Near Field Communication och ett praktiskt exempel på användbarheten

Trond Larsen

Examensarbete

Informations- och medieteknik

2013

Trond Larsen

EXAMENSARBETE	
Arcada	
Utbildningsprogram:	Informations- och medieteknik
Identifikationsnummer:	4177
Författare:	Trond Larsen
Arbetets namn:	Near Field Communication och ett praktiskt exempel på användbarheten.
Handledare (Arcada):	Johnny Biström
Uppdragsgivare:	

Sammandrag:

NFC är en teknologi som de senaste åren blivit mycket populär. Den möjliggör trådlösa lösningar på flera tjänster, som också kan implementeras i mobiltelefonerna. Detta examensarbete kommer att behandla NFC i huvudsak. Arbetet baserar sig huvudsakligen på litteraturstudier men det har också gjorts en del tester och intervjuer. Man kommer att kunna läsa om hur NFC fungerar och vad som bör tas i beaktan då man bygger ett system där NFC är en del av funktionaliteten. Efter genomgång av detta arbete kan läsaren lätt beskriva vilka komponenter NFC kräver för att fungera och vilka funktioner de olika komponenterna har. Jämförelser kommer att göras med andra trådlösa teknologier som till exempel Bluetooth. Flera olika säkerhetsrisker kommer att nämnas men även åtgärder för att undvika säkerhetsproblem kommer att tas upp. Det finns otaliga ställen där man kunde använda, och har använt NFC och flera av dem kommer att nämnas i detta arbete. Man kommer att kunna se en framtid fylld med förenklade tjänster inom trådlös betalning. HSL som ansvarar för kollektivtrafiken i huvudstadsregionen, samt deras nuvarande resekortslösningar och framtida planer kommer att behandlas mera grundläggande. Det beskrivs hur HSL i framtiden vill dra nytta av NFC och förbättra sina tjänster med hjälp av tekniken. Det presenteras även information om applikationer som HSL inte ännu publicerat för allmänheten.

Nyckelord:	Near Field Communication, NFC-teknik, RFID, trådlös teknik, automatisk identifiering, Bluetooth, Smartkort, Säkerhetsattacker
Sidantal:	42
Språk:	Svenska
Datum för godkännande:	30.4.2013

DEGREE THESIS	
Arcada	
Degree Programme:	Information and Media Technology
Identification number:	4177
Author:	Trond Larsen
Title:	Near Field Communication och ett praktiskt exempel på användbarheten.
Supervisor (Arcada):	Johnny Biström
Commissioned by:	

Abstract:

In the past few years NFC, and the technology behind it, has become increasingly popular. It facilitates wireless solutions and transfers them to our everyday mobile phones. This thesis will mainly focus on NFC. The study is mostly based on literature studies but some tests and interviews are also included. One will learn about how NFC works and what should be considered when building a system where NFC is a part of the functionality. One will also be able to describe the different components required for NFC to serve its purpose and what various functions they all have. Comparisons will be made with other wireless technologies such as Bluetooth. Several security issues of NFC will be brought up including the solutions for avoiding security related problems. There are countless places where NFC is used today and could be used in the future. Several of those will be brought up in this study. One will see the future of simplified wireless payment solutions. The public transport service provider in the area of Helsinki, HSL, will be discussed in more detail. The future of the company and how it can take advantage of NFC in their services will also be brought up. Finally there will be information on their newest applications not yet available for the public.

Keywords:	Near Field Communication, NFC-technology, RFID, wireless technology, automatic identification, Bluetooth, Smartcards, Security attacks
Number of pages:	42
Language:	Swedish
Date of acceptance:	30.4.2013

INNEHÅLL

Figurer

1 INLEDNING

I detta kapitel behandlas bakgrunden för studierna, syftet och avgränsningen, men också studiemetoderna som använts för examensarbetet. En lista på terminologi presenteras också för att göra svåra termer begripliga för läsaren.

1.1 Bakgrund

Man har alltid försökt göra interaktionen mellan människan och de tekniska apparaterna så bekväm som möjligt. Den mest aktuella teknologin som kommer att möjliggöra denna upplevelse kallas Near Field Communication (NFC). NFC har under flera år varit en teknologi som inte riktigt slagit igenom ordentligt. Orsakerna är bland annat att implementeringen av tekniken i telefonerna har skett väldigt långsamt. För att kunna utnyttja teknologin för fullt och för att leverantörerna av NFC baserad service skulle visa intresse för teknologin, krävs det att största delen av användarna har tillgång till telefoner med inbyggd NFC.

Flera år har gått och nu börjar tiden för NFC blomstra. Nästan alla telefoner på marknaden har inbyggd NFC och det finns redan flera ställen där man kan utnyttja sig av funktionaliteten. Ett av alla användningsområden är kollektivtrafiken där det redan tagits i bruk i flera stora städer runtom i Europa. I Asien är det redan vardag att använda sig av telefonen då man köper biljetter och till och med som betalningssystem.

På grund av tidspunkten och den snabba utvecklingen av NFC just nu är det ett mycket attraktivt ämne att studera. Det ligger intressant teknik bakom NFC och det är viktigt att människor lär sig om den så att utvecklingen inte stannar upp.

1.2 Syfte

Syftet med detta arbete är att ge läsaren en grundlig överblick över tekniken bakom NFC och förstå eventuella risker i användningen av teknologin. Man skall lättare kunna utveckla sina egna NFC lösningar på basen av erfarenheter ur den användning som implementerats hittills. Det genomgås en del praktiska exempel på hur man kan använda NFC och även framtida planer och implementeringar inom flera företag. Man kommer också att få en kunskap i hur Helsingforsregionens kollektivtrafiks biljettsystem kommer att kunna se ut i framtiden och hur utvecklingen i allmänhet fortskrider inom det området.

1.3 Avgränsning

Arbetet behandlar främst tekniken bakom NFC, säkerheten och olika användningsområden men tar också upp en fallstudie som behandlar kollektivtrafiken i Helsingforsregionen och HSL:s framtida planer. Det kommer också att göras jämförelser med Bluetooth och RFID, som har flest likheter med NFC. Inga andra teknologier kommer att tas upp. Fastän arbetet främst är en genomgång av tekniken bakom NFC kommer det ändå inte att gås igenom alla de olika t.ex. ISO standarder NFC stöder och andra mera ingående aspekter. Gällande mjukvaran och dataformaten NFC använder kommer vi endast att ta upp den överlägset mest använda NDEF standarden.

1.4 Metoder

Informationen till arbetet kommer för det mesta att vara litteraturkällor från nätet. Det finns många väldigt pålitliga källor där man hittar långa artiklar om tekniken och om den nuvarande situationen inom NFC. En tryckt bok, som behandlar både teori och praktik, kommer också att vara en av de viktigaste källorna. Intervjuer kommer också att ingå i arbetet för att få så aktuell information som möjligt. När tekniken och användbarheten behandlas så kommer det att göras några enkla tester för att bekräfta att de teoretiska specifikationerna som NFC står för också stämmer i praktiken.

1.5 Terminologi

- ASK = Amplitude-shift keying. En form av modulering som representerar digital data som variationer i amplituden hos en bärvåg.
- ECMA = European Computer Manufacturer's Association. En internationell organisation som står för standardiseringar inom informations- och kommunikationssystem.
- EMV-kort = Förkortning av Europay, MasterCard och Visa. En global standard för smartkort som används inom betalning.
- ETSI = European Telecommunications Standard Institute. En internationell organisation för standarder inom telekommunikation.
- HSL = Helsingin Seudun Liikenne. Organisationen som ansvarar för kollektivtrafiken i huvudstadsregionen i Finland.
- ISO = International Organization for Standardization. En internationell organisation som grundades i 1947. Den främjar olika sorters standarder inom hela världen.
- ISO-14443 = En standard som definierar en del av de kontaktlösa kretskorten som används inom NFC.
- MB = Message Begin. Indikerar att ett NDEF meddelande börjat.
- ME = Message End. Indikerar att ett NDEF meddelande tagit slut.
- Hz = Hertz. Perioderna hos vågorna som används för trådlös kommunikation inom till exempel NFC.
- MWC = Mobile World Congress. En världskänd årlig mobilmässa som i år hölls i Barcelona, Spanien.
- NDEF = NFC Data Exchange Format. Det mest använda dataformatet för trådlös kommunikation inom NFC.
- NFC = Near Field Communication. Namnet på teknologin behandlat i detta examensarbete. Kan också kallas närfältskommunikation.
- NFC Forum = En organisation som grundades år 2004 av NXP Semiconductors, Sony och Nokia för att främja användningen av NFC. Har nu över 170 medlemmar.
- NFCIP-1 = Near Field Communication Interface and Protocol.
- NXP = NXP Semiconductors. En tillverkare av bland annat NFC-taggar och medlem av NFC Forum.

