Near Field Communication och ett praktiskt exempel på användbarheten

Trond Larsen

Examensarbete
Informations- och medieteknik
2013

Trond Larsen
Sammandrag:


Nyckelord: Near Field Communication, NFC-teknik, RFID, trådlös teknik, automatisk identifiering, Bluetooth, Smartkort, Säkerhetsattacker

Sidantal: 42
Språk: Svenska
Datum för godkännande: 30.4.2013
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

<table>
<thead>
<tr>
<th>Keywords</th>
<th>Near Field Communication, NFC-technology, RFID, wireless technology, automatic identification, Bluetooth, Smartcards, Security attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of pages</td>
<td>42</td>
</tr>
<tr>
<td>Language</td>
<td>Swedish</td>
</tr>
<tr>
<td>Date of acceptance</td>
<td>30.4.2013</td>
</tr>
</tbody>
</table>
## INNEHÅLL

1 Inledning........................................................................................................................................... 7
   1.1 Bakgrund....................................................................................................................................... 7
   1.2 Syfte ............................................................................................................................................. 8
   1.3 Avgränsning .................................................................................................................................. 8
   1.4 Metoder ........................................................................................................................................ 8
   1.5 Terminologi .................................................................................................................................. 9

2 NFC teknologin .................................................................................................................................. 11
   2.1 Olika sätt att kommunicera ........................................................................................................ 11
       2.1.1 Peer to Peer - läge ............................................................................................................... 12
       2.1.2 Reader/Writer - läge .......................................................................................................... 13
       2.1.3 Kortemuleringsläge ............................................................................................................ 13
   2.2 Hårdvaran ..................................................................................................................................... 13
       2.2.1 Taggar .................................................................................................................................. 15
   2.3 NDEF ......................................................................................................................................... 16
   2.4 NFC i jämförelse med andra trådlösa tekniker .......................................................................... 17
       2.4.1 RFID ..................................................................................................................................... 17
       2.4.2 Bluetooth ............................................................................................................................ 18

3 Användningsområden ......................................................................................................................... 20
   3.1 Betalning ....................................................................................................................................... 21
   3.2 Android ........................................................................................................................................ 23
   3.3 Andra användningsområden ......................................................................................................... 25

4 Säkerheten ......................................................................................................................................... 27
   4.1 Olika metoder för attack ............................................................................................................. 27
       4.1.1 Avlyssning ........................................................................................................................... 27
       4.1.2 Datakorruption .................................................................................................................... 28
       4.1.3 Data-modifiering ................................................................................................................ 28
       4.1.4 Införande av data ............................................................................................................... 29
       4.1.5 Tredjepartsattack .............................................................................................................. 29
   4.2 Slutsatser om säkerhet ................................................................................................................ 29

5 HSL och NFC ..................................................................................................................................... 31
   5.1 Allmänt ......................................................................................................................................... 31
   5.2 Utvecklingen mot NFC ................................................................................................................. 32

6 Avslutning .......................................................................................................................................... 34
Figurer

Figur 1. NFC teknologins olika arkitekturer. (NFC-Forum, 2013a) ......................... 12
Figur 2. En Blackberry telefons NFC arkitektur. Här fungerar BlackBerry applikationerna som Host Controller. (Blackberry, 2013) ................................. 14
Figur 4. Ett antal olika taggar. ........................................................................... 16
Figur 5. Så här ser ett NDEF meddelande ut. (Rahman & Willee, 2012) .............. 17
Figur 6. Hastigheter och räckvidd för trådlösa teknologier. (NFC-Forum, 2013b) ... 19
Figur 8. PayPal Here kortläsaren. (Yellowdogdesigns, 2013) ................................. 22
Figur 10. Touch to Beam funktionen i S Beam. (Samsung, 2012) ......................... 25
Figur 11. Det nuvarande gröna resekortet och kortläsaren. (Havumäki, 2013) ........ 32
Figur 12. Till vänster: Framsidan av HSL:s resekortsapplikation. Till höger: Ett resekort är avläst och informationen visas på skärmen. ............................................. 33
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 interactionen 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 telefongen då man köper biljetter och till och med som betalningssystem.

På grund av tidpunkten 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 fortskrids inom det området.

