Thesis no: BCS-2016-05

A survey on contactless payment methods for smartphones

David Andersson

Faculty of Computing
Blekinge Institute of Technology
SE–371 79 Karlskrona, Sweden

This thesis is submitted to the Faculty of Computing at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of BSC. The thesis is equivalent to 10 weeks of full time studies.

Contact Information:
Author(s):
David Andersson
E-mail: daan13@student.bth.se

University advisor:
Adjunct Lecturer Francisco Lopez Luro
Department of Creative Technologies

Faculty of Computing
Blekinge Institute of Technology
SE–371 79 Karlskrona, Sweden

Internet : www.bth.se
Phone : +46 455 38 50 00
Fax : +46 455 38 50 57

Abstract

Context. The use of smartphones has increased drastically in the last years. More and more areas of use are discovered each day. One of the new fields of use is to make contactless payments with the help of a smartphone. A contactless payment system for a smartphone is a solution that will allow the user to make a payment by placing the smartphone in near proximity of the payment terminal in order to make a payment instead of using a regular credit card or cash.
Objectives. The aim of this thesis is to present the current state of the smartphone systems used to conduct contactless payments, how they are implemented, possible flaws, and suggested solutions to remove the flaws.
Methods. A literature study was conducted in order to find reliable information regarding how the systems works. Since the field of contactless payments is still new, there are several knowledge gaps regarding how parts of the systems works. In those cases, the company behind the systems was contacted, or patents and white papers where used.
Results. An analysis of the current state of contactless payment systems were conducted. In most cases, the studied systems were similar in functionality, however there are a few differences, such as how the tokenization process is conducted