- PIN = Personal Identification Number. Ett hemligt numeriskt lösenord som används för autentisering.
- RFID = Radio-frequency Identification. En föregångare av NFC som fungerar med hjälp av samma teknologi.
- RF = Radio Frequency. Radiofrekvenserna ligger mellan 3 kHz till 300 GHz.
- Wi-fi Direct = En standard som tillåter två Wi-fi enheter, till exempel smarttelefoner, att kommunicera med varandra utan ett behov av en trådlös router.

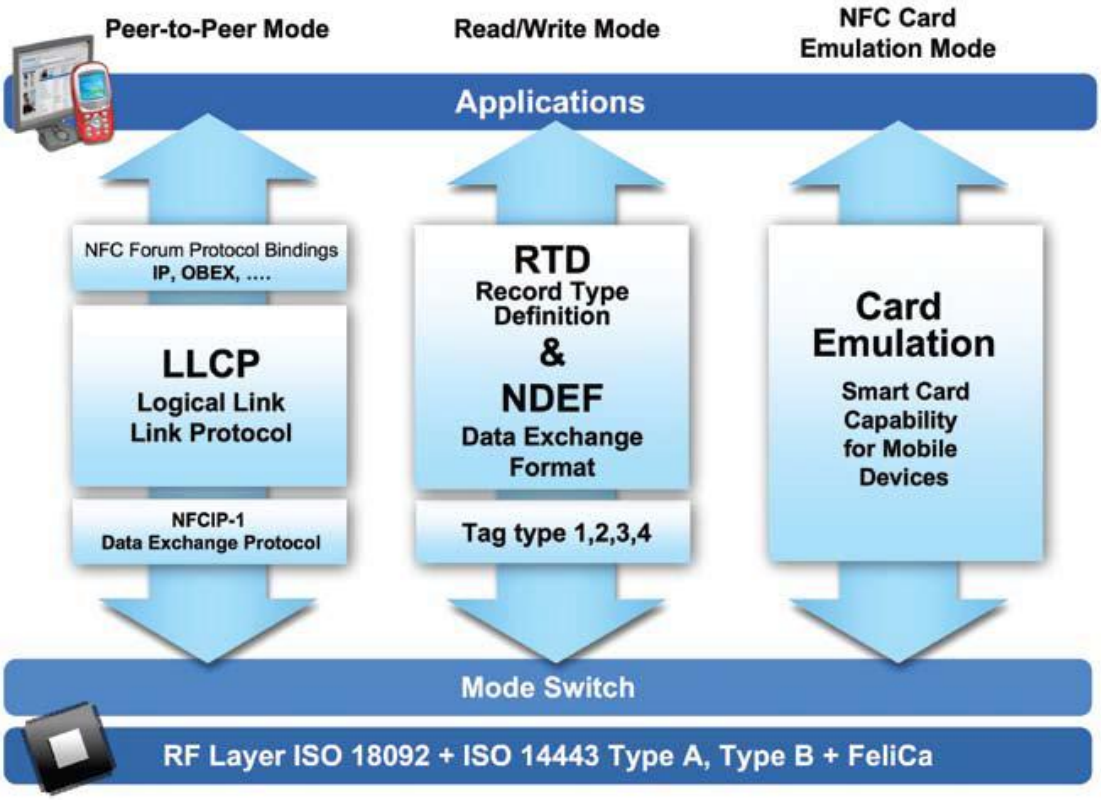
2 NFC TEKNOLOGIN

NFC är en trådlös kortdistanskommunikation baserat på magnetiska induktionsfält. Det är en utvecklad version av RFID, som bland annat använts mycket inom logistik för att identifiera laster och varor. RFID är ganska begränsat då man endast kan läsa information från en tagg medan med NFC kan taggen vara både läsaren och skrivaren. Tekniken fungerar med hjälp av radiovågor på 13,56 MHz med ett totalt frekvensband på nästan 2 MHz. Radiovågorna är ändå oftast koncentrerade till ett område på ±7 kHz. Tanken bakom NFC är att få en berörelselik upplevelse där det endast krävs en liten beröring mellan de två enheterna varefter en kommunikation bildas mellan dem. Hastigheterna kan variera mellan 106 kbit/s, 212 kbit/s och 424 kbit/s vilket betyder att kommunikationen endast är gjord för små dataöverföringar. Den teoretiska räckvidden för NFC är 20 cm men i praktiken krävs ett avstånd på 1-10 cm. (Liikenne- ja viestintäministeriö, 2010) (Curran et al., 2012 s. 68-70) (Wikipedia, 2013a)

För att testa den angivna räckvidden avläser vi en NFC-tagg med en Samsung Galaxy S3:a. Det visar sig att telefonen reagerar på taggen då avståndet är 3-4 cm. Alltså räckvidden för telefoner anser vi då inte vara den maximalt möjliga.

2.1 Olika sätt att kommunicera

Det finns tre olika sätt för NFC att kommunicera. Peer to peer, reader/writer läget och kortemuleringsläget. Då man kommunicerar via NFC måste åtminstone en av enheterna vara aktiva. Den passiva enheten har ingen egen strömkälla utan den genererar ström med hjälp av den aktiva enhetens radiovågor och sin egen induktiva koppling. När den passiva enheten sedan genererat tillräckligt ström kan den börja skicka signaler till den aktiva enheten. Man använder sig av två olika kodningsscheman, Manchesterkodning och Modifierad Millerkodning. Man använder Modifierad Millerkodning då hastigheterna är 106 kbit/s och Manchesterkodning då hastigheterna är 212 kbit/s och 424 kbit/s. (Kurtti, 2011) (Curran et al., 2012 s. 68-70) (Wikipedia, 2013a)



Figur 1. NFC teknologins olika arkitekturer. (NFC-Forum, 2013a)

2.1.1 Peer to Peer - läge

Peer to Peer kallas läget då två NFC kompatibla enheter kommunicerar med varandra. Då behövs det en påbörjare och en mottagare. Man kan också dela in Peer to Peer i aktiv och passiv typ, då den aktiva typen innebär att båda parter förser kommunikationen med energi medan i den passiva försörjer endast den påbörjande parten energin. NFCIP-1, alltså dataöverföringsprotokollet, är definierat så att alla enheter befinner sig i passivt läge och genererar inte någon RF signal. Applikationen måste be telefonen om lov att använda sig av det aktiva eller passiva kommunikationsläget. Om sedan ingen annan aktiv enhet hittas i närheten kan då den påbörjande enheten börja skicka ut signaler. (Kurtti, 2011) (Kerschberger, 2011)

2.1.2 Reader/Writer - läge

Reader/Writer läge kallas det då man kommunicerar med en RFID/NFC-tagg eller smartkort. Det kallas också Passive Mode då taggen/kortet befinner sig i passivt läge. Man använder den aktiva enheten för att läsa information ur taggen/kortet. Taggarna kan till exempel användas för reklamer, busstidtabeller, öppna nätsidor i en webbläsare eller för att koppla sig till ett trådlöst nätverk med hjälp av färdiga konfigureringar inne i taggen. Smartkorten används oftast för passeringskontroll men har under de senaste åren utvecklats också för betalningskort. (Kurtti, 2011) (Kerschberger, 2011)

