää väärinkäytösten määrää merkittävästi. Samoin niissä tapauksissa, missä nykyään käytettävät RFID-tunnisteet siirtyvät matkapuhelimeen, koska mikään muu ei muutu kuin se, että turvallisuustasoa voidaan nostaa. Tämä siksi, että matkapuhelimessa on huomattavasti enemmän elektroniikkaa käytettävänä tehokkaan suojauksen lisäämiseen. Esim. kortilla maksamisen sijaan matkapuhelin voi liittää yhteen matkapuhelimen yksilöllisen koodin sim-korttiin ja sitä kautta sim-kortilla olevaan maksukorttiin. Lisäksi käyttäjän matkapuhelimen pin-koodi ja maksamisen yhteydessä mahdollisesti käytettävä nykyisen kaltainen pin-koodi takaavat sen, että NFC-maksaminen on huomattavasti nykyistä järjestelmää turvallisempi. Ainoa uhka on se, että kassan ja puhelimen välistä radioliikennettä voidaan seurata, jos toinen lukulaite on hyvin lähellä. NFC:ssä käytetään vahvaa salausta, joten ei ole mitään syytä olettaa, että ongelmia syntyy. Jos nyt internetin kautta joko langallisesti tai langattomasti siirretään valtavia rahasummia ja tähän datavirtaan on erittäin helppo päästä käsiksi (esim. GPRS tai WLAN) on NFC näitä järjestelmiä huomattavasti turvallisempi. Käteismaksamisessa raha siirtyy suoraan puhelimelta kauppiaille. Tässä operaatiossa ainoa kontrollipiste on kauppias ja asiakas ja kukaan kolmas osapuoli ei tiedä tästä transaktiosta mitään. Tietysti, jos sim-kortin tietoja siirretään kauppiaille, tästä jää jälki kauppiaan tietokantaan. Tilanne olisi uusi nykyiseen verrattuna, ainakin tapauksessa, missä asiakas ei samalla näytä asiakaskorttiaan. Tämä ongelma ei tietysti realisoidu pitkään aikaan, koska asiakas voi aina käyttää perinteistä käteistä ja näin varmistua siitä, että ostotapahtumasta ei jää jälkeä.

Koska useimmissa tapauksissa autentikointi ja hyväksyntä ja tiedon reitittäminen tapahtuu yhden ns. kontrollipisteen kautta, näiden toimijoiden valvonta korostuu. Tämä ei tietysti poikkeaa nykykäytännöstä merkittävästi, koska jo nyt kaupat toimivat kontrollipisteinä etukorteissa, operaattori tietoliikenteessä ja luottokunnat ja pankit korttimaksamisessa. Kysymys on oikeastaan vain siitä, synnyttääkö RFID uusia kontrollipisteitä tai saavatko nykyiset kontrollipisteet sellaista tietoa, jonka käyttöä ei vielä ole viranomaisten taholta määritely. Ainoa selkeästi nähtävä uusi piirre nykykäytäntöön on se, että kuluttajan lukiessa NFC-matkapuhelimellaan tuotetietoja ja jos hän samalla ottaa yhteyden kaupan palvelimeen tai sitä kautta yhteyden joko kaupan palvelimeen tai avoimeen internetiin, tieto tästä jää kauppiaan tietokantaan. Nykyään kauppias ei saa käyttää etukorteilta keräämiään tietoja yksilötasolla vaan ainoastaan tilastollisesti, ja jos tämän ehdon katsotaan riittävän suojaamaan kuluttajaa tässä uudessa tilanteessa, mitään muutoksia nykykäytäntöihin ei tarvita.

Ehkä suurin uhka liittyy siihen, että jos ja kun logistiikan ja teollisuuden nyt käytössä olevat tunnisteet (heikosti suojatut) siirtyvät kuluttajarajapintaan. Esimerkiksi vaatteessa oleva aktiivinen tunniste voidaan tällöin lukea niin kaukaa, että vaateen käyttäjä ei sitä välttämättä huomaa. Tämä riski voidaan minimoida vain siten, että tuotteen myyjän tulee aina tuhota tunniste (voidaan tehdä helposti ostotapahtuman yhteydessä), jos asiakas ei halua jättää sitä aktiiviseksi myöhempää käyttöä varten. Asiakkaan kannalta käyttökelpoisempi tapa olisi tietysti se, että tunniste vain deaktivoitetaan ostotapahtuman jälkeen, mutta kuluttaja voisi aktivoida sen tarvittaessa puhelimellaan, ainakin tapauksissa, missä hän käyttää tuotetta vain kotiloissa. On kuitenkin hyvin tärkeää, että kauppiailta

edellytetään, että kuluttajan täytyy olla aina tietoinen siitä, että tuotteessa on RFID-etätunniste. Tämä voidaan hoitaa helpoiten siten, että tuotteessa on selkeä merkki siitä, että se sisältää tunnisteen. Tämä merkki pitää tietysti olla yhtenäinen vähintään EU-tasolla. Kuluttajia olisi myös hyvä informoida siitä, että ohutkin metalloitu laminaatti estää RFID-tunnisteen lukemisen. Esim. yksikin kukkarossa oleva pankkikortin kokoinen ohut metallipinnoitteinen kortti tekee kaikki kukkarossa olevat kortit lukukelvottomiksi.