1.3 Avgränsning


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 stämmar 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-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 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


2.1 Olika sätt att kommunicera

2.1.1 Peer to Peer - läge

Peer to Peer kallas läget då två NFC kompatibla enheter kommunikerar 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


2.1.3 Kortemuleringsläge


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. Där- till har vi en Host Controller som kan vara till exempel själva telefonen och applikatio-

![Diagram](image)

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

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)

![Diagram of an RFID/NFC tag](image)

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


- **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 att 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.

![Bild av olika taggar](image)

*Figur 4. Ett antal olika taggar.*

### 2.3 NDEF


2.4 NFC i jämförelse med andra trädlösa 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 skivas på eller också läsas 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


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.

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 självtjänster efterföljare för till exempel äldre passeringskontroll och betalningssätt.


### 3.1 Betalning


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


![PayPal Here kortläsaren. (Yellowdoggdesigns, 2013)](image)

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-
ning. 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)


### 3.2 Android

3.3 Andra användningsområden


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 skärmens som ett ord. Därefter 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. (Ma
nio, 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
- Rabatkuponger
- 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


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.

4.1.4 Införande av data

När två enheter kommunikerar 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 svarsmeddelanden skickas samtidigt tolkas det som en korruption i data.


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 nätilda 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)

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 utnyttjt 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 biljettsystemsavdelning. Det har också gjorts en del tester med olika NFC aplikationer. (Vaattovaara, 2013)

5.1 Allmänt


**5.2 Utvecklingen mot NFC**


![Skämdump ur applikationen för Android](image1)

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


Jag som skribent har också fått en mycket bra uppfattning om NFC och tycker ämnet har varit intressant att förska 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 Biljettsystemsavdelning i HSL. 2013, Intervju om NFC och HSL.
Intervjufrågor, se Bilagor.

Elektroniska källor

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:
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

Tillgänglig:  
Hämtad: 1.4.2013

Tillgänglig:  
Hämtad: 1.4.2013

Tillgänglig:  
http://www.youtube.com/watch?v=49L7z3rxz4Q  
Hämtad: 1.4.2013

Hämtad: 1.4.2013
Tillgänglig:
http://www.youtube.com/watch?v=HkzPc8ZvCeo
Hämtad: 1.4.2013

Tillgänglig:
http://trombit.net/2013/04/05/hsl-tarjoaa-kahden-viikon-ilmaiset-matkat/
Hämtad: 7.4.2013

Tillgänglig:
https://www.auto.tuwien.ac.at/bib/pdf_TR/TR0156.pdf
Filnamn: TR0156.pdf
Hämtad: 25.3.2013

Tillgänglig:
Hämtad: 28.3.2013

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

Tillgänglig:
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:
Hämtad: 1.4.2013

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
Tillgänglig:
Hämtad: 1.4.2013

Miller Charlie. 2012b, *Attacking NFC.*
Tillgänglig:
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:
Hämtad: 1.4.2013

Tillgänglig: http://www.nfc-forum.org/aboutnfc/nfc_in_action/
Hämtad: 5.4.2013

Tillgänglig:
http://www.nfc-forum.org/aboutnfc/nfc_and_contactless/
Hämtad: 6.4.2013

Tillgänglig:
http://www.nfc-forum.org/news/pr/view?item_key=2c0cb92de7d47bbbe7c99f13912b3307fc03e1e6
Hämtad: 7.4.2013

Tillgänglig:


Hämtad: 1.4.2013


Tillgänglig:

https://www.op.fi/op/op-pohjola-ryh-ma/uutishuone/?id=80300&srepl=1#/mediassa/5496/etaluettava_maksukortti_vahentaa_pin-koodin_nappailya!1363715323

Hämtad: 1.4.2013


Tillgänglig:

https://www.paypal.com/webapps/mpp/credit-card-reader

Hämtad: 1.4.2013


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:


Hämtad: 1.4.2013

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

Tillgänglig:
http://en.wikipedia.org/wiki/Bluetooth#Uses
Hämtad: 28.3.2013

Tillgänglig:
Hämtad: 6.4.2013
BILAGOR

Bilaga 1. Intervju

Intervjufrågor:

- Hurudan feedback har ni fått på det nuvarande systemet som baserar sig på smartkorten?
  - 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 implementerat i telefonerna?
  - Några förslag skulle vara: underlättandet av resekortens laddning, borttappandet av resekort och produktion av resekort.