2.1.3 Kortemuleringsläge

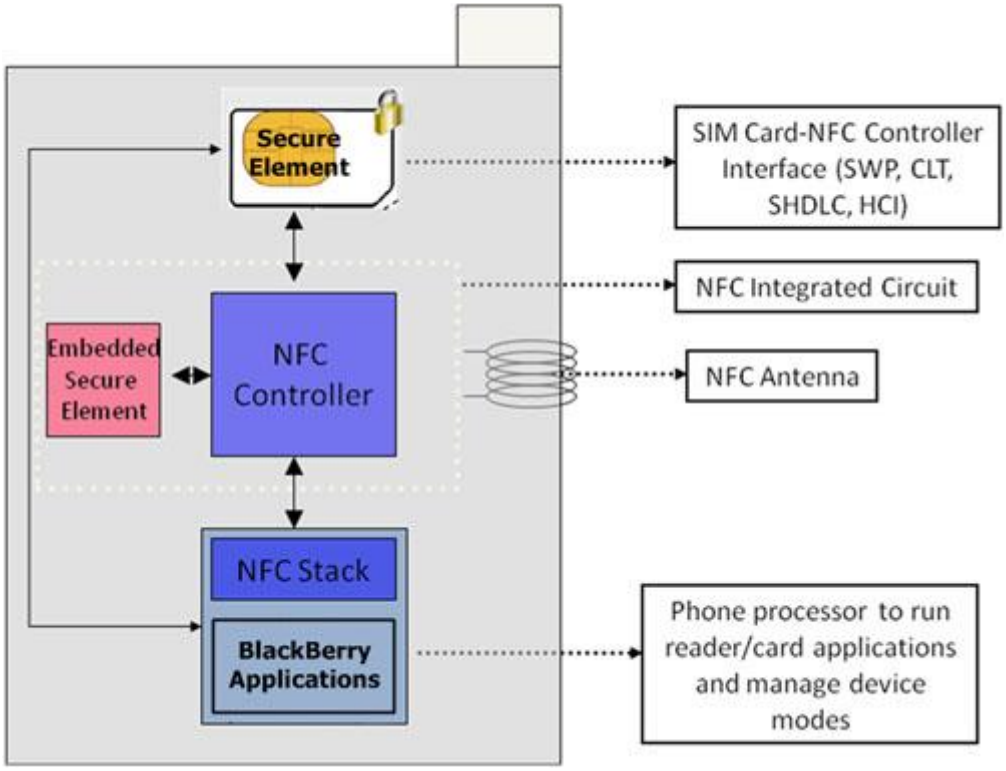
Man kan ersätta de nuvarande smartkorten med hjälp av kortemuleringsläget. Då flyttas smartkortens information över till den NFC kompatibla enheten och den fungerar då med de existerande läsarna. Detta möjliggör användningen av till exempel betalning med telefon och passeringskontroll. Huvudstadsregionens kollektivtrafik HSL har också planerat överföra deras resekort till telefoner med NFC och då kommer kortemuleringsläget att utnyttjas. (Kurtti, 2011) (Kerschberger, 2011) (Vaattovaara, 2013)

2.2 Hårdvaran

NFC fungerar med hjälp av en induktiv koppling mellan de två kommunikationsparterna. Den aktiva, eller påbörjande enheten, skapar en RF signal på 13,56MHz. Denna signal genererar också ström för den passiva parten så att den också kan skicka signaler tillbaka till den aktiva enheten.

För att kunna använda NFC inom till exempel betalning och andra ställen där hög säkerhetsnivå krävs, har man planerat systemet ganska grundligt. Det består av flera olika delar som tillsammans gör att systemet kan köras utan bekymmer. Först har vi antennen som också fungerar som en induktiv strömgenerator för enheter i passivt läge. Så finns det en NFC Controller som sköter om transaktionerna mellan alla de olika delarna. Därtill har vi en Host Controller som kan vara till exempel själva telefonen och applikatio-

nerna som använder sig av NFC. Det krävs också ett Secure Element, alltså ett slags ”säkert element”, som sparar kritisk data som till exempel kreditkortsinfo. Det finns några olika sätt att implementera ett Secure Element. Det kan antingen vara inbyggt i telefonens hårdvara, eller så kan det vara inkluderat i ett minneskort eller ett sim kort som man sedan skilt anskaffar. (Coskun et al., 2012)

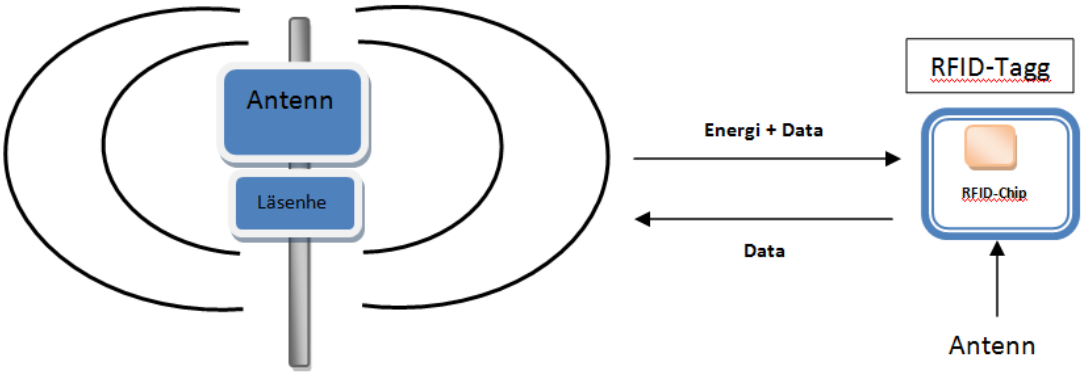


Figur 2. En Blackberry telefons NFC arkitektur. Här fungerar BlackBerry applikationerna som Host Controller. (Blackberry, 2013)

Om man tänker utnyttja telefonen som betalningsmedel måste den också fungera fastän batteriet tagit slut eller telefonen stängts av. Detta är möjligt då telefonens NFC antenn också kan generera ström för NFC Controllern och Secure Elementet fastän all annan strömförsörjning tagit slut. Då fungerar det med hjälp av kortemuleringsläget och telefonen ser ut som ett smartkort. Kortläsaren försörjer den nu passiva enheten med ström som den också skulle göra för ett vanligt smartkort. (Kerschberger, 2011)

2.2.1 Taggar

En NFC tagg är en passiv komponent där man kan spara information såsom till exempel nätsidor, kontaktinformation och telefoninställningar. Det är byggt upp av ett litet mikrochip, kopplat till en antenn som tar emot och skickar informationen. (Sefedini & Al-Ashraf, 2010)



Figur 3. Så här fungerar en RFID/NFC tagg. (Sefedini & Al-Ashraf, 2010)

Det finns ett antal olika typer av taggar. NFC Forum har definierat dem och de kallas helt enkelt Type 1, Type 2, Type 3, och Type 4 taggar. De tre första är baserade på existerande RFID taggar, medan den fjärde taggtypen baserar sig på existerande smartkorts standarder. Nedan följer en närmare beskrivning av de olika taggarna. (Koistinen, 2010) (Kerschberger, 2011) (Coskun et al., 2012 s. 101-102) (NFC-Forum, 2007)

- Type 1 tag: Denna taggtyp är både läs- och skrivbar, men kan också göras endast läsbar om man så önskar. Minneskapaciteten varierar från 96 byte ända upp till 2 kB. Kommunikationshastigheten är 106 kbit/s. Type 1 taggen är enkel och billig vilket gör den populär bland taggtyperna. Den produceras av Innovision.
- Type 2 tag: Ganska långt en kopia av Type 1. Enda skillnaden ligger i sättet hur den svarar på kommandon från läsaren. Så har den också en kollisionsundvikande mekanism så att det är möjligt at avläsa taggen fast det finns flera taggar inom läsarens räckvidd. Denna typs tagg är också osäker. Produceras av Philips och NXP.
- Type 3 tag: Baserar sig på Japanska FeliCa standarden. Maximala minneskapaciteten kan vara till och med 1 MB och hastigheterna ligger på 212 kbit/s eller 424

kbit/s. Denna taggtyp är mera gjord för komplexa applikationer och är därför lite dyrare än andra versioner. Produceras av Sony.

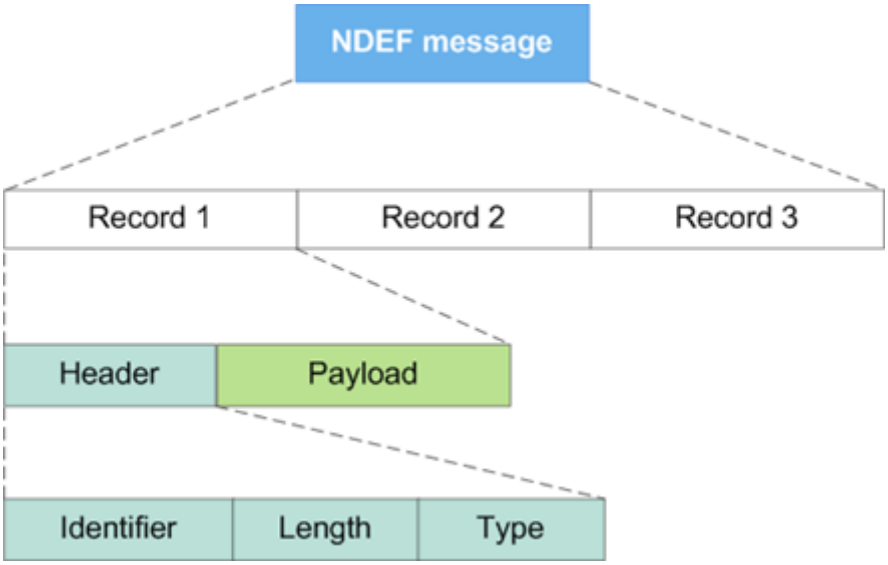
- Type 4 tag: Denna taggtyp konfigureras under tillverkningsfasen. Man kan då välja om den skall vara läs- och skrivbar eller bara läsbar. Minneskapaciteten kan vara upp till 64 kB och hastigheterna varierar mellan 106 kbit/s och 424 kbit/s. Dessa taggar produceras av flera olika leverantörer.

