UNIVERSITY OF OSLO
Department of informatics

Investigation of security features in Near-field communication (NFC)

Master thesis

60 credits

Øyvind Berget

1st November 2008

Abstract

With the increasing use of NFC and RFID technology it is important to look at the security, both for the user and for the system owner to see that the system is reliable. NFC is a standard inheriting some of the RFID standards and it is important to see how the old standards have handled security and how it is handled in NFC. There are certain RFID systems that are already in use, which is especially close to NFC. For example is Mifare a system used in many public transportation systems as ticket and in contactless access cards. Another example is electronic passports which uses a standard which is included in NFC. Examining the security in these and also investigate the use of NFC tags to make secure use of them is the focus in this thesis.

Acknowledgment

I would like to thank Prof. Josef Noll for his constructive discussions, support and advices. He has made this paper possible. I would also like to thank György Kálmán for his advices, support and helpful ideas. I also want to thank Kjell Myksvoll at Telenor for his knowledge and help when I have had problems. I would like to thank Encap and especially Arne Riiber, Gjermund Johre and Petter Taugbøl who have been helpful and have had some nice inputs. In the end I want to thank Knut Eilif Husa at Tellu.

Table of contents

1. Motivation

Whenever a new technology comes to market there are certain areas in which the technology was first thought of, but it might be other areas the technology will have impact as well. Near Field Communication (NFC) is an upcoming technology that will impact the daily life of people. The NFC technology has been developed for certain aspects and the designers have used those aspects when developing it, but they have not looked at every way it might be used. Looking at brand new technology and look at different security aspects, it has a quite large probability that some new ideas and sides could be found that the developers have not yet thought of. Therefore it is very interesting to look at NFC and related technology and try to explore ways that could impact the way people and machines will interact.

The research to investigate security functions in NFC led into areas and problems that I did not see before I started. Radio Frequency Identification (RFID) technology in passports have similarities with NFC that at first was not important, but looking at security I found those similarities interesting. Internet bank security is something that do not relate at first to NFC neither, but I found that this is an area which could benefit from NFC technology.

The thesis was done in cooperation to Encap[1], which wanted to look at benefits combining their technology with NFC. Also Tellu[2] and Telenor[3] have been important partners during the investigation to this thesis.

[1] http://www.encap.no/

[2] http://www.tellu.no/tellu-web/tellu_webpage.html

[3] http://www.telenor.no/

2. Introduction

NFC and RFID technologies have evolved into a phase where it is integrated into various systems for general public use. Commercially available mobile phones are now starting to have NFC technology integrated. With the increasing use of NFC and RFID technology it is important to look at the security aspects of these, both for the user and for the system owner to see that the system is reliable. In this thesis I will look at some of the pitfalls that exist in Norwegian electronic passports and Mifare. Explaining ways to make this technology more secure is also an area of focus in this paper. Within this area I have also looked at the use of NFC peer-2-peer technology for enhancing computer security.

3. Scenario

RFIDs have been used for many years and are used in everything from alarm in shops, controlling content of stores and in ticketing systems. NFC is a standard inheriting some of the RFID standards and it is important to see how the old standards have handled security and how it is handled in NFC.

There are certain RFID systems that are already in use, which is especially close to NFC. For example is Mifare a system used in many public transportation systems as ticket and in contactless access cards. Another example is electronic passports which uses a standard which is included in NFC.

I will examine the security in these and also investigate the use of NFC tags to make secure use of them. Passports are documents which the citizens of the state would have to trust. Failing to have trust in passports would be critical for the society to actually accept identity.

NFC as a tool for increasing security should be an area which should be examined. For example could it be possible to increase security for authentication or using NFC as an enabler for making a secure authentication. Comparing solutions of current web authentication systems with solutions using NFC is done in this thesis to see the advantages in NFC.

4. Technological overview

To understand the security measures and the security pitfalls in a technology it is necessary to understand the underlying and related technology. This chapter will present an overview of different kind of relevant technology as well as the underlying theory.

4.1 Radio Frequency Identification

RFID was initially invented during the Second World War[1]. RFID is a system consisting of two parts. One of the parts, the reader, is sending radio signals to the other part, sending commands like read or write information. The other unit, tag or responder, will answer either by using the energy received from the transmission or by using its own power source to transmit the response. A RFID tag has an antenna which will utilise the emitted power to generate power for the chip in the tag. Just enough to do the commands told and then reply back. A system which uses the power it receives to respond is called passive RFID system. The ones with its own power source are called an active RFID system. Both will return an answer which the reader part interprets.

There is a wide range of RFID systems. It could be used to store medical information about a patient or it could be used for alarms. But the way it works is the same. One reader send out emitting power which will wake the other part and the other part will respond to the challenge from the reader. In an alarm system this will make the alarm go off. In other systems such as tickets for public transport it will count down the uses left on the ticket. But this is the result of the background system connected with the reader.

4.2 Near Field Communication

NFC is a form of contactless communication closely related to RFID. NFC communicates between a device to another device or a certain type of RFID tag. The standard is supported by the NFC Forum which consists of leading cooperations such as Philips, Nokia, Sony, Visa, Microsoft and Panasonic[4]. The NFC Forum works for a standard for easy and secure communication between devices being a few centimetres close to each other. Contactless infrastructures are used amongst others in public transportation as bus ticket, payment and ski elevator systems. NFC incorporates some of the existing proximity and contactless standards. ISO 14443 A and B and FeliCa are the basic protocols used in NFC for contactless communication. These standards are inherited from RFID technology and enables NFC to be compatible with many existing infrastructures. The ability to have a two-way communication between two active parts is included into the standard as well. The two-way communication standard is described through the NFCIP-1 protocol explained in ISO standard 18092. NFCIP-2 is a protocol for investigating which technology standard to set up a communication session with. This protocol allows the use of all of the NFC Forum standard and the proximity standard ISO15693. They both use the same frequency, 13.56 MHz, as ISO 14443 but the difference is that proximity cards is able to communicate over a greater distance than the NFC Forum technology is. NFCIP-2 makes the protocol selection process invisible for the user, so the standard used in the communication is not something the user will have to understand.

4.2.1 Modes of operation

To explain the NFC technology, it is necessary to look at the basic idea of NFC. NFC is in general terms a communication between two entities over RFID technology.

	Initiator	Responder
Active use	Active	Passive
Emulate tag	Passive	Active
Peer-to-peer	Active	Active

Table 1: Different modes of NFC for two devices communicating [2]

[4] http://www.nfc-forum.org/member_companies/

There are two communication modes for a device, a passive and an active, although a device might only be passive or active. This makes three possible modes of operation. The first possible mode is when an initiator, active part, communicates with a passive device or a tag. Another communication for an active device is emulating that it is a tag and then work as a passive device. This is only a slight modification of the first mode of operation, as it just implies that an active device might be used in a passive way. The third mode is when both devices are active.

The emulated tag could reside in either the phone itself or in the Subscriber Identity Module (SIM). The GSM Association (GSMA) has made a drawing of how different NFC elements in the phone interact. The NFC application interface (API NFC) on the Universal Subscriber Identity Module (USIM), which is shown in figure 1, is only introduced in some demonstration phones. The functionality of this API is implemented through a Secure Element (SE) in the phone.

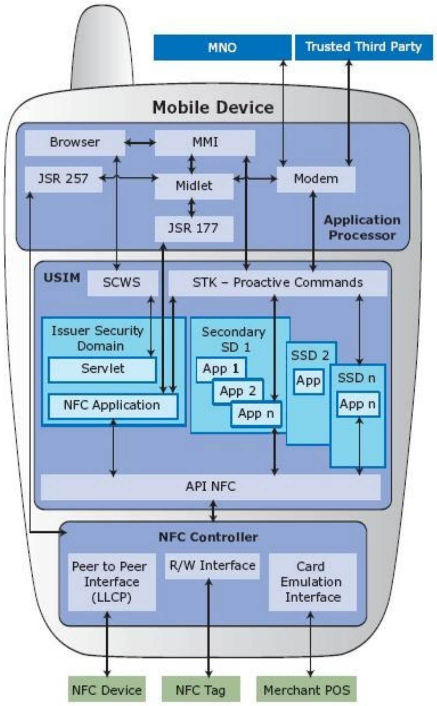


Figure 1: Interaction between different parts of a NFC phone[5]*.*

[5] http://cenriqueortiz.com/images/nfc/gsma-mobile-NFC-device-functional-architecture.jpg

The use of the different modes is dependent on the task of the system is. The modes make it possible to have a variety in how to communicate with user and the system.

4.2.2 NFC operations

NFC technology has a set of modes. Because of former standards, which all communicates in different ways, that are merged into NFC and also new development that allow a higher bandwidth, different type of physical characteristics are existing in NFC. The data rates of 106, 212 and 424 Kbit/s are making it possible to transfer small amounts of data between devices in all modes. The selection of transmitting speed depends on the tag that is used and is selected during communication set-up. NFC devices use a frequency of 13.56 MHz. This is a spectrum, which is secured for Industrial, Scientific and Medical (ISM) use in most countries. ISM bands are unlicensed, where there are some few restrictions, but everyone might use the frequencies.

ISO 14443 A and B are structured into four parts. A and B differs in two parts [3].

1. Physical characteristics
2. Radio frequency power and signal interface (Different in A and B).
3. Initialisation and anti-collision (Difference in A and B).
4. Transmission protocol.