On hyvin tärkeätä huomata, että huonosti suojatuissa etätunnisteissa on ainoastaan tuotteeseen tai palveluun liittyvä koodi ja tällaisessa tapauksessa tunnisteen lukeminen antaa vastaukseksi ”tunte-maton koodi”. Tämä koodi on kytketty vastaamaan tiettyä tuotetta tietokannassa, jonka saa selville vain, jos tähän tietokantaan pääsee käsiksi. Eli tapauksessa, jos tietoa ei haluta antaa, tietoturvaongelma palautuu internetin tietoturvaongelmaksi. Kuluttajille tarkoitetuissa tunnisteissa koodi on tietysti avoin, koska muuten kuluttajat eivät pystyisi hyödyntämään sitä esim. huoltopalveluja etsiessään.

Suomessa on tehty pilotti, missä oppilaat koskettivat pulpettiin istuessaan tunnistetta puhelimellaan, joka lähetti vanhemmille viestin lapsen saapumisesta kouluun. Oppilas sai myös tätä kautta lukujärjestyksen ja muita tietoja koulupäivän tapahtumista. Tämä tietysti tuntuu merkityksettömältä, mutta jos tällainen käytäntö laajenee koskemaan lapsen tai vanhusten liikkumista yleisemmin, seuraukset voivat olla yksityisyyden suojan kannalta vaikeampi hyväksyä. Tietysti jo nykyiset paikantavat puhelimet mahdollistavat paikkatiedon siirtämisen joko toiseen puhelimeen tai internetiin. Tällaisia järjestelmiä on jo nyt käytössä.

Ikäviä seurauksia voi tulla myös siitä, jos ns. ”kolmannet” osapuolet, kuten ravintolat, jakavat vakioasiakkailleen etätunnisteita esim. alennusten saamiseen, mutta käyttävätkin tätä asiakkaan seuraamiseen ilman asiakkaan hyväksyntää. Ravintolat eivät tietysti tule tätä laajassa mittakaavassa käyttämään, koska riski asiakkaiden menettämisestä on suuri. Tosiasiassa jokaisessa yksityisessä tilassa voidaan kameravalvonnalla ja automaattisilla kuvantunnistusohjelmilla tehdä hyvinkin tarkkaa seuranta. Esimerkiksi Lontoossa on asennettu optisia kameroita lähes kaikkialle ja viranomaisilla on erittäin tehokkaat kuvankäsittelyohjelmat käytössään. He pystyvät seuraamaan yksittäistä ihmistä hyvinkin tarkkaan ja jopa tietämään, keitä hän päivän mittaan tapaa. RFID-tapauksessa henkilö voi poistaa tunnisteen hyvinkin helposti, mutta kasvojen peittäminen herättää epäilyä. Eli voidaan väittää, että RFID ei merkittävästi lisää riskiä tulla seuratuksi, koska nykyiset seurantajärjestelmät ovat jo käytössä ja pystyvät jopa luotettavampaan seurantaan kuin RFID. Tietysti RFID mahdollistaa tuotteiden ja ihmisten (jos vaatteissa pitkän lukuetaisyyden tunniste) havaitsemisen seinän läpi. Selkeintä tietysti olisi, että kuluttajat käyttäisivät vain HF/NFC-tunnisteita kotona. Näiden lukeminen seinän läpi onnistuu vain, jos lukulaite on suuri ja tunniste on hyvin lähellä seinää.

Kun tavalliset kuluttajat ryhtyvät kirjoittamaan tunnisteisiinsa tietoja, voi tiedon salaus usein unohtua. Tällaisessa tapauksessa joku toinen voi periaatteessa muuttaa tätä tietosisältöä ja vahinko voi syntyä, jos tietoa ei ole tallennettu tietokoneeseen. Pitkän lukuetaisyyden antureita (esim. rakennusten kosteusanturi) voidaan periaatteessa häiritä tai niiden lukemia vääristellä. Tästä voi olla ikäviä seuraamuksia. Kuitenkin näissä antureissa on usein mukana myös patteri, joten niihin voidaan laittaa vahva salaus tietovuoto-ongelmien poistamiseksi. Sama ongelma koskee periaatteessa myös nykyään käytettyjä langattomia antureita.