Figur 4. Ett antal olika taggar.

2.3 NDEF

För att NFC enheter skall kunna kommunicera med varandra krävs ett gemensamt dataformat. NFC Forum har definierat en standard som kallas NFC Data Exchange Format (NDEF). Det används för att kommunicera, oftast mellan en aktiv och en passiv partner

men också mellan två aktiva. När man kommunicerar via NFC är det alltid en av enheterna som skickar meddelanden åt gången, alltså turvis. Ett NDEF meddelande består av binär kod som sammanfattas ur ett eller flera olika Records, eller poster som de också kallas. Dessa i sin tur innehåller information om bland annat hur långt meddelandet är och vad för slags data det innehåller. Den första posten av ett NDEF meddelande är alltid markerat med ett MB (Message Begin) och i slutet finns det alltid en post med ME (Message End). (Rahman & Willee, 2012) (Coskun et al., 2012 s. 102-108) Nedan finns ett exempel på hur ett NDEF meddelande är uppbyggt.



Figur 5. Så här ser ett NDEF meddelande ut. (Rahman & Willee, 2012)

2.4 NFC i jämförelse med andra trådlösa tekniker

2.4.1 RFID

RFID är egentligen grunden för NFC och därför är de två mycket lika. Ofta är ändå NFC utrustade enheter fullt kompatibla med äldre RFID lösningar. De behöver bara använda sig av kortemuleringsläget så fungerar de som vilka som helst andra RFID taggar eller kort. De största skillnaderna mellan de två är bland annat att RFID taggar inte kan modifieras i senare skeden utan är låsta till sina, under produktionen angivna, roller.

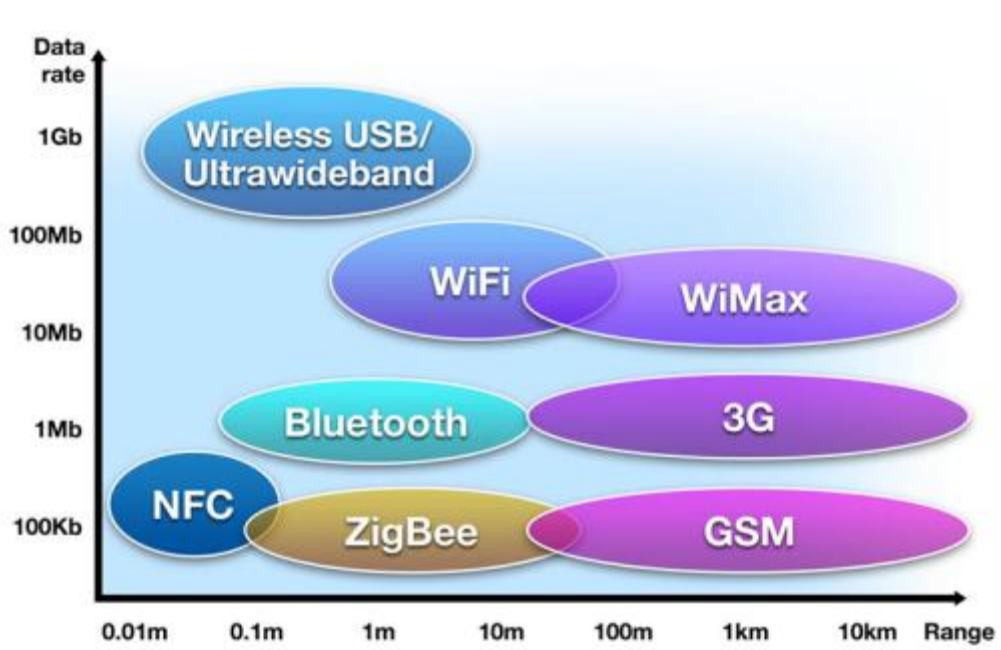
NFC taggar kan däremot skrivas på eller också låsas när som helst. Dessutom har NFC den fördelen att läsaren också kan fungera som en passiv enhet. Avstånden är också lite varierande. RFID kan fungera på upptill flera tiotals meter medan NFC bara fungerar i praktiken på upp till 10 cm. Detta gör att NFC kan användas för att göra säkra transaktioner eftersom det är mycket svårare för utomstående att kapa kommunikationen. NFC innehåller också ett Secure Element (se kapitel 2.2) som hjälper till att hålla kritisk data säkert mot intrång. (Kumar, 2010) (Koistinen, 2010)

2.4.2 Bluetooth

Bluetooth har redan länge funnits som en av telefonernas egenskaper. Det används för trådlös kommunikation mellan enheter utrustade med tekniken i fråga. För att två enheter skall kunna kommunicera via Bluetooth krävs ändå att man parar dem. Detta är något som man totalt uteslutit inom NFC. Man ville helt och hållet bli av med parningen. Det gör också NFC mera användarvänligt. Tiden det tar för två NFC enheter att paras är endast 0,1 s. (Koistinen, 2010)

För att underlätta användningen av Bluetooth har man utnyttjat det att parningen görs via NFC. Man berör alltså då enheterna som skall paras och NFC sköter parandet. Då undviker man det extra steget med parningen. Till exempel har Nokia introducerat flera trådlösa hörlurar och högtalaren som man parar med hjälp av NFC.

Bluetooth har också sina fördelar eftersom hastigheterna kan nå upp till 24 Mbit/s. Det är en mångfald av vad NFC kan åstadkomma. Räckvidden är också mycket större och kan vara i bästa fall 100 meter. (Wikipedia, 2013b) Nedan ser vi en ungefärlig bild över räckvidden och hastigheten över de mest kända trådlösa teknologier.



Figur 6. Hastigheter och räckvidd för trådlösa teknologier. (NFC-Forum, 2013b)

3 ANVÄNDNINGSOMRÅDEN

NFC är en kommunikation på mycket kort distans. Detta gör den mycket användbar inom säker överföring av data eftersom det är svårt att utöva olika attacker på kommunikationen. Den baserar sig också på RFID och är kompatibel med de flesta äldre RFID taggar och system. Detta innebär att man ofta kan fortsätta utvecklingen utifrån tidigare RFID lösningar. I detta kapitel går vi igenom några av de möjliga användningsområdena för NFC.

Möjligheterna för utnyttjandet av NFC är omfattande. Det har sagts att framtiden är fylld med nya användningsområden som vi inte ens kunde tänka oss. Eftersom allt flera har tillgång till tekniken börjar det vara en självklar efterföljare för till exempel äldre passeringskontroll och betalningssätt.

Ett intressant exempel på ett nytt sätt att använda tekniken är Hyundai som introducerat bilnycklar som fungerar med hjälp av telefonens NFC. Man förväntar sig ta systemet i bruk redan år 2015. Då skulle man samtidigt som man låser upp bilen få alla sina personliga inställningar, musik, kontakter, och så vidare, överfört till bilens huvudskärm (Clark, 2013).

Den första telefonen med NFC funktionalitet, en Nokia 6131, som kom ut på marknaden år 2006, hade nästan inga av de nuvarande telefonernas egenskaper. Man kunde varken skicka filer via en liten beröring eller programmera in några kommandon på NFC-taggar. Nu har det blivit vanligt att man använder NFC för att förenkla vanliga saker där det förr krävdes konfigureringar av olika slag. Till exempel kan man programmera in sitt hems trådlösa nätverks konfigureringar i en NFC tagg och när man får gäster behöver de bara röra med sina telefoner vid taggen så är de kopplade till nätverket.