In general terms the two standards are not similar when it comes to encoding of signals with bits and bytes and electronic properties such as how the magnetic coupling interacts with tags and how communication between multiple tags is handled. For example ISO 14443 B is using a modulation form in the magnetic coupling which allows both the reader and the card to have power continuously during a communication session. ISO 14443 A cannot do this.[3] The NFC standard supports both ISO standards so the difference is not notable for the user. Still the standard might give different aspect when it comes to devices supporting it. The NFC standard is flexible and if a device does not support every part it could still be a NFC device. Eventually the support for both standards will hopefully be implemented in every device.

To transfer NFC information from one device to or from a tag or another device, a standard encapsulated format is used. The NFC Data Exchange Format (NDEF) describes how information should be sent and organised in the exchange. The standard contains only information on how to organise the information transferred and does not define what is transferred or how the transmission is done. Two NFC devices close to each other will start sending NDEF messages over the NFC Forum Logical Link Control Protocol which is a part of ISO18092, but when a device is close to a tag it will start communicating NDEF messages over the specific tag protocol[4][5].

Because of the NDEF, there is a need for a standard which informs the devices on metadata that is received or sent. NFC Forum has defined different Record Type Definitions (RTD), which defines how metadata should be interpreted. A service provider using a tag could define the tag with their own RTD. Alternatively there are three predefined RTDs from the NFC Forum. The predefined RTDs are Text, Universal Resource Information (URI) and Smart Poster (SP).

- Text RTD is information that contains plain text information.
- SP RTD is for posters containing information with text, audio and or other types of data.
- The URI RTD is for internet resources.
- SP RTD could be considered an expanded version of URI RTD, but is defined in a separate specification at NFC Forum.

4.2.3 NFC Tags

Currently there are four types of tags that are specified[6]. Although all the tags are member of these standard tags, the speed and the size of the tags are different from

[6] http://www.nfc-forum.org/specs/

type to type. Some existing infrastructure use these tags already and it is easy to convert these existing infrastructures into using NFC. The following list describes the four different types.

Type	Name	Manufacturer	Size	Speed	Standard
Type 1	Topaz	Innovision	96 byte	106 Kbit/s	ISO 14443 A
Type 2	Mifare Ultralight	NXP (Philips)	48 byte	106 Kbit/s	ISO 14443 A
Type 3	FeliCa	Sony	1 Mbyte	212, 424 Kbit/s	(JIS) X 6319-4
Type 4	Mifare DESfire	NXP (Philips)	32 Kbyte	up to 424 Kbit/s	ISO 14443 A B

Table 2: Types of NFC Forum defined tag[4].

Figure 2: Tags stickers[7].

Even though these tags are the defined NFC tags, there may also be some other tags supported, which use different chips. For example Mifare Classic 1k and 4k or Innovision Jewel tags. A device that is able to read a NFC tag can read other ISO14443 tags as well.

4.2.4 NFC availability

NFC has not been commercially available except some projects and it has been made just a handful of phones with NFC capability. Even though the commercially available phones are a scarce, Nokia released their first regular phone with NFC technology in the 3rd quarter of 2008, the Nokia 6212 Classic. BBC claimed in early 2008 that NFC

[7] http://www.mulliner.org/nfc/nfcimages/sticky_tags/index.html

would become one of the top technologies starting to make it big in 2008[8]. One of the reasons they think this is because of the intuitive use of NFC.

Movation has an analysis on the market penetration for different kinds of mobile technologies 2008 to 2010[6]. They predict that NFC will reach the market in the first quarter of 2008 and that ten percent have tried NFC in 2010, but with Nokia's release of Nokia 6212 Classic in the 3rd quarter of 2008 the predictions could be half a year too early.

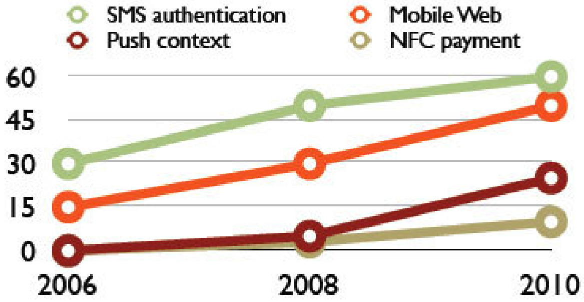


Figure 3: Expected customer usage in precent "have tried" of mobile services in the Nordic Market [6].

NFC is a highly flexible system that supports a large set of applications. Because none interoperable RFID systems make confusion, some national standards have adopted parts of NFC. An example is the Norwegian Specification for Interoperable Electronic Ticketing System using the DESFire tag, which is NFC type 4 tag, as the standard for new ticketing system [7] . The standard is implemented so that it should be possible to use one card everywhere. Another system using ISO14443 is the electronic passport, which is a standard from the International Civil Aviation Organisation (ICAO)[8]. ID-card for building workers will have ISO14443 A as a minimum [9][10]. This shows that NFC technology will be used in future systems and have become standard in places where RFID technology would be convenient.

[8] http://news.bbc.co.uk/2/hi/programmes/click_online/7182701.stm

4.3 Bluetooth

Bluetooth got its name from a Scandinavian king who united the Danish, Norwegian and Swedish kingdoms during the Viking age[9]. The technology was named so, because the idea of using technology to interact between several devices through wireless communication in a Personal Area Network (PAN). The Bluetooth Special Interest Group (SIG) is a collection of companies that is implementing and developing the standard. The Bluetooth SIG is a non-profit organization.

The main objective of Bluetooth is to connect devices up to 10 meters a part [11], but some classes is even able to communicate up 100 meters. As the wireless communication standard Bluetooth operates in the ISM frequency band of 2.4 GHz. It is using the available frequency spectrum through Frequency Hopping Spread Spectrum (FHSS) which make the system more resilient against interference. Bluetooth is using a master-slave system to communicate. One master might have seven active slaves and up to 255 parked slaves. Such network is a piconet. One device maybe in several piconets, but can only be a master in only one. Several interconnecting piconets are called scatternet. The communication between the devices in a piconet is shared through Time Divided Multiplexing (TDM).

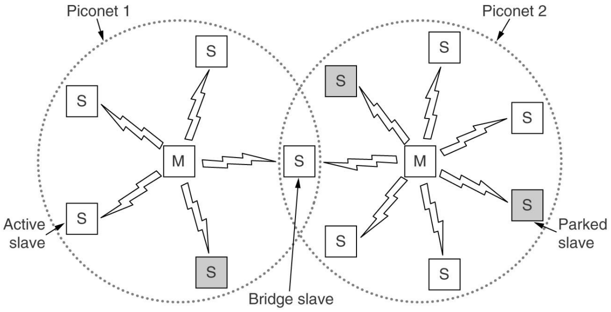


Figure 4: Two piconets connected to a scatternet [11]

Two Bluetooth devices must in many cases be connected by sharing a pin code to establish a secure communication. After the initial connection the two devices will be able to connect later without user interaction. The initialisation between the two

[9] http://www.bluetooth.com/Bluetooth/SIG/

devices takes care of the secure connection as mentioned earlier, but it will also negotiate what kind of services the two devices support. If they support a compatible protocol they will be able to use those services. Pairing of Bluetooth devices is possible through NFC technology.

4.4 Man-in-the-middle

Man-in-the-middle (MITM) is an attack where the malicious entity E appears between A and B. E will then act as A for B and vice versa[10]. To successfully accomplish a MITM attack messages between A and B will have to be stopped by E and E will have to send out message pretending to be A or B. E will by this be able to manipulate the way both A and B will act.

For example could a MITM attack on the internet work like this:

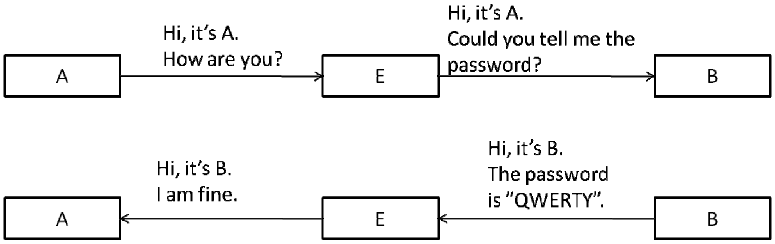


Figure 5: MITM attack

1. Entity A want to chat with B
2. A greets B and ask a question
3. E greets B as A did and ask a question about a password
4. B replies E as it thinks it is A with the password
5. E response A saying everything is good

In this example both A and B thinks that they have a connection that could be trusted. This is obviously not something they should, but there are ways to protect against such attacks.

[10] http://www.schneier.com/crypto-gram-0404.html#6

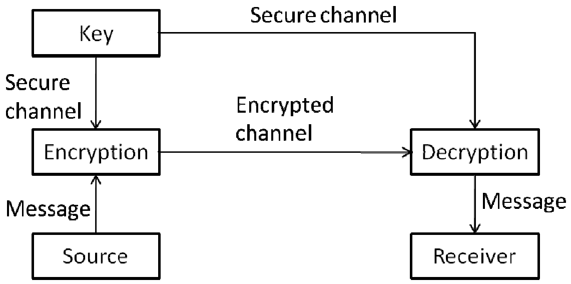


Figure 6: Cryptography with a secure channel

One of the basic defences for this attack is to share a secret key through a secure channel and then use this secret to encrypt the unsecured channel. It should be an easy defence, but the difficulties arise when the secure channel should be established. MITM could work on a secure channel as well. Therefore MITM is an attack form which is difficult to handle in a digital world because it needs trust which is difficult to make.

4.5 Digital certificates

An individual person has his own identity in the real world. To prove the identity it is often necessary to use a passport or other means of ID-cards. Digital Certificates is a way of having ID-cards in the digital world. All tough it has several functions as non-repudiation, secure authentication and integrity protection. It could act as a signature as well. A digital certificate would prove that the person that has a certain object, for example an e-mail, signed is the person who has written it.