Matkalaukkuja merkataan jo nyt useilla lentokentillä RFID-tunnisteilla. On tietysti järkevää, että tunniste jätetään pysyvästi matkalaukkuun. Nykyisestä käytännöstä poiketen tämä johtaa siihen, että lentoyhtiöille tulee mahdolliseksi seurata yksittäisen matkalaukun liikkumista ja sitä, kuka sitä kulloinkin kuljettaa mukanaan. On tietysti luonnollista, että viranomaiset ovat tästä mahdollisuudesta

kiinnostuneita. Tavalliselle matkustajalle tästä todennäköisesti ei ole haittaa, mutta se voidaan kuitenkin kokea yksityisyyden loukkauksena.

Jos verrataan nykyisten teknologioiden (kameravalvonta, matkapuhelin- ja internetliikenteen seuranta ja satelliittipaikannus) muodostamaa uhkaa yksityisyyden suojalle, ei RFID merkittävästi lisää ongelmia kuluttajan kannalta. Kaikista tärkeintä on se, että kuluttajat ovat tietoisia mahdollisista etätunnisteista tuotteissaan tai jatkossa pitkän etäisyyden kulunvalvontakorteista ja näihin mahdollisesti liittyvistä riskeistä. Suomen ei kannata toimia missään yhteydessä kansallisesti, vaan kaikki toiminta riskien minimoimiseksi kannattaa tehdä vähintään EU-tasolla. Tekniikka yleistyy nyt joka puolella maailmaa hyvin samaa tahtia, joten Suomi ei poikkea tässä suhteessa enää mitenkään muista maista. Euroopan maiden tietoturvaluottotut ovat jo yhteistuumin käyneet läpi mahdollisia riskitekijöitä ja tiedottaneet näistä EU:n komissiolle. EU:lla on myös asiantuntijaelimiä, jotka antavat EU-mandaatilla ohjeita standardisointia tekeville tahoille. Muun muassa Suomessa SFS on tehnyt raportin liittyen RFID-tekniikkaan ja he ovat aktiivisesti mukana myös RFID:hen liittyvässä standardoimistyössä. Suomalaiset yritykset, kuten mm. UBM Rafsec ja Nokia, ovat hyvin merkittävässä roolissa kansainvälisissä standardointikomiteoissa

Yhteenvedona voidaan sanoa, että RFID-teknologia ei ole merkittävä uhka yksityisyyden suojalle, jos sitä vertaa nykyisiin jo laajasti käytettäviin teknologioihin: internet, matkapuhelimet, pankki-, luotto- ja kanta-asiakaskortit, kameravalvonta, satelliittipaikannus ja lentokentillä ja julkisissa tiloissa tapahtuvat turvatarkastukset (esim. lentokentillä yleistyvät röntgenkamerat). On kuitenkin oleellista, että RFID-järjestelmiin oleellisesti liittyviä kontrollipisteitä valvotaan siten, että ne eivät voi väärinkäyttää kuluttajista keräämiänsä tietoja. Tuotteisiin mahdollisesti jäävät pitkän lukuetaisyyden etätunnisteet tulee ehdottomasti tuhota tai deaktivoida ostopilanteessa. Vain, jos kuluttaja erityisesti pyytää jättämään etätunnisteen toimintakuntoon, se voidaan jättää tuhoamatta. Kaikissa etätunnisteen sisältävissä tuotteissa pitää olla tästä informoiva merkintä. Lisäksi kauppojen tulee informoida asiakkaita mahdollisista ongelmista, joita voi seurata, jos etätunniste jätetään aktiiviseksi. NFC-teknologiaan liittyvistä tietoturvaongelmista ja kehittymisen esteistä saa tietoa liikenne- ja viestintäministeriön raportista (Julkaisu 4/2011).

7. Yhteenveto

Koska RFID-teknologioissa on useita variaatioita (lyhyt tai pitkä lukuetaisyys, passiivinen tai semi-passiivinen, pienen tai suuren muistimäärän omaavat etätunnisteet, jne.) ja toisaalta niitä voidaan soveltaa useissa hyvinkin erityyppisissä sovellutuksissa (esim. logistiikka, maksaminen, anturit), sitä ei voi pitää yhtenä innovaationa vaan hyppäyksittäin etenevänä innovaatioprosessina, joka on tuottanut ja tuottaa vielä pitkään uusia hyötyjä sekä teollisuudelle että kuluttajille. Vaikka RFID-teknologian kasvu alkoi jo 1980-luvulla, sen todellinen yhteiskunnallinen merkitys tulee näkyviin vasta kymmenien vuosien päästä. Suomi on ollut 1990-luvun alusta lähtien erittäin merkittävässä roolissa RFID-kehityksessä; esim. NFC-teknologia on puhtaasti suomalainen innovaatio. Nähtäväksi jää, pystyykö Suomi hyödyntämään maksimaalisesti hyvää RFID-teknologian osaamistaan nyt, kun sovellutusmarkkinat ovat voimakkaassa kasvussa.

Eduskunnan tulevaisuusvaliokunnan julkaisu 9/2011

ISBN 978-951-53-3371-1 (nid.)
ISBN 978-951-53-3372-8 (PDF)