Figur 7. Ett exempel på ställen där NFC kan utnyttjas. (Nordström & Nyqvist, 2012)

3.1 Betalning

Det finns flera aspekter att ta i beaktande då man planerar att skapa ett nytt betalningssystem baserat på ny teknologi. Den viktigaste aspekten, som även berör kunden mest är säkerheten (Se kapitel 4). Vaattovaara nämnde också i en intervju att de trådlösa betalningskorten inte är tillräckligt snabba för att fungera ordentligt. I London har man testat kontaktlösa EMV-kort men man ansåg att den uppnådda svarstiden på 600 ms inte var tillräckligt liten för att göra upplevelsen tillräckligt bekväm. Utveckling sker dock hela tiden och om inte så länge tror man att svarstiden förminskats till ett acceptabelt värde. Ett annat dilemma är alla mellanhänder som vill ha sin del av kundernas pengar. Det har lett till att det uppstått flera olika allianser av företag som planerar sina egna lösningar. Till exempel har MasterCard introducerat sitt PayPass, som implementerar smartkortsfunktionaliteten i bankkorten och telefoner. De introducerade i början av 2013 ännu en

utvecklad version av servicen, nämligen MasterPass. Tjänsten kommer att lanseras i flera länder under året 2013. (Vaattovaara, 2013) (MasterCard, 2013) (Dignan, 2013)

PayPal lanserade en mobilapplikation för Android år 2012 där man kunde bland annat utväxla lunchsedlar mellan sina kolleger. De planerade också ett system som skulle möjliggöra betalning via NFC men senare under samma år meddelade de att projektet lagts ner. PayPals före detta VD John Donahoe nämnde i ett publikt sammanhang att NFC aldrig kommer att vara färdigt för användning inom betalning. PayPal utesluter ändå inte möjligheten att ta NFC i bruk vid ett senare tillfälle. De har utvecklat sitt eget system, PayPal Here, som baserar sig på en skild läsare som man pluggar in i telefonen. Med hjälp av den kan man ta emot vilket som helst betalningskort mycket enkelt. De tror sig lansera systemet globalt år 2013. (Lui, 2012) (Clark, 2012) (PayPal, 2013)

Figur 8. PayPal Here kortläsaren. (Yellowdoggdesigns, 2013)

En annan kombination är Visa och Samsung som under MWC (Mobile World Congress) 2013 meddelade att de startat ett globalt samarbete för att snabba på NFC betal-

ningen. De kommer att redan samma år lansera telefoner med färdigt installerad Visas mobilapplikation payWave, för betalning med NFC. Dessa telefoner kommer att ha en aktiv Secure Element del som krävs för en säker trådlös kommunikation. (Lui, 2013)

Det finns också system som varit i bruk redan länge. Till exempel i Japan finns världens mest utbredda NFC betalnings- och biljettssystem. Där togs de första kontaktlösa betalningssystemen i bruk redan år 2004. (Balaban, 2011)

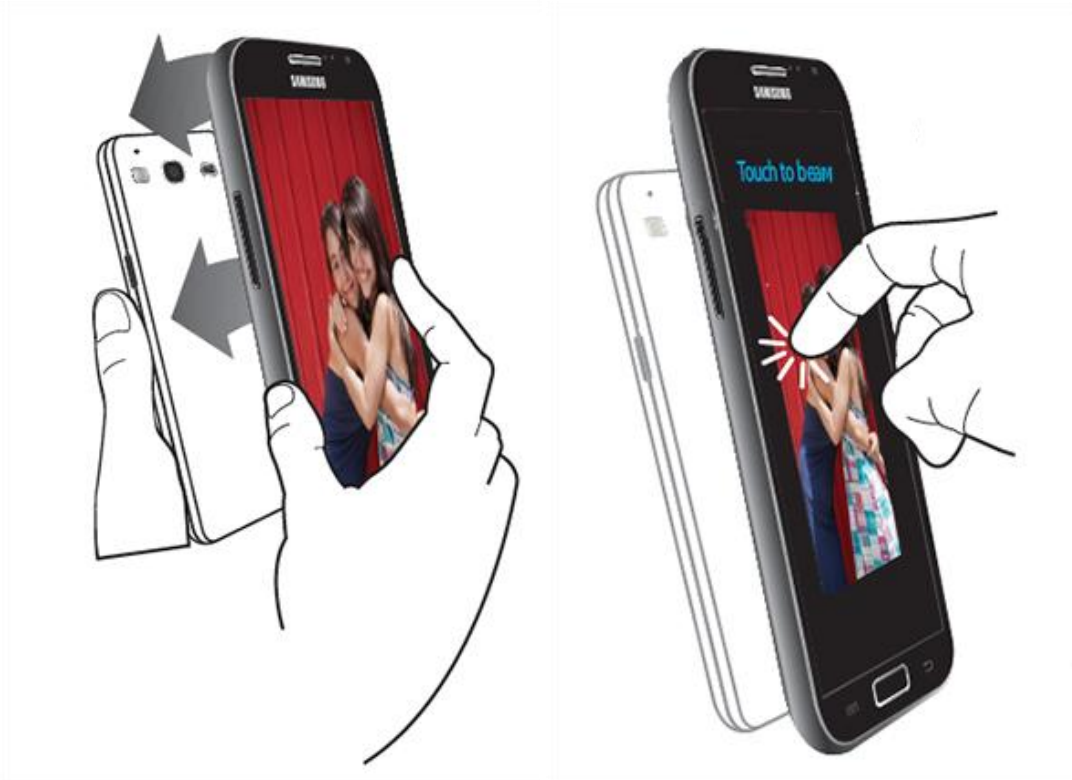
I Finland går man också framåt i utvecklingen. Man har i flera banker börjat ta i bruk trådlösa bankkort som skall fungera med att bara vifta framför kortläsaren. OP-Pohjola skall under våren 2013 förse alla kort som ges ut till kunderna med trådlös betalning. Man kan då betala med korten för upp till 25 euro utan att behöva slå in sin pinkod. (OP-Pohjola, 2013)

3.2 Android

En plattform där man diskuterar mycket NFC är Android. Google behandlade ämnet mycket redan år 2011 på deras populära I/O konferens och följande år fortsatte trenden. De har bland annat gjort det mycket lätt att överföra länkar till artiklar och applikationer genom beröring av två telefoner med NFC-funktionalitet. Man kan också överföra bilder, videon och filer genom att starta en Bluetooth kommunikation med hjälp av en enkel NFC beröring. Google kallar sitt NFC system Android Beam och det utvecklas hela tiden för att förbättra och lägga till funktionaliteter. Den senaste versionen av operativsystemet, Jelly Bean, inkluderade många förbättringar och funktionaliteter, en av dem parning med Bluetooth försedda högtalaren med hjälp av NFC. (GoogleDevelopers, 2011) (GoogleDevelopers, 2012) (Murph, 2012)

Figur 9. Android Beam. (Android, 2012)

En version av Android Beam kallas S Beam och är vidareutvecklad av Samsung. Där är det möjligt att överföra filer med hjälp av Wifi Direct. Man kan överföra bilder, videon, kontaktuppgifter och länkar mycket enkelt och snabbt. Andra funktioner ingår också som till exempel bildspels- och videovisning på flera telefoner samtidigt. (Samsung, 2012)



Figur 10. Touch to Beam funktionen i S Beam. (Samsung, 2012)

3.3 Andra användningsområden

År 2010 började Kesko testa trådlösa plussa-kort. Det visade sig fungera bra och idag är alla nya plussa-kort utrustade med egenskapen. Man behöver alltså inte mera dra kortet genom läsaren utan det räcker bara man viftar plånboken vid läsaren så registreras medlemskapen. Ett litet problem uppstår ändå ifall man råkar ha flera smartkort i plånboken, då vill inte läsaren godkänna kortet och man måste ta ut det ur plånboken. Keskos plussa-kort valdes år 2012 till årets bästa NFC baserade service. (Kesko, 2012)

I Uleåborg har man använt sig av NFC-taggar för att lära utländska barn finska i skolorna. Läraren har programmerat ett ord i en tagg som sitter ihop med till exempel en bild på en färg eller någon sak. Då skal eleven gå runt i skolan med telefonen och hitta de olika färgerna/sakerna som sedan syns på skärmen som ett ord. Därifrån går de vidare och skall hitta alla bokstäver till ordet. Detta har visats sig vara ett mycket effektivt sätt

att lära sig och i en barnträdgård lärde sig barnen upp till 20 bokstäver i timmen. (Mainio, 2013)

Några andra ställen där man har stor nytta av NFC är:

- Checka in på flygplatser
- Betala parkeringsbiljetter
- I kontoren för passering genom dörrar och inloggning på datorer
- Olika evenemangs biljetter på telefonen
- Turistinformation
- Rabattkuponger
- Hotellnycklar

4 SÄKERHETEN

När man behandlar en teknik som används för betalning och överföring av pengar kommer det alltid att ställas frågan; är det säkert? Detta gäller speciellt NFC eftersom det implementeras i de personliga telefonerna som också lätt kan tappas bort eller bli stulna. Även om man tänkt på säkerheten då man definierat NFC som en teknik som fungerar på mycket kort avstånd, är det inte tillräckligt för att skydda mot säkerhetshot. I detta kapitel går vi igenom några av de vanligaste säkerhetshoten inom NFC, och vad man kan göra för att undvika dem.