Using a digital certificate is possible because the use of asymmetric cryptography, where it is possible to encrypt a message with one key and another key is needed to decrypt the message. The encryption and decryption key have a mathematical connection between them. The way the two keys are calculated it is not feasible, within an accepted time limit, to calculate that connection. This is known as public key cryptography.

The main difference between signing a document and encrypting it is which key to use. In encryption the public key is used to encrypt. Then the message is only readable by the ones that have the private key. But if the message is encrypted with the private key, then everyone with the public key could read it. This makes it impossible to alter the message, because it would have to be encrypted with the secret private key. It could also be that a signature is added by hashing the message and then encrypt only the hash with the private key and add it to the message.

The main problem with digital certificates is the trust of the certificate or in a setup face it could be vulnerable for man-in-the-middle attacks. It could also be stolen on the computer. Digital certificates are used in many applications, for example in Java programs on mobile phones and other applets in web pages even though they have some weaknesses it is secure enough for many applications.

4.6 Communication with smartcards

Communication with NFC chips is defined in NFC standards. But it also allows the use of Application Protocol Data Unit (APDU), an ISO standard for communicating with smartcards. The unit communicating with APDU to a smartcard or other chip it is first requesting an application to be run. After that the unit starting the communication will order the chip to do certain functions. The commands are usually only series of numbers which are sent and translated into functions. The chip will answer through the communication and that makes it hard to read information from the chip unless the reader knows what it should ask for. Smartcards also have the capability to encrypt and decrypt information.

4.7 NFC telephones

As mentioned earlier a limited range of NFC phones is available[11]. Most of the available phones are to test out the technology. Nokia initially released two phones, Nokia 6131NFC and Nokia 3220 with a special chip and cover, which both mainly are

[11] http://www.nfcnews.com/articles/2008/01/14/contactless-market-continues-to-grow-while-nfc-forecasts-revised-downward

used for development and they have released a third phone in the third quarter of 2008 which is aimed towards consumer market.

Today only the Sagem-Orga my700X supports the Single Wire Protocol (SWP) protocol implemented. In the future SWP might be used to communicate with the SIM card and use it as the Secure Element (SE). The operators want the SE to be in the SIM card and the manufacturers want the secure element to be in the phone. The Sagem-Orga phone has an operative SE when it is turned off. Samsung, BenQ and Motorola have also developed their own NFC telephones[12].

4.7.1 Nokia 6131 NFC

One of Nokia's NFC phones is the Nokia 6131 NFC. The phone has NFC hardware and software as well as other communication possibilities like Bluetooth, Infrared and GSM, but no UMTS[13]. This phone runs the Series 40 3rd edition platform. The software environment which programs might run in is Java ME. There is also possible to develop application on Java Card. The OS on the Java Card is Giesecke & Devrient’s (G&D) Sm@rtCafé Express 3.1.

4.7.1.1NFC interface on the phone

The phone can operate in the three different modes that NFC technology allows. First the phone can read and write tags and smart cards. The phone supports all NFC Forum defined tags[12] and some RFID standards not a part of NFC like Mifare classic. In this mode the phone acts as an initiator.

[12] http://www.nfc-research.at/index.php?id=45

[13] http://www.forum.nokia.com/devices/6131_NFC

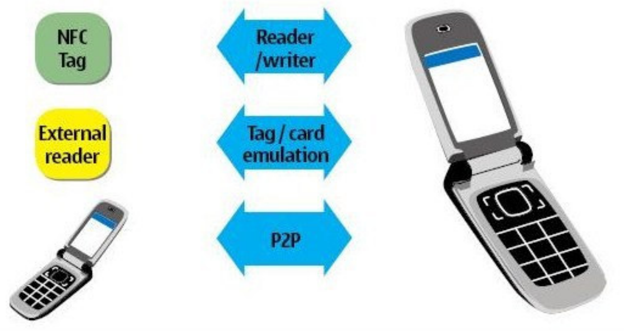


Figure 7: Modes of Nokia 6131 NFC[12].

As a second mode the phone acts as a tag or contactless card. In this mode the other part cannot tell the difference between the phone and a contactless card or tag. A secure element is integrated into the phone which can be used in this and the other modes. The element stores data for applications like ticket or payment systems. The secure element is able to emulate Mifare 4k and Java Card on Global Platform. This makes the phone compatible with a selection of existing contactless reader infrastructure. As a third and last mode there is a peer-to-peer mode. Then there are two phones or another NFC device that can communicate and share information through the NFCIP-1 protocol. The phone will switch between these modes without the users interaction.

The NFC communication of the phone is done through a modem with an antenna made for this purpose. This modem will distribute the information going in and out of the phone and channels the information to right module. External communication from phone environment to Java Card is using the ISO 14443 specification. For tag emulation the modem will send information to and from the secure element and the phone environment. The secure element is divided into a Java Card part and a Mifare 4k part. Mifare 4k is used for storage and the Java Card part can run Java Card applets. Both the phone environment with Java ME and the Java Card environment are able to communicate with the secure storage. The Java ME can communicate with the SIM.

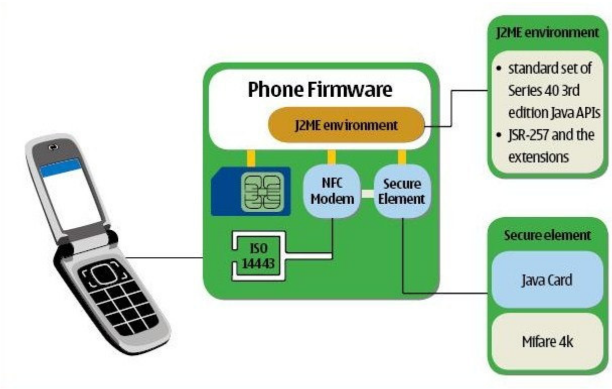


Figure 8: Architecture of Nokia 6131 NFC[12]

As a security feature the phone ask the user when an external device want to connect to the Secure Element. This is easy for the user to accept or deny, but it makes it impossible for the NFC tag emulation to function without battery. This could also be a disadvantage. Users are used to not have power left on the phone, but they would probably not accept that they might not be able to use subways or buses without power.

4.7.1.2Programming interface

The Java environment consists of Connected Limited Device Configuration (CLDC) 1.1, Mobile Information Device Profile (MIDP) 2.0 and several Application Programming Interfaces (API's). The API for NFC is described in Java Specification Request (JSR) 257. Nokia has released an SDK for this specific telephone.

Java application run with MIDP 2.0 is called midlets. The midlets can start up at user initiative or by actually respond to right activity on a communication interface like NFC or SMS. Midlets can be digital signed by a third party, the manufacturer or the operator, but it is not necessary. A signed midlet will give advantages in security and user friendliness for the user. Communication with the internal secure element needs a signed midlet to function.

The Nokia 6121 NFC can communicate through several interfaces and is a fully integrated NFC phone. Being a fully integrated NFC phone makes it an easy platform to make prototypes and proof of concepts. Even though the environment is Java ME and should be considered similar on every phone, supported libraries differs from phone model to phone model and has only certain areas where it is equal. The native NFC functionality of the phone makes it possible to read information services and content downloading. The native functionality shows some of the spectre where NFC could be used, but does not limit the functionality.

The SDK that is released have a wide range of features. There is an emulator of the phone which can emulate the phone communicating with NFC tags. The secure element is emulated but is able to emulate the Java Card on the Secure Element. The emulation needs to be programmed in a certain emulation code of Java that the SDK interpret and act as the SE.

4.8 Java environment

The JSR 257 is a key component in developing for the Nokia 6131 NFC. Since most programs for mobile phones are developed in Java ME it is not that difficult to implement the JSR 257 features into the program. Checking if a telephone has support internally for the NFC interface is done by asking for the value in *microedition.contactless.version,* which returns null if it is not supporting NFC.

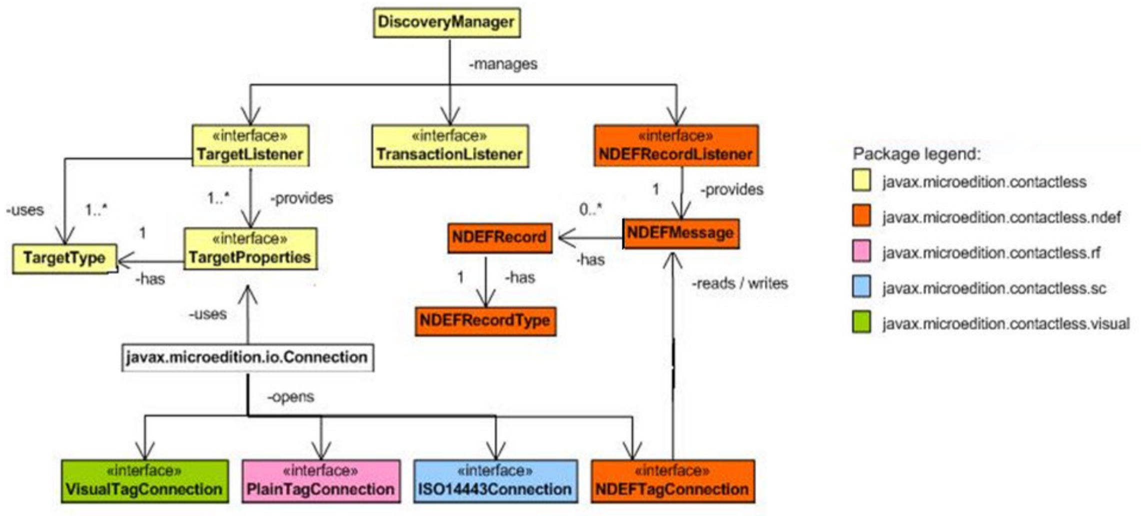


Figure 9: The architecture of JSR 257[13]

The DiscoveryManager is the entity that check if a certain contact should be responded to. If it is a NFC tag it will send the task to the NDEFRecordListener. This will then read the target and get the information stored on the NFC tag. When the data in the NDEFMessage is of the right NDEFRecordType the application will start. This has to be registered in the PushRegistry either by command or in the JAD file. Another part of the JSR 257 which could be relevant, when discussing NFC, is the ISO14443Connection which is the interface to the SE. The peer-2-peer functionality is not implemented in the JSR 257 yet, but it is mentioned as future work in [13]. Nokia have an implementation of peer-2-peer in their phone but it is proprietary.

5. Cooperation with the industry

One important part of this thesis was cooperation with the industry. Here Tellu and Encap were the partners. In this cooperation there was a tutorial showing the possibilities with NFC. Then there was then made a demo midlet which showed the implementation on starting a midlet with NFC. This midlet is described in Appendix B. In the end there was a report describing the possibilities with NFC for Encap. This report is in appendix A.

6. NFC security

Security in tags and phones/readers is an important aspect of NFC technology. In order to earn the users trust to the technology, security should have the highest priority. In this chapter we will first have a look at how mobile phones and tags could be used together securely. Then we will see how security is implemented in an RFID tag in the Electronic passports. NFC technology has many similarities with RFID chips in passport. Passports should have high end security in their RFID chip and is therefore an interesting object for looking at security in NFC. Although it is not officially a NFC technology it is using NFC compatible hardware and have therefore features that are important to understand.

6.1 Tag security

The NFC tags do not in general need to have the same security as for example passports. For example information on a product in a store is not always in danger for being tampered with for commercial gain. Still there are possibilities where such products might be tampered with just for fun or by a competing company. Ticketing systems, credit card systems or other systems using NFC handling valuable information will have a higher risk for being tampered with or cracked. Tags that contain personal information like health records and information that could be a risk for privacy will need to have a good solution so the public will trust it. To see possible threats and look at way to prevent those risks will not be feasible in every scenario, but looking at the threats could give a system designer or a security interested persons an idea of what to might expect. There are many threats for systems like NFC, but in this thesis the focus will be on a few interesting threats and discuss solutions that might help in preventing those threats.

6.1.1 Secure use of tags and readers

There are certain tags which have built-in security features and some others that have very few. Even if there are tags without security features it is possible to use these tags as secure tags. They will need security in the background system, but it is possible to use the little security that is there to make secure tags.

In a NFC system both the tag and reader might be the part the user is interacting with. The interaction is the same but the security requirements could be different. A ticket, which might be a tag, could be copied to decive the system and should therefore not be possible to copy, but a commercial tag, for example a price tag or information tag should be able to be copied, but not to be replaced.

6.1.1.1 Analysing the system

A system using NFC might be divided into three parts.

- the tag
- the NFC reader, which in many cases is the phone
- background system

A user-centric system such as NFC would in many cases have the phone as the interface towards the user because the user is used to operate the phone. We could put the user in as the fourth part, but since NFC is a fairly user centric system and there could be reasoned that the user is a part of mobile phone in this system. Users are already familiar with a phone and with the interface on the phone it is easy to interact with the system.

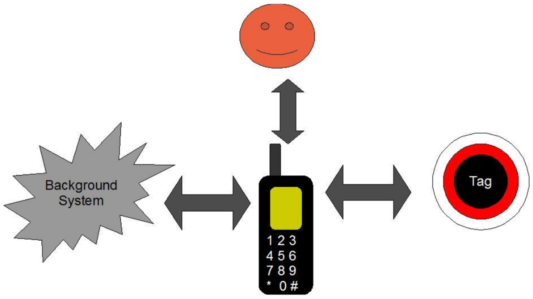


Figure 10: Interaction between system parts.

A system could also easily be based on the user interaction with the tag. So looking at the user centric system it will not be that different when it comes to security. A user could always be counted in, but a good system will take into account that the user could do use the system wrong. Therefore it will be important with security in both the reader and the tag in a way so that the experience for the user is not degraded.

6.1.1.2 Dangerous tag content

One of the obvious threats in NFC is the threats when it comes to URI and links. It is possible for a system to start up when a connection between the tag and the phone is established. For example the tag is put on a commercial leaflet of a bank. When the user touches the leaflet the phone would ask to download a program. This program could be a specially designed for connecting to the bank through the mobile phone. The tag carries only the information about the location to a program published on server. Nokia NFC 6131 has a built-in feature to read web-links and react on them. The problem with this kind of installing application is that the phone will not be able to check if the address is a fake address or not. Therefore the user does not know if he is installing a legitimate program from the bank or installing a malicious program. Users tend to believe that the commercial for a company is from the company that the commercial is for. This has been a problem in e-mails. Fake e-mails have been sent to users to get personal information[14]. A solution to this should be that for example only programs signed by a trusted third party are allowed to be installed from a link on a tag. This is not a published solution at the moment but if the threat becomes large it could be solved. It should also be noticed that a company might not using NFC technology, but might be affected by this kind of frauds because fake commercial like the experience with spam and phising.

Multiple kinds of fraudulent use of tags are possible. Another example that is a threat to the economy for a user is a stored SMS on a taxi station where you could order a taxi to that location. The SMS could contain information like the number to the taxi service and information like the stations address. This information is then sent by the user to the number which is thought to be the taxi service. In a fraud like this, the tag could then be replaced by another tag with other information and another number. If the number is switched with the malicious number for a beneficial company the price for that SMS could be much more than the regular price. It will be very similar with the scam where someone from foreign countries called Norwegians and people called

[14] http://en.wikipedia.org/wiki/Image:PhishingTrustedBank.png

back to an expensive number[15]. NFC Forum has implemented SMS and web links handling in a very easy way to make frauds. It could be argued that a lot of these features should be better implemented, but on the other hand it should be possible to make applications easy with NFC. One of the main objectives with NFC is the practicality. This means that it should not be as many hinders. Even though security would be affected and make problematic aspects.

6.1.1.3 Increase security

If an application is installed on the phone that will respond to a certain record type it is possible to increase the security. Because then the application could handle the security. Some of the tag types have the possibility to store the information on this tag encrypted [14]. But it is not necessary to copy the information so it is encrypted inside the tag. It is possible to store the information on a tag encrypted outside the tag as well. The cryptographic key should then be associated with the unique ID (UID) of the tag. Then it would be difficult to copy the information to another tag that has another UID. The type 1 Topaz, type 2 Mifare UltraLight and type 3 DESFire all have a 7 byte UID which could be used[15][16][17].

NXP has published a paper on securing Mifare UL tags[16]. They suggest that data stored on a tag should be stored and enciphered with a key which derived from a master key which is enciphered with the UID. This can be done in several ways. The way described from NXP is to expand the 7 byte UID into 8 bytes by a given method. The key could be used to encrypt using 3DES encryption standard from The National Institute of Standards and Technology (NIST) to encrypt the information that should be stored on the tag. The given method and the 3DES encryption can be switched to another algorithm as the system designer wish. Another way of using such a method is to encrypt the UID into the data that will be encrypted. This will make it very difficult to copy content from one source into another. A similar method is adding a signature in the end that also is calculated with the UID. The fourth method of doing this is to

[15] http://www.dinside.no/php/art.php?id=783778

encrypt information with a key that have no obvious relation with the UID. The mobile phone sends both, the content and the UID, to the background system that interprets the information. This can be looked upon as storing only content necessary to retrieve the right information on the tag like a web link, only with a security that the UID will have to have a connection to the content stored on the tag. This could for the user look like information is stored on the tag, but is then retrieved Over The Air (OTA). This system only stores an index of information that is interpreted in the background system and is dependent on being online.

The four ways to use UID to not get copied is summarised as:

1. Use the UID to make a unique card key
2. Put the UID into the data that will be enciphered
3. Put a signature at the end of the data that is calculated with the UID
4. Put content on the tag which is connected in the background system with the UID

These ways in using tags have advantages and disadvantages. System number one will be very good for encryption data stored on the tag, but will if the data is random numbers it will be difficult to detect if the decryption is correct. Because the random numbers do not has an integrity check with the UID. In general in cryptography secrets are kept confidential by a key that is secret. In system number one it would be necessary to have the master key to make the card key. This allows for a secure system where the encryption key varies from card to card.

In system number two it is possible to make a secure system. The UID in the system would make it difficult to copy the content from one tag to another when the UID is linked to the tag. Even though there are pitfalls here. Type 1 and 2 tags have a scarce room for data. With Mifare UltraLight, which has only 48 bytes and then uses 7 of those to make sure that the content is linked to the right tag is not a very effective use of the content space.

The third way of making a system has similarities with the second system. Even thought the space would be used not very effective in this system. Still there is an advantage as the main content is not enciphered and may therefore be used. For example for use in links or other kind of information where confidentiality in content is not that important, but a security feature for integrity is more important.

Privacy usually becomes an issue when it comes to using a background system. A tag that connects a user via the mobile phone to a centralized background system makes it possible to monitor and log the user. Managing the tag representation on a server makes it impossible to understand what the tag represents without asking the server or getting it from the server. It would be secure from offline decryption because it is not enciphered. Still there are some difficulties. Privacy is only one. Another problem is what happens when the reader is not online. The advantage of such a system is the possibilities to revoke tags and to reprogram the tags without ever touching them.