4.1 Olika metoder för attack

Här behandlar vi fem olika sätt att angripa NFC på. Det finns andra också men dessa är de mest omtalade och de som mest sannolikt kommer att orsaka problem och kräver därmed olika slags säkerhetsåtgärder.

4.1.1 Avlyssning

Eftersom NFC fungerar trådlöst och det skapas RF-vågor för att kommunicera, är avlyssning ett av de största säkerhetshoten. Då används en ändamålsenlig antenn för att fånga upp signalerna som skickas under kommunikationen. Det är svårt att definiera avståndet för att attacken skall fungera eftersom så många aspekter anses vara avgörande. Några saker som påverkar är effekten på signalen som skickas ut från enheterna och omgivningen, till exempel väggar och metallföremål i närheten. Det är också lättare att avlyssna aktiva enheters signaler eftersom de är mycket starkare och har en längre räckvidd än de passivas. Skillnaden varierar från ungefär 1 meter för de passiva enheterna till ungefär 10 meter för de aktiva.

Avlyssning är svårt att förhindra helt och hållet. Inom NFC kan man ändå skydda sig genom att använda en säker kanal för kommunikationen. Det betyder att informationen som skickas mellan enheterna krypteras med hjälp av en krypteringsnyckel. (Coskun et al., 2012 s. 270–272) (Nordström & Nyqvist, 2012)

4.1.2 Datakorruption

Det är också möjligt att ändra på informationen som skickas så att den blir oanvändbar. För att kunna utföra datakorruption måste man förstå hur moduleringen och kodningen görs. Man skickar då giltiga frekvenser ur data spektrumet under rätt tid och stör därmed den ursprungliga signalen.

De kommunicerande NFC enheterna kan motverka denna typs attack genom att testa den inkommande RF signalen. Detta kan göras samtidigt som dataöverföringen och då är det inte svårt att upptäcka attacken. (Coskun et al., 2012 s. 270–272) (Nordström & Nyqvist, 2012)

4.1.3 Data-modifiering

Under data-modifiering är angriparens mål att ändra på informationen och skicka den vidare. Då man i NFC använder två olika amplitudmoduleringsgrader skiljer sig också riskerna för attacken. Vid hastigheter på 106 kbit/s mellan aktiva enheter, används en Modified Millerkodning ASK(Amplitude Shifting Key) med 100 % modulering vilket gör att fullständiga data-modifieringar är omöjliga. I andra fall används Manchester kodning med 10 % modulering. Angriparen kan då överlappa den ursprungliga RF-signalen med en signal som ändrar på de skickade bitarna. I 100 % Millerkodningen kan endast en del av bitarna ändras på och vid 10 % Manchesterkodningen kan alla bitar utsättas för attack.

På samma sätt som under data-korruptering kan NFC-enheterna testa RF-signalen och upptäcka störningar. Man undviker också data-modifieringar totalt genom att använda en säker kanal för dataöverföringen. (Coskun et al., 2012 s. 270–272) (Nordström & Nyqvist, 2012)

4.1.4 Införande av data

När två enheter kommunicerar kan en angripare utnyttja pauser i kommunikationen och skicka sitt eget meddelande, som då tolkas som ett svar istället för det ursprungliga. Detta kräver ändå att den svarande enheten inte hinner svara tillräckligt snabbt och angriparen således hinner skicka sitt svarsmeddelande istället. Ifall båda svarsmeddelandena skickas samtidigt tolkas det som en korruption i data.

För att undvika att en utomstående inför data i kommunikationen kan man se till at svarsmeddelandet skickas omedelbart. Då är det omöjligt för angriparen att få sitt svarsmeddelande skickat före det ursprungliga. Den svarande parten kan också avlyssna kommunikationen och därmed upptäcka en potentiell angripare. Det tredje sättet är att använda sig av en säker kanal för dataöverföringen. (Coskun et al., 2012 s. 270–272) (Nordström & Nyqvist, 2012)

4.1.5 Tredjepartsattack

En tredjepartsattack eller "Man-in-the-Middle" som det också kallas kan beskrivas så att två personer kommunicerar medan en tredje person är inblandad i kommunikationen utan deras vetskap. Den tredje parten fungerar som en sändare och mottagare mellan de två egentliga parterna. Eftersom den påbörjande parten lyssnar på ett svar från den mottagande parten är det praktiskt taget omöjligt för den tredje parten att skicka något till den mottagande parten utan att bli upptäckt av den påbörjande parten. Detta leder till att tredjepartsattacker inte är möjliga inom NFC. (Coskun et al., 2012 s. 270–272) (Nordström & Nyqvist, 2012)

4.2 Slutsatser om säkerhet

Som vi lyft fram i detta kapitel så finns det flera olika sätt att attackera NFC på. Men man kan genom att använda de rätta säkerhetsåtgärderna få till stånd en trygg kommunikation mellan parterna. Det finns ändå undersökningar som visar att attacker är fullt möjliga och att man till exempel kan få en NFC enhet att gå in på en nätsida med oönskade konsekvenser. En mycket känd säkerhetsforskare, Charlie Miller, har publicerat

sina undersökningar om NFC och konstaterat att det inte alls är så säkert som vi tror. De som vill läsa mera om ämnet kan bekanta sig med hans publikation och presentation nämnd i källförteckningarna. (Miller, 2012a) (Miller, 2012b)

När det gäller fysiska element som till exempel taggar som är placerade på allmänna platser, finns det dock alltid risk för manipulering och förstörning av dem. Man kan exempelvis lätt byta ut den ursprungliga taggen mot en som innehåller något skadligt och således ställa till med problem.

5 HSL OCH NFC

Vi har redan behandlat en hel del olika användningsområden i tidigare kapitel, men för att få en djupare syn på hur ett system baserat på NFC verkligen kan underlätta människors liv skall vi bekanta oss lite närmare med HSL. Orsaken till att just HSL valts är deras stora betydelse i huvudstadsregionens kollektivtrafiksverksamhet och företagets intresse av NFC relaterade tjänster. Det är också ett företag som nästan alla människor inom deras verksamhetsområde vet om och har på något sätt utnyttjat sig av deras tjänster.

För att få en så aktuell bild av situationen som möjligt har en intervju gjorts med Risto Vaattovaara som fungerar som gruppchef för HSL:s biljettssystemsavdelning. Det har också gjorts en del tester med olika NFC applikationer. (Vaattovaara, 2013)

5.1 Allmänt

Huvudstadsregionens kollektivtrafik tog i bruk ett gemensamt trådlöst biljettsystem år 2001. Systemet förnyades år 2009 från Idesco Oy:s ostandardiserade system till ett som följde ISO-14443 standarder. Då togs alltså i bruk de kort som också idag används. Man kunde då läsa korten med alla slags olika läsare och det krävdes inte speciella apparater för läsandet som var fallet tidigare. Enligt Vaattovaara var ända dåliga sidan med de nya korten att de måste föras lite närmare läsaren än tidigare. Förnyelsen var ett tidigt skede av en större förnyelse som planerats för 2015. Då skall kortens tekniska egenskaper förbättras för att senare kunna användas i eventuella andra tjänster. (Kurtti, 2011) (Vaattovaara, 2013)