6.1.1.3.1 Privacy

When for example a user is buying a book over the internet it is necessary to log the purchase, until you know that the book is delivered, that the book have been bought. Both the user and the seller want to be sure that the transaction would go as planned. The shop want to know that they get the money from the buyer and the buyer wants to get the book. When buying a book at for example amazon.com the link between the buyer and the seller is done by a user account that is logged into. With NFC technology it would be possible to transfer the idea of the user picking out what he wants to shop in a real shop like in a web page and pay the same way. Use the phone as an ID and use the tag to represent the goods that is sold. This could be very similar with barcode that exist on goods to today, only the user is one that scans the product. The problem here is that it is not certain that the buyer want the shop to know everything he buys. Therefore could an online system step on some toes when it comes to privacy and therefore should be used with care.

6.1.1.3.2 Increasing network security

Another way of using this kind of system would be to confirm something on the internet, for example paying bills. Banks on the internet are having problems with phishing attacks. One of those problems comes from MITM attack. With NFC technology it would be possible to get around this problem.

Internet banks may by mail send a sticker which has a NFC chip to the users of the internet bank. This tag can then be put on a computer which the user usually uses for internet.

1. User would log in with username and password.
2. A number would be presented on the screen of the computer.
3. The user touches the tag with his mobile phone.
4. The program for internet bank would start in the mobile phone.
5. The program would then ask the user to type in the number represented on the screen.

The program of the mobile phone is already registered with this username at the bank. Both the number and the information confirming the mobile phone would then be sent to the internet bank which confirms the login at the bank. Now the user may is correctly authenticated and logged in and can start using the services in the internet bank. For example he might pay a set of bills. When he wants to confirm paying bills his mobile phone would ask if the information for the bills is right. This is also published at the screen of his computer summarising the bills. If the two sets of information is correct and the bills are correct then the user just touches the tag to confirm the payment.

A further security measure might be added if it is allowed to write to the tag. When a user touches a tag it might write what the tag has been used for last time. Writing the information to the tag would give the user the information if it has been misused. The information encrypted would help both in confidentiality and integrity if it is encrypted from the centralized background system. It would also be very difficult to have two equal tags even when someone is replaying information that have been gathered from eavesdropping on the communication between the mobile phone and the tag.

This system could be used in many different scenarios where secure interaction and authentication would be necessary. Stealing a tag would still give away the user when a tag is used, because it is possible to register which mobile phone has been used. Revoking a tag would be possible as well if it is reported stolen. It would also be difficult to start the application anonymously which is necessary to do if the phone is stolen because the tag would tell who is using it. As long as both the tag and the phone are linked to each other it would be necessary to steal both the tag and the phone.

Usually computer security does not use a physical ID, but is more often of a logical ID. Some have started using fingerprints, but they are not revocable. This system would make a physical ID to get into a digital place. The privacy could be a problem. Because of that, a careful consideration should be done to ensure that the design allows for both the privacy necessary and the security needed. To increase internal security features in for example DESFire should be used to increase security as we see when it is used in ticketing systems.

6.1.1.3.3 Ticketing systems

The Norwegian Public Roads Administration has published a set of guidelines concerning ticket systems for public transportation [18]. These guidelines advices how new ticket systems should be designed. One of the advices is implementing using the DESFire tags in season tickets and tickets that are not for one time use. The advantages of using such system is that the tag is capable of internally encrypt information with strong cryptography. This has several advantages for use in ticket systems.

- It is possible to store information like the user can only travel 20 times for the amount paid
- It is the same all over the nation so the same ticket can hold tickets from different service providers
- It is not a system that has been cracked

For example a user could buy 10 trips with service provider A and 5 with service provider B. For each trip with the right service provider the card counts down, until the card says the user can not travel any more. There are several reasons for storing such information on a card instead of background system. Two valid reasons are privacy concerns and that the system should be able to work offline.

6.1.2 MiFare Classic

Mifare Classic is a system developed from NXP Semiconductor. They have also developed Mifare Ultralight and Mifare DESfire which is NFC Forum type tags. It is used in several ticketing systems as the RFID ticket, amongst others in the Dutch public transport system and the Greater London public transport system[19]. It is also used in access control systems as the key to enter a room or building. The technology was introduced in 1994 and has been a commercial success all over the world[20]. The design of the system has been open, but not the security feature of the cryptographic algorithm which has only been said it is 48 bits and is secure.

NXP designed the Mifare Classic system using the CRYPTO1 stream cipher algorithm which is proprietary and made by NXP Semiconductors. The design of the algorithm was kept a secret and was not tested by outsiders until researchers, Karsten Nohl and Henryk Plötz, presented that they had started to reverse engineer the Mifare Classic chip by peeling of layers by layers on the microchip and taking photos of the architecture. Analysing the photos they were able to reengineer the design of the Mifare Classic chip. By doing this they were able to present weaknesses on it in 24th Chaos Communication Congress in December 2007. During 2008 more weaknesses were found and eventually Mifare was considered not safe even by national authority[21][22].

The weaknesses found were in the implementation, the authentication key was linked to the UID and that the cipher now was known. The implementation had a weakness in the pseudo-random number generator (PRNG). The PRNG in Mifare Classic works as Linear Feedback Shift Register (LFSR) shifting the registers every 9.44µs which is the same as the time communicating one bit. In theory a nonce in the PRNG would reappear in 0.618s. Knowing the algorithm makes it also possible to attack the Mifare Classic system offline, which was not possible before. But without knowing the algorithm, but knowing the weakness in the PRNG, Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia showed in [19] that it was possible to clone a Mifare Card.

When a system becomes cracked it has commercial and trust from consumer consequences. Ticketing systems become vulnerable and may lose income from pirate tickets. But access control systems could be compromised by the possibility to copy the key card. Replacing a system that has been in use since mid 90's could be costly. Learning form the mistakes from the failures in Mifare Classic should be essential for NFC to become a success. If the design had been open from the beginning it might have been discovered earlier. Electronic passport could be a much greater risk for every citizen in a country and the security for public transportation than the Mifare Classic if vulnerability in those were found.

6.1.3 Norwegian electronic passports

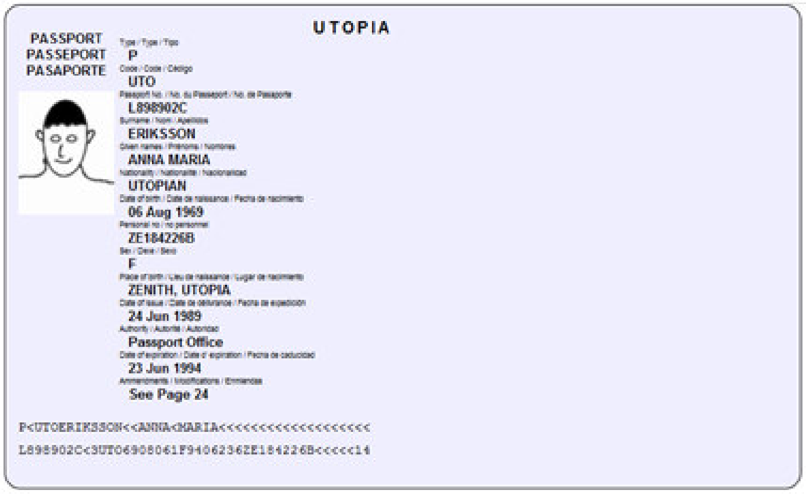
3rd of October 2005, Norwegian government issued new passports which contained an RFID chip which contains the information already visible in the passports[23]. The government claims the security is not in danger because it only contains information that is already in the passport. The information is also protected according with the International Civil Aviation Organisation (ICAO) guidelines. Norwegian passports use Basic Access Control (BAC) like the EU has required. BAC is a standard way to protect the information from being read unauthorised. Electronic passports are a type of Machine Readable Travel Documents (MRTD). MRTD passport contains a Machine

Readable Zone (MRZ) of the passport. The MRZ contains the key information for securely transmitting information between the passport reader and the passport in an electronic passport. So when a person shows his passport at a border crossing, the border guard will make the machine read the MRZ and then read the electronic part of the passport.

6.1.3.1MRZ

The information that the MRZ contains is standardised by ICAO as well. There are two lines as shown:

```
P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<
L898902C<3UTO6908061F9406236ZE184226B<<<<<14
```



UTOPIA

PASSPORT
PASSEPORT
PASAPORTE

Type / Type / Tipo
P
Code / Code / Código
UTO
Passport No. / No. du Passeport / No. de Pasaporte
L898902C
Surname / Nom / Apellidos
ERIKSSON
Given names / Prénoms / Nombres
ANNA MARIA
Nationality / Nationalité / Nacionalidad
UTOPIAN
Date of birth / Date de naissance / Fecha de nacimiento
06 Aug 1969
Personal no. / no personnel
ZE184226B
Sex / Sexe / Sexo
F
Place of birth / Lieu de naissance / Lugar de nacimiento
ZENITH, UTOPIA
Date of issue / Date de délivrance / Fecha de expedición
24 Jun 1989
Authority / Autorité / Autoridad
Passport Office
Date of expiration / Date d' expiration / Fecha de caducidad
23 Jun 1994
Amendments / Modifications / Enmiendas
See Page 24

```
P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<
L898902C<3UTO6908061F9406236ZE184226B<<<<<14
```

Figure 11: Example passport from[24].

For reading a passport electronically it is only necessary to read certain parts of the second line on the MRZ.

- passport number (red)
- date of birth (blue)
- expiration date (orange)

These three parts have their own check digit, green. The check digit is easily computed from the digits right before. The computation is done like this:
The alphabet is represented as two digit numbers.

L * 7 = 21 * 7	= 147
8 * 3 =	= 24
9 * 1 =	= 9
8 * 7 =	= 56
9 * 3 =	= 27
0 * 1 =	= 0
2 * 7 =	= 14
C * 3 = 12 * 3	= 36
< * 1 = 0 * 1	= 0
Sum	313

The last digit of the sum is the check digit. In this example three is the correct check digit. For the other two numbers, blue and yellow, the calculation is done the same way, but with just two sequences of 7-3-1 as multiplier.

6.1.3.2 MRZ security

To read the passport electronically it is not necessary to read the entire MRZ. The MRZ could be guessed and therefore not read at all. Knowing the expiration date of the passport and the date of birth for the passport holder as well as the passport number is enough to calculate the check digits and get the right information to pass the BAC. Looking at the numbers, which is relevant in the MRZ for BAC, it is enough to see that it is a vast number of possible numbers to test. Therefore it is considered a good enough solution. The date of birth of a person in Norway is not very difficult. Social networks and homepages as Facebook, LinkedIn and MySpace are all very wide spread and people tend to publish that information. This makes it very easy to find a person's date of birth. Knowing that the date of birth is published has implications on how secret the date of birth could be and could be considered easy to find. The next number that should be difficult to find is the expiration date. Contradictory to what is mentioned in [25] is it not 365 days in the year of expiration date. A passport is valid 10 years after it is manufactured. In Norway it is only possible to get passports with expiration date of Monday to Friday in that particular year it is made. So only valid dates would be Monday to Friday and add 10 years on these dates. It could be used as a good approximation for calculations since there actually less days when counting in holydays. A table of days with valid expiration date is quite easy to make. It is also stated by the police that there are more passports with expiration date in the summer[26]. Calculating the amount of valid expiration dates in a 10 years period is:

$$\frac{365 * 5}{7} = 260{,}7\ each\ year\ which\ makes\ 2607\ possibilities$$

Now knowing the passport number and the birthday of passport holder it is necessary to try 2607 different combinations.

The last numbers to find is the passport numbers. In Norway the passport number is 8 a digit number. The first digit is 2 for regular police passports. The second number is 5 or 6 if it is electronically readable. Then there are 6 last digits. This makes 2 000 000 combinations. Each passport would then require $2607 * 2\,000\,000 = 5\,214\,000\,000$ tries.

This might seem as very high number of possibilities. But still there is ways of bringing this number even lower. In Norway passports are made one place [27]. The writer of this thesis also found that in his passport the name of the producer is represented in one block of the Security Object Document (SOD). There the name is “Setec Norge AS”. Looking at this company it seems likely that they are produced in one place as they have address two places in Oslo. Without knowing how passport numbers are generated it is likely to think that because of the centralisation it is no link to where the consumer lives. Therefore it is unlikely that knowing the range of passport numbers in a given police district will give better guessing rate. On the other hand it is easier to analyse passport numbers when there is one less factor to use in the calculation. Looking for links between passport numbers and expiration dates could result in drastic reduction of the key space.

Passport numbers and expiration dates are showing signs of being sequential. Knowing the way the numbers are generated is relevant since knowing the profile on how these numbers are generated is essential for cracking the BAC. The more accurate the link between expiration date and passport number is the fewer tries are needed to successfully pass the BAC. Collecting passport numbers would be effective for finding an algorithm. Making an algorithm where in the winter every expiration date could try 500 passport numbers and during summer try 2000 passport numbers could be a place to start. This are just some figures that just shows that by doing it this way it is possible to narrow down the search. Also factors like the price adjustments that come with the Norwegian state budget could have impact on people buying passports. So when passports become cheaper, people will wait until the next year to buy it. From 2007 to 2008 the price got reduced from 990 to 450 NOK. People know this from October to December and probably will not buy a new passport in that time when they do not have to. Since I do not have available a large set of passports and have not collected passport numbers the passport generation algorithm used in the production is an open question. A hotel owner in Mallorca or Greece would quite well have a large set of passport numbers and expiration dates and could have the key for Norwegian passports.

6.1.3.3Cracking the BAC

To automate the reading of passports I used my own passport, a computer with SDI010 contactless reader and the free software wzMRTD[16]. Small adjustments were needed in the software. The program is in appendix C. This was done to efficient test a whole set of MRZ's. The APDU command sequence is explained below.

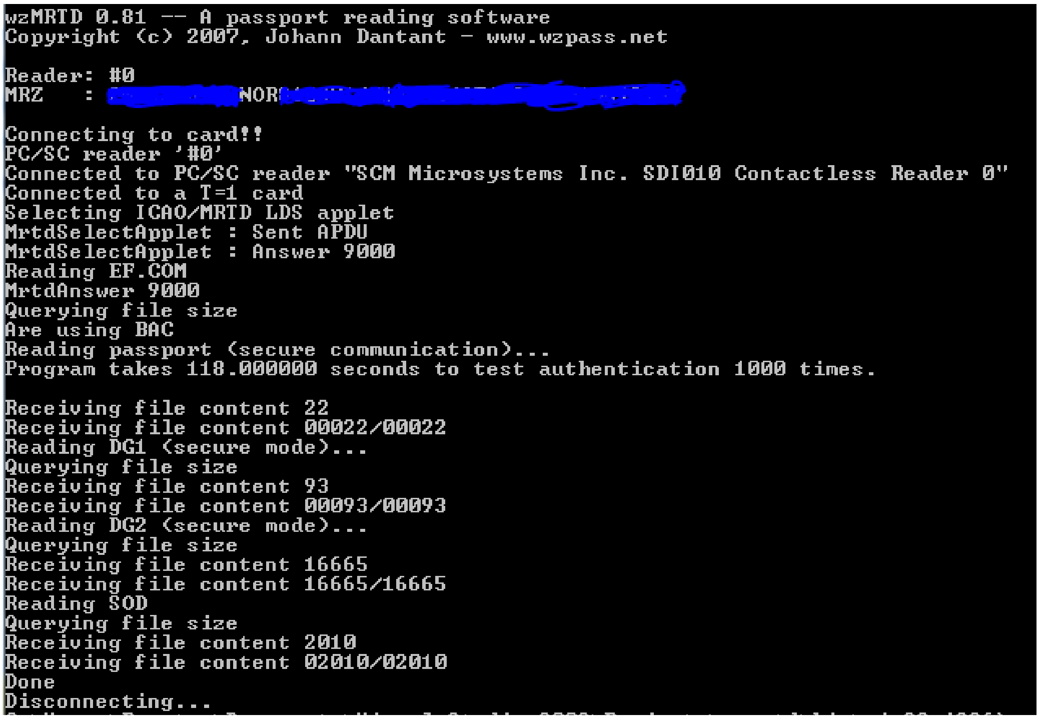
[16] http://www.waazaa.org/wzmrtd/index.php

1. wzMRTD selects the ICAO Logical Data Structure on the passport with the APDU command: "00 A4 04 0C 07 A0 00 00 02 47 10 01"
2. The passport would then respond: "90 00"
3. wzMRTD asks for the file EF.COM: "00 A4 02 0C 02 01 1E"
4. The passport would then respond: "90 00"
5. wzMRTD asks to read binary: "00 0B 00 00 00"
6. The passport with BAC would then respond: "69 82"
7. wzMRTD would with the respond in 6 that know that BAC is needed. The modified version of wzMRTD would now try to make the key out of a fake MRZ given to it.
8. Will repeat 7 untill solved. Counting 1 up on passport numbers.
9. wzMRTD will then read the passport.

As shown above it is quite easy to brute force since the only step needed to reproduce is step 7. If the entire procedure would have to be done it would make the time much longer or by only allowing tests three times before the passport would ask the read application to start at step 1 again. This would increase the brute force time considerably.

6.1.3.4 Analysis of result

Cracking the BAC on the passport gave some different results. Testing several times with the same passport ended up with the passport becoming harder and harder to read. This could be the reader or the passport or other factors, but if the passport got tired from the continuous test to read the information, it is perhaps weak to denial of service attacks. Although such an attack will take some time, but this is a question which could use some further research.



```
wzMRTD 0.81 -- A passport reading software
Copyright (c) 2007, Johann Dantant - www.wzpass.net

Reader: #0
MRZ   : [redacted]NOR[redacted]

Connecting to card!!
PC/SC reader '#0'
Connected to PC/SC reader "SCM Microsystems Inc. SDI010 Contactless Reader 0"
Connected to a T=1 card
Selecting ICAO/MRTD LDS applet
MrtdSelectApplet : Sent APDU
MrtdSelectApplet : Answer 9000
Reading EF.COM
MrtdAnswer 9000
Querying file size
Are using BAC
Reading passport (secure communication)...
Program takes 118.000000 seconds to test authentication 1000 times.

Receiving file content 22
Receiving file content 00022/00022
Reading DG1 (secure mode)...
Querying file size
Receiving file content 93
Receiving file content 00093/00093
Reading DG2 (secure mode)...
Querying file size
Receiving file content 16665
Receiving file content 16665/16665
Reading SOD
Querying file size
Receiving file content 2010
Receiving file content 02010/02010
Done
Disconnecting...
```

Figure 12: Screenshot of the wzmrtd software that was slightly modified to bruteforce attack on Norwegian passports

Testing 1000 times as seen in picture XX shows that it took 118 seconds. It only counts whole seconds. That is under 2 minutes. Other times testing for 10 000 numbers the time is 1158 seconds or up to 1210 seconds. Looking at this it takes approximately 20 minutes to test 10 000 numbers. So to test all the expiration dates which we found was fewer than 2607 would take close to 5 minutes. Knowing this, it is possible to calculate how many passport numbers would be tested for each date over a certain timeframe to cover the most passport numbers and dates over the time available. By using the knowledge that in the summer there are more passports and fewer in the winter it could be possible to make statistical test which would have a possibility of cracking the number. The more passport numbers that get known the more statistics would help in making the cracking faster and easier.