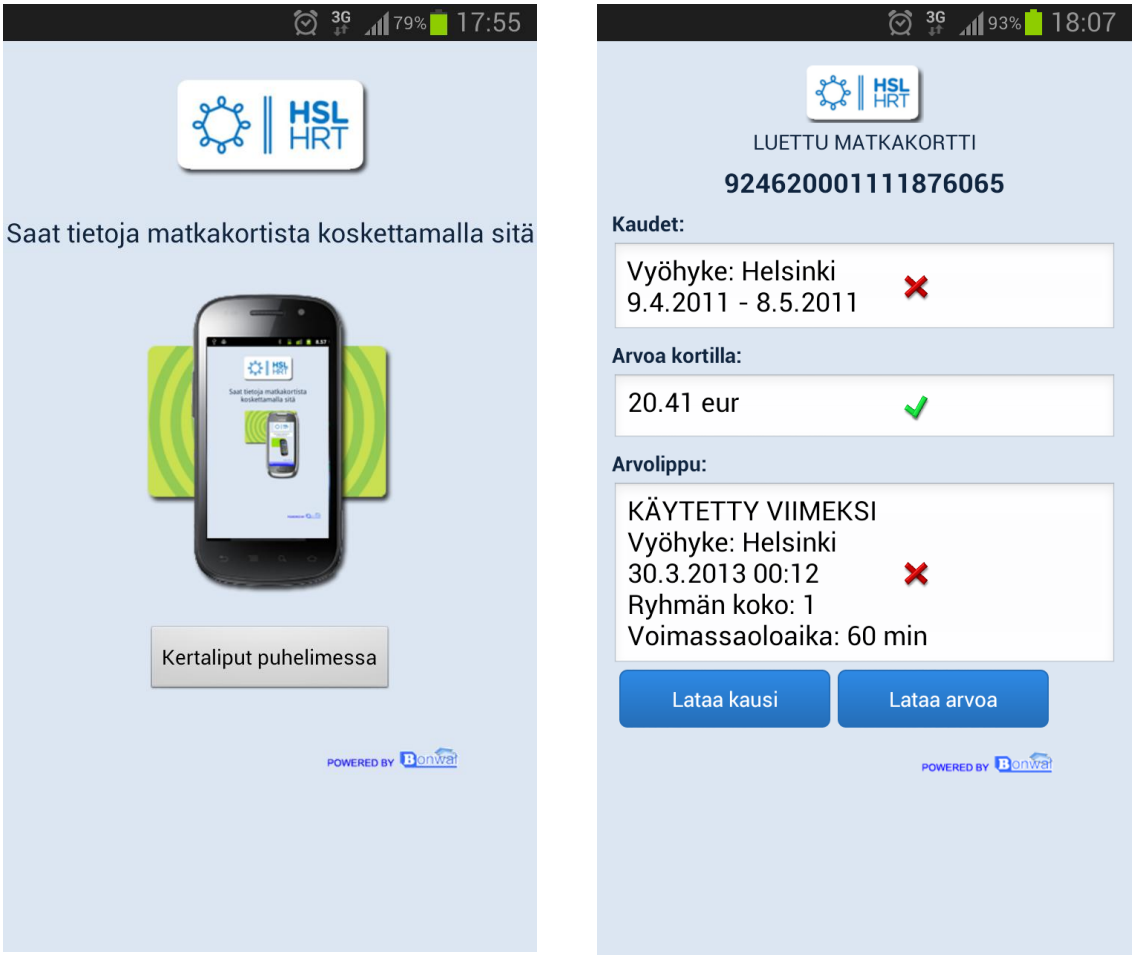
Figur 11. Det nuvarande gröna resekortet och kortläsaren. (Havumäki, 2013)

Det nuvarande personliga resekortet är det möjligt att skaffa om man är boende inom HSL:s kollektivtrafiksområde och vill använda sig av deras tjänster. Det finns också ett innehavarkort som kan användas av flera personer, dock inom samma kundgrupp. Man kan också köpa vanliga pappersbiljetter från biljettautomater och chaufförer. Biljetter kan även beställas genom att skicka ett SMS till ett visst nummer.

5.2 Utvecklingen mot NFC

Det största problemet biljettsystemsleverantörer stött på är att få telefontillverkarna att implementera tekniken i sina produkter. Man har länge väntat på att kunna ordentligt ta i bruk ett system som fungerar tillsammans med telefonerna. Redan år 2005 deltog Vaattovaara i ett seminarium om NFC och mobilbetalning där det lovades att telefoner med NFC skulle bli vanliga inom ett eller två år. Detta utlåtande har upprepats år efter år utan större förändringar. Det är först de senaste åren som NFC blivit standard tillbehör i mobiltelefoner. Därför tycker man tiden är inne för att lansera system baserat på NFC. (Vaattovaara, 2013)

I början av 2012 gjorde HSL samarbete med en av sina underleverantörer och utvecklade en applikation för Symbian som kunde läsa de nuvarande resekorten. När det visade sig fungera bra utvecklades också en applikation för Android. Utvecklingen av Windows Phone 8 applikationen kunde man inte påbörja ännu eftersom det endast fanns stöd för avläsning av taggar. Med HSL:s applikation, som ännu inte finns tillgänglig för allmänheten, kan man ladda värde till kortet med hjälp av telefonen. Laddning av perioder till kortet har ännu inte utvecklats färdigt, eftersom den processen är mycket mera komplicerad på grund av de olika prisgrupperna och områdena. Nedan ser vi en skärmdump ur applikationen för Android och hur det ser ut då man avläst ett resekort. Man kan få reda på hur mycket pengar man har på kortet och vilka typs biljetter man använt eller köpt senast. (Vaattovaara, 2013)



Figur 12. Till vänster: Framsidan av HSL:s resekortsapplikation. Till höger: Ett resekort är avläst och informationen visas på skärmen.

6 AVSLUTNING

Detta examensarbete har behandlat grunderna inom NFC och syftet var att ge läsaren en god förståelse över hur helheten fungerar. De olika komponenterna som krävs för tekniken har nämnts och några exempel på användningen har också getts. Om man vill gå djupare in på de tekniska detaljerna finns det mycket mera att lära. Det finns protokoller, arkitekturer, ISO, ECMA, ETSI standarder och mycket mera som förklarar tekniken så grundligt man någonsin kan kräva. Bekantande med dessa skulle ändå ta en betydligt längre tid.

Jag som skribent har också fått en mycket bra uppfattning om NFC och tycker ämnet har varit intressant att forska i. Fastän det inte fanns någon uppdragsgivare bakom arbetet, var det inte svårt att komma på vad man skulle skriva om. Det fanns mycket information om ämnet, ibland till och med för mycket, så man måste utelämna flera av de från början planerade källorna. Det var också lätt att få kontakt med människor som jobbat med ämnet och hade lång erfarenhet inom branschen.

NFC är något som man måste sprida till människor som inte har någon aning om vad det handlar om. Man hoppas ju på att det, allt eftersom företagen implementerar tekniken i sina tjänster, blir alltmer bekant för flera. Till exempel då jag frågade mina kolleger på Clas Ohlson om de visste vad NFC var, svarade nästan alla att de inte hade någon som helst aning om vad det var och vad det användes till.

KÄLLOR

Tryckta källor

Coskun Vedat, Ok Kerem, Ozdenizci Busra. 2012, *Near Field Communication: From Theory to Practice.*
Förlag: Wiley, United Kingdom
Antal sidor: 361

Intervju

Vaattovaara Risto, Gruppledare för Biljettssystemsavdelning i HSL. 2013, *Intervju om NFC och HSL.*
Intervjufrågor, se Bilagor.
Intervjun hölls: 13.2.2013, kl. 14:30.