Another scenario is the mailman which delivers the passports. By printing the highly unnecessary information about the passport number on the envelope it makes the possibility of copying the passport too easy. By knowing that the passport was printed the working day before or the day before that, the number of expiration date is not many. We could amount the numbers of expiration date to four. Then we could argue that we do not know how old this person is, although a mail man could probably easy find this if he brings the mail each day. Still we can calculate the number of tries with a wrong date would be 365 days within 100 years.

$$365 * 100 = 36\,500$$

Times the four days before:

$$36\,500 * 4 = 146\,000$$

$$\frac{146\,000\ tries}{10\,000\ tries} * 20min = 292min$$

In 292 minutes, under 5 hours and within a work day, a mailman is actually certain to get the information about the person in the passport. It is always possible to argue that a mailman could probably get the hold this information anyways, but it is not necessary to give such information away anyways. In the digital world the knowledge the mailman will be able to obtain is probably bound to become less as more and more information is sent electronically, except for passports which must be physical.

6.1.3.5 Discussion

BAC is an easy way to protect information, but should not be the only way of protecting the digital information stored on a passport. It would probably be enough if the government had implemented the passport with random passport numbers. The entropy of the cryptographic key would then be greater. Implement random passport number would be of no greater difficulty in a digital world, but using sequential numbering is a fault that makes the entire BAC only a better than nothing implementation. It is also highly questioned why the passport number is written on the envelope that is sent to the passport holder. It has nothing to do there and why it is put there should have a very well defined answer.

Another way of protecting the passport from skimming is with a shielding[28]. The shielding will work when the passport is completely closed, but it might be that the front is slightly open in a sack or something. There it could still be vulnerable if not a small bag or pouch with shielding in a size that only is able to contain the passport. This way a faradays cage is effective implemented. Still there should be a shielding in the passport so that it is secure when walking around in an airport or places where a frequent check of passport is normal.

The passport could be much more secured, but this is always a cost versus security trade-off. Passport is an important document in Norway and the reason for security evaluation should be publically available. When the Norwegian government wants to be serious about hindering ID-theft they should not send out the passport with a part of the key as a unnecessary text on the envelope. If the passports where to have random numbers it would increase the security, but to implement a shield on the outsides of the passport would probably not cost that much since the United States have implemented it.

6.2 NFC input security

NFC gives a lot of possibilities and exploring the security features in the system there are interesting aspects. NFC could act as the medium to send malicious information into a system. This could either be by accident or by malicious exploitation of a system. By accident it could happen that a person uses the wrong tag and therefore sends information to a badly designed reader system that would crash the reader, or by sending false information like a file that contains a malicious code. This would be a really large threat for background systems and readers and should be looked upon when designing systems.

6.3 Increase internet security with NFC

There are several ways of making web experience more secure with NFC. First there is the possibility which is explained in chapter “Increasing network security”. That chapter explains how to connect the content of a tag with the UID. The connection between the UID and the content on the tag is only known by a server and is not related or calculated of each other. This makes it impossible to brute force the meaning of the content.

By using such a strategy it is possible to make a more secure way of logging into web sites. Internet banks have usually a high degree of security so to look at how the banking industry use web security is a way to compare a solution with NFC. BankID is the standard in the banking industry in Norway so it is natural to compare the NFC strategy with BankID.

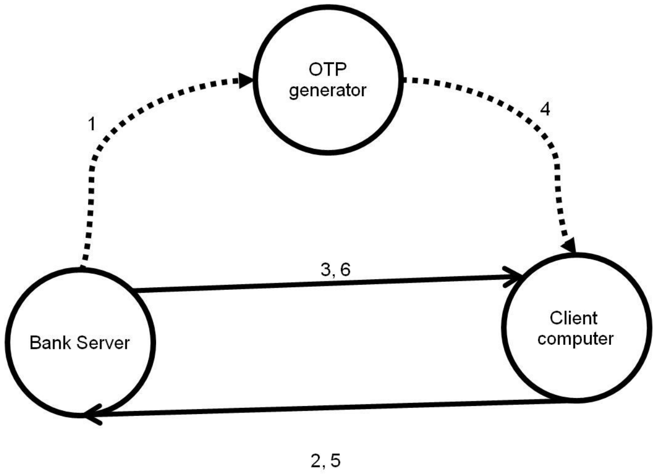
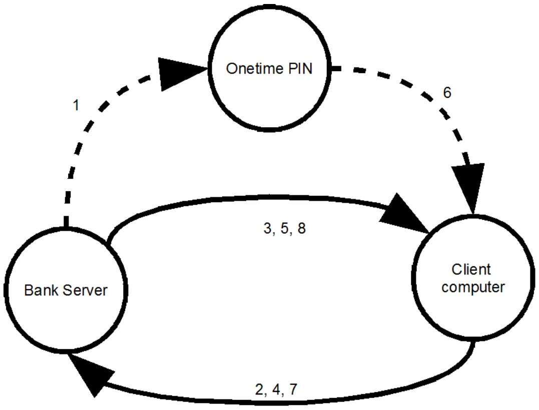


Figure 13: A rough figure on how BankID function

1. A One Time Password (OTP) generator which calculates password is sent by mail to the user.
2. Client request a session to log into his internet bank
3. The internet bank sends back a login page which is signed by a bank or third party
4. User calculates his OTP
5. User sends information as the OTP together with his username and PIN
6. Bank accept the information and sends requested information

- Number 4, 5 and 6 might be used to confirm actions as paying bills
- The scattered lines is where manual interaction is needed

The BankID solution is a way of making a secure login which has had success. Still there are certain aspects where the security is allegedly not very good. The security for the client that the bank has signed its session could easily be manipulated and the user will not know. This makes it possible to do a MITM attack. So there are other ways of having a secure login for internet banks, for example the way which is implemented by Skandiabanken.



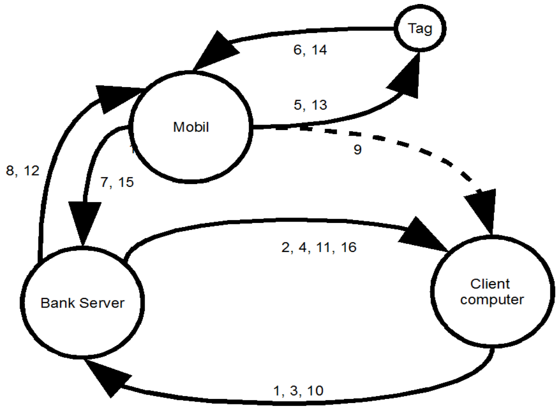
Picture 14: Description on how Skandiabanken function

1. A onetime PIN card is sent by mail to the user, might be requested by SMS.
2. The Client asks for a certificate for his client.
3. Bank sends a certificate to the client and sends an e-mail of the action to the user
4. Client request a session to log into his internet bank
5. The internet bank sends back a login page which is signed by a bank or third party
6. User reads of his onetime password.
7. User sends information as the onetime password together with his username and PIN
8. Bank accept the information and sends requested information

- Number 6, 7 and 8 might be used to confirm actions as paying bills
- The scattered lines is where manual interaction is needed

The Skandiabanken solution has some advantages over the BankID solution regarding security against MITM. The client has a certificate which can be used to sign the action from the user. This hinders the MITM attacks as long as the certificate is not stolen from the computer or is requested without the user's knowledge. It might be that someone has written off the onetime password card as well as the PIN and username so they are able to malicious use the bank access. To make this solution more secure it is possible to make a solution where the secure communication channel, which today usually are the mail or SMS, more online.

The first solution with NFC could be to use the mobile phone as the place to confirm actions. There are already programs for mobile phones making it more online, but not using the benefits of NFC when confirming an action or authenticating in a more secure manner.



Picture 15: Secure solution A

1. Client ask for a session
2. Internet bank starts a session and send login data
3. Client login at the internet bank with username and password
4. Internet bank sends over information that the user is requested to send in session information from mobile phone to complete login
5. Mobile phone is requesting information from tag

6. Tag sends information to mobile phone
7. The mobile phone sends over information as tag information and mobile phone information, which is linked to the user
8. Bank accept information and sends back the requested session information at point 4
9. Session ID is manually written into the browser
10. Browser sends the information that was requested
11. Login is completed
12. When the bank wants to confirm an action inside the netbank, it send the information to the mobile phone
13. The user reads one the phone the actions that is requested to be confirmed and confirms with asking tag for the same information as at point 5
14. Same as point 6
15. Mobile phone confirms action
16. User get to know that action is confirmed

- The scattered lines is where manual interaction is needed

By using the mobile phone as the confirmer of actions it would be difficult to be a MITM in two separated communication channels at the same time. The tag need to be registered to a user so the use can be logged by phone and tag used. This forces a more geographical authentication of the user. The problem with this is that the tag might get lost or stolen as well as users want to use internet banks on travels and other places. Secure solution A has these flaws that could be fixed, but only by removing the tag. NFC technology has introduced other means for communication. By using NFCIP-1 protocol for peer-2-peer communication it could be possible to implement a solution using two communication channels.

Secure solution B uses the peer-2-peer possibility in NFC technology to transfer a certificate that arrives from the mobile phone to the PC. This is another way of using the Skandiabanken system but changes the way the certificates are stored and distributed. This also requires the OTP for login and confirmation. Although the security is increasing with such a system, the amount of action the user will have to do is increasing and it is therefore not something the user will appreciate.

To make things easier and still have the security the user could skip the part of writing in the onetime password. Secure solution C uses the mobile phone's NFC interface to confirm login and changes the interface in which the onetime password is transferred. With NFC the certificate and the onetime password is transferred from the server via the mobile phone to the PC. To now confirm an action with OTP just touch the NFC interface on the PC with the mobile phone.

Using OTPs are solving the fundamental problem with MITM. Certificates can be stolen or sent to computers in internet cafés and that makes a security problem. But a user which receives the certificate to the mobile phone does not need to transfer the certificates to the mobile phone. This is called secure solution D. Signing with a certificate might be done on the mobile phone itself. Sending the information from the PC to the phone then signing the information with a certificate which is received from the server will make it hard to steal the certificate. For logging in the OTP does not need to exist. The user will sign a session ID sent form the bank. This ID will then have to be signed by the right user to get logged in. To get a confirmed action there will have to be a signature as well. The mobile phone will then act as a secure channel between the PC and the server, though the certificate will never be on the PC so it would not be possible to recover it or use the certificate without the knowledge of the owner of the mobile phone.

	BankID	Skandiabanken	A	B	C	D
Security vs bruteforce	🟩	🟩	🟩	🟩	🟩	🟩
Security vs MITM	🟥	🟨	🟩	🟩	🟩	🟩
Security vs trojan infected computer	🟥	🟥	🟥	🟥	🟥	🟩
Security vs stealing	🟥	🟥	🟥	🟥	🟥	🟩
Usability	🟩	🟩	🟩	🟨	🟨	🟩

Table 3: Comparing the different solutions against threats

The login procedures that exist today are quite secure. Still there is proof of concept hacks that have been able to penetrate the BankID architecture[29]. The researchers have two problems with the BankID system. First it is possible to attack the system with a combination of phishing and MITM attacks. The second issue is that BBS, which develop and run BankID, is owned by the Norwegian banks and that there is no third party control over the PKI. The Norwegian Financial Services Association and The Norwegian Savings Banks Association claims in a joint letter to the Norwegian government that the security breaches that was showed have not yet been proven to be tried against BankID [30]. They claim as well in the same letter that even though the PKI architecture is run by BankID it will be secure and trustworthy for the users. This might be true as well as the claim that it has security features to prevent MITM, but since BBS which produces BankID does not publish and explain the features it is not proven.

The problems of both the phishing combined with MITM attack and the trustworthy use of BankID could be removed with a system which the phone contains the certificate to sign every action or transaction. Secure system D solves these problems with a simple solution. If the certificates are not connected to BankID it will be possible to give the certificate service from a third party.

NFC could be used to increase user friendliness by sending the OTP from the mobile phone to the PC. In theory it could be transferred with Bluetooth or WLAN as well since this is technologies that are more widespread. The reason that NFC will be better for these kinds of connections is that it requires a physical move with the user. Bluetooth and WLAN and most other wireless technologies might transfer over greater distance than NFC. By controlling the physical connection the user would still have the control over the action. It will not be enough to just push ok on a question, but the user will have to do a physical movement connecting PC with mobile phone. This makes it more likely that the user will understand if he is getting scammed.

Looking in a wider space NFC can then transfer a certificate instead of the OTP as in secure solution C. This enables NFC technology to merge with current technology to sign documents or by allowing certain objects to represent you like the SIM is representing people for the phone company. Mobile phones with NFC technology could with secure solution D function like an ID card that would be secure and easy to use. Looking at the possibilities for this is something that needs further research.

6.3.1 Discussion

The financial industry has to have total control over their products. They calculate the risks expected different kind of technologies and implement them only if they receive a commercial benefit. As long as the financial or banking industry only deals with in the financial world and will pay back if a fraud is done there is no need to worry about security. The problem arises if BankID becomes a standard for other kinds of businesses like buying things or voting. These are threats that the banking industry does not know every aspect of. Therefore it is necessary to examine options on how to increase security in systems. The benefit with NFC is that it is a user-centric system that makes new possibilities in a simple and intuitive way. There are of course the pitfalls that have been discussed, but as long as the design of systems is easy it will be able to take bank security into new areas.

7. Conclusion

Looking at many of the different aspects which could influence the security in NFC shows that it is a system which is made easy to use, but it is possible to use it securely. There are several possible modes to use which makes NFC a good building block. Using the right building block would be important to have the best security. This is seen especially when looking at increasing internet security with NFC. Here it is possible to increase security with tags. This is helping somewhat, but with shifting out the tag with the peer-2-peer would make the security much more secure. Another important part of security is to implement the design in a correct way. The Norwegian passports are most likely to have a sequential or close to sequential numbering which makes the security much less than it could be. Using the guidelines from ICAO could give a secure passport. The implementation Norway has chosen show that the idea of electronically readable passports could be better planned.

8. Bibliography

[1] RFID Journal. RFID Journal. [Online]. http://www.rfidjournal.com/article/articleview/1338/1/129/

[2] E. Haselsteiner and K. Breitfuß, "Security in Near Field Communication (NFC)," , 2006.

[3] OTI, "ISO 14443 An introduction to the contactless standard for smart cards and its relevance to customers,".

[4] P. Henzen, "Near Field Communication Technology and the Road Ahead," , 2007.

[5] NFC Forum, "NFC Data Exchange Format (NDEF) Technical Specification," 2006.

[6] J. Noll. (2007, May) Movation. [Online]. http://www.movation.no/index.php?option=com_content&task=view&id=78&Itemid=9

[7] Norwegian Public Roads Administration, "Handbook 206-3 Specification for Interoperable Electronic Ticketing System," 2005.

[8] International Civil Aviation Organisation, "Machine Readable Travel Documents, sixth edition," 2006.

[9] Arbeids- og inkluderingsdepartementet, "Kravspesifikasjon identitetskort for bygge- og anleggsnæringen," 2007.

[10] Arbeids- og inkluderingsdepartementet, "Id-kort Endringsdokument 16.05.2007," 2007.

[11] A. S. Tannenbaum, "Computer Networks 4th ed.," in *Computer Networks 4th ed.*

[12] Nokia, "Nokia 6131 NFC Technical product description," 2007.

[13] JSR 257 Expert Group, "Contactless Communication API," 2006.

[14] Innovision Research & Technology plc, "Near Field Communication in the real world – part II,".

[15] Arygon Technologies AG, "NFC Forum Type 1 Tag (Topaz)," 2007.

[16] NXP B.V., "AN 073120 - mifare Ultralight features and hints," 2006.

[17] M. Meriac and H. Plötz, "Practical RFID Attacks," , 2007.

[18] The Norwegian Public Road Administration, "Electronic billetting," , 2004.

[19] G. de Koning Gans, J.-H. Hoepman, and F. D. Garcia, "A Practical Attack on the MIFARE Classic," , 2008.

[20] MIFARE.net. MIFARE.net. [Online]. http://mifare.net/about/milestones.htm

[21] National Security Authority, "Sårbarhet i elektroniske adgangssystemer," Sikkerhetsvarsel 2008 nr. 2, 2008.

[22] GOVCERT.NL, "Vulnerabilities of Mifare Classic chips in access cards," FACTSHEET FS-2008-03, 2008.

[23] Ministry of justice and the police. (2005, September) Ministry of justice and the police homepage. [Online]. http://www.regjeringen.no/en/dep/jd/Whats-new/News/2005/Nye-elektroniske-pass-og-personvernet.html?id=99556

[24] A. D. Smet. (2004, January) High Programmer. [Online]. http://www.highprogrammer.com/alan/numbers/mrp.html

[25] J. F. Pettersen, "Sårbarhetsanalyse av utvalgte deler av norske biometriske pass," 2006.

[26] The Norwegian Police. Politiet. [Online]. http://www.politi.no/portal/page?_pageid=34,49023&_dad=portal&_schema=PORTAL&articles7_mode=skjemadetails&articles7_articleId=33089&articles8_mode=downloadskjema&articles8_articleId=33089&uicell=uicell02b&navigation1_parentItemId=192

7&navigation1_selected

[27] I. Oftebro. (2006, March) IT-avisen. [Online]. http://www.itavisen.no/sak/295852/Vi_tester_bio-pass/

[28] K. Mahaffey, "RFID Passport Implementation Vulnerabilities: Technical Analysis,".

[29] Y. Espelid, L.-H. Netland, A. N. Klingsheim, and K. J. Hole, "A Proof of Concept Attack against Norwegian Internet Banking Systems," in *12th International Conference on Financial Cryptography and Data Security (FC08)*, Cozumel, Mexico, 2008.

[30] A. Skauge and A. Hyttnes, "Brev fra FNH og Sparebankforeningen om sikkerheten ved BankID publisert," December 11, 2007.

Appendix A

The report to Encap is attached electronically.

Appendix B

The midlet programmed for Nokia 6131 NFC is attached electronically to this thesis. Both the source code and the compiled program are attached.

Appendix C

The program to brute force attack passport is attached electronically. It is in compiled version and the source code that is changed in the program from wzMRTD v0.81.