Elektroniska källor

Android. 2012, *Android 4.2: A new flavor of Jelly Bean.*
Tillgänglig:
http://www.android.com/whatsnew/
Hämtad: 6.4.2013

Balaban. 2011, *NTT DoCoMo.*
Tillgänglig:
http://nfctimes.com/company/ntt-docomo
Hämtad: 1.4.2013

Blackberry. 2013, *NFC Primer for Developers.*
Tillgänglig:

http://supportforums.blackberry.com/t5/Java-Development/NFC-Primer-for-Developers/ta-p/1334857
Hämtad: 5.4.2013

Clark Sarah. 2012, *PayPal: "NFC will fail to gain mass adoption".*
Tillgänglig:
http://www.nfcworld.com/2012/12/18/321595/paypal-nfc-will-fail-to-gain-mass-adoption/
Hämtad: 1.4.2013

Clark Sarah. 2013, *Hyundai shows off NFC car key concept*
Tillgänglig:
http://www.nfcworld.com/2013/01/08/321777/hyundai-shows-off-nfc-car-key-concept/
Hämtad: 25.3.2013

Curran Kevin, Miller Amanda, Mc Garvey Conor. 2012, *Near Field Communication.*
Tillgänglig:
http://www.iaesjournal.com/online/index.php/IJECE/article/view/234
Hämtad: 1.4.2013

Dignan Larry. 2013, *MasterCard launches MasterPass: Will this digital wallet fly?*
Tillgänglig:
http://www.zdnet.com/mastercard-launches-masterpass-will-this-digital-wallet-fly-7000011771/
Hämtad: 1.4.2013

GoogleDevelopers, YouTube. 2011, *Google I/O 2011: How to NFC.*
Tillgänglig:
http://www.youtube.com/watch?v=49L7z3rxz4Q
Hämtad: 1.4.2013

GoogleDevelopers, YouTube. 2012, *Google I/O 2012 – Up Close and Personal: NFC and Android Beam.*

Tillgänglig:
http://www.youtube.com/watch?v=HkzPc8ZvCco
Hämtad: 1.4.2013

Havumäki Maaria. 2013, *HSL tarjoaa kahden viikon ilmaiset matkat.*
Tillgänglig:
http://trombit.net/2013/04/05/hsl-tarjoaa-kahden-viikon-ilmaiset-matkat/
Hämtad: 7.4.2013

Kerschberger Martin. 2011, *Near Field Communication: A survey of safety and security measures.*
Tillgänglig:
https://www.auto.tuwien.ac.at/bib/pdf_TR/TR0156.pdf
Filnamn: TR0156.pdf
Hämtad: 25.3.2013

Kesko. 2012, *Lähiluettava K-Plussa-kortti valittiin parhaaksi NFC-konseptiksi Suomessa.*
Tillgänglig:
http://www.kesko.fi/fi/Kaupat-ja-palvelut/Ajankohtaista/Lahiluettava-K-Plussa-kortti-valittiin-parhaaksi-NFC-konseptiksi-Suomessa/
Hämtad: 28.3.2013

Koistinen Ossi. 2010, *NFC-tekniikka.*
Tillgänglig:
http://publications.theseus.fi/handle/10024/24246
Hämtad: 25.3.2013

Kumar Anurag. 2010, *NEAR FIELD COMMUNICATION.*
Tillgänglig:
http://dspace.cusat.ac.in/jspui/bitstream/123456789/2214/1/NEAR%20FIELD%20COMMUNICATION.pdf
Hämtad: 25.3.2013

Kurtti Joni. 2011, *Mobiilipalvelut ja NFC.*
Tillgänglig:
http://publications.theseus.fi/handle/10024/34126
Hämtad: 1.4.2013

Liikenne- ja viestintäministeriö. 2010, *Near Field Communication: NFC-työryhmän loppuraportti.*
Tillgänglig:
http://www.lvm.fi/c/document_library/get_file?folderId=1551284&name=DLFE-11779.pdf&title=Julkaisuja%204-2011
Hämtad: 1.4.2013

Lui Spandas. 2012, *PayPal yet to give up on NFC.*
Tillgänglig:
http://www.zdnet.com/au/paypal-yet-to-give-up-on-nfc-7000007367/
Hämtad: 1.4.2013

Lui Spandas. 2013, *Samsung-Visa alliance to boost NFC payments adoption.*
Tillgänglig:
http://www.zdnet.com/samsung-visa-alliance-to-boost-nfc-payments-adoption-7000011810/
Hämtad: 1.4.2013

Mainio Tapio. 2013, *Oulussa opiskellaan suomea kännykän ja älytarrojen avulla.*
Helsingin Sanomat, 15.1.2013.

MasterCard. 2013, *What is PayPass NFC?*
Tillgänglig:
http://www.mastercard.com/us/paypass/phonetrial/whatispaypass.html#
Hämtad: 1.4.2013

Miller Charlie. 2012a, *Exploring the NFC Attack Surface.*
Tillgänglig:
http://media.blackhat.com/bh-us-12/Briefings/C_Miller/BH_US_12_Miller_NFC_attack_surface_WP.pdf
Hämtad: 1.4.2013

Miller Charlie. 2012b, *Attacking NFC.*
Tillgänglig:
http://2012.video.sector.ca/video/51115364
Hämtad: 1.4.2013

Murph Darren, Engadget. 2012, Android 4.1 Jelly Bean review: a look at what's changed in Google's mobile OS.
Tillgänglig:
http://www.engadget.com/2012/06/28/android-4-1-jelly-bean-review-a-look-at-whats-changed-in-googl/
Hämtad: 1.4.2013

NFC-Forum. 2013a, *NFC in Action.*
Tillgänglig: http://www.nfc-forum.org/aboutnfc/nfc_in_action/
Hämtad: 5.4.2013

NFC-Forum. 2013b, *NFC and Contactless Technologies.*
Tillgänglig:
http://www.nfc-forum.org/aboutnfc/nfc_and_contactless/
Hämtad: 6.4.2013

NFC-Forum. 2007, *NFC Forum Issues Specifications For Four Tag Types.*
Tillgänglig:
http://www.nfc-forum.org/news/pr/view?item_key=2c0cb92de7d47bbbe7c99f13912b3307fc03c1c6
Hämtad: 7.4.2013

Nordström Daniel, Nyqvist David. 2012, *Near Field Communication: En studie av säkerhetsaspekternas påverkan för mobila betalningar.*
Tillgänglig:
http://uu.diva-portal.org/smash/record.jsf?pid=diva2:545449
Hämtad: 1.4.2013

OP-Pohjola. 2013, *Aamulehti: Etäluettava maksukortti vähentää pin-koodin näppäilyä.*
Tillgänglig:
https://www.op.fi/op/op-pohjola-ryh-ma/uutishuone/?id=80300&srcpl=1#/mediassa/5496/etaluettava_maksukortti_vahentaa_pin-koodin_nappailya!1363715323
Hämtad: 1.4.2013

PayPal. 2013, *PayPal Here. There. Anywhere.*
Tillgänglig:
https://www.paypal.com/webapps/mpp/credit-card-reader
Hämtad: 1.4.2013

Rahman Mahbub, Willee Hamish. 2012, *Understanding NFC Data Exchange Format (NDEF) messages.*
Tillgänglig:
http://www.developer.nokia.com/Community/Wiki/Understanding_NFC_Data_Exchange_Format_(NDEF)_messages
Hämtad: 25.3.2013

Samsung. 2012, *What is S Beam, and how do I use it?*
Tillgänglig:
http://www.samsung.com/us/support/supportOwnersHowToGuidePopup.do?howto_guide_seq=7042&prd_ia_cd=N0000003&map_seq=48157
Hämtad: 1.4.2013

Sefedini Arban, Al-Ashraf Samir Daniel. 2010, *Prototyper för NFC implementeringar.*

Tillgänglig:
http://dspace.mah.se/handle/2043/10319
Hämtad: 28.3.2013

Wikipedia. 2013a, *Near field communication.*
Tillgänglig:
http://en.wikipedia.org/wiki/Near_field_communication
Hämtad: 6.4.2013

Wikipedia. 2013b, *Bluetooth.*
Tillgänglig:
http://en.wikipedia.org/wiki/Bluetooth#Uses
Hämtad: 28.3.2013

Yellowdoggdesigns. 2012, *Featured Friday Freebie: PayPal Here.*
Tillgänglig:
http://blog.yellowdoggdesigns.com/featured-friday-freebie-paypal-here/
Hämtad: 6.4.2013

BILAGOR

Bilaga 1. Intervju

Intervjufrågor:

- Hurudan feedback har ni fått på det nuvarande systemet som baserar sig på smart-korten?
    - Vad har varit de goda och de dåliga sidorna med systemet?
- Har ni några NFC baserade tjänster tillgängliga just nu?
- Vilka NFC baserade tjänster är på kommande/under planering?
- Vilka är de största utmaningarna då man vill införa ett nytt system baserat på NFC?
- Skall de nuvarande resekorten implementeras i telefonerna?
- Skulle det vara möjligt och samarbeta med SIM-kortstillverkaren och således få SIM-kort med integrerad NFC funktionalitet?
- Har någon försökt hacka sig in i ert smartkortssystem och till exempel försökt ladda värde på korten? (Korten går att läsa med flera applikationer från Androids Play Store)
- På vilka sätt kan man finansiellt dra nytta av ett system baserat på NFC implemente-rat i telefonerna?
    - Några förslag skulle vara: underlättandet av resekortens laddning, borttap-pandet av resekort och produktion av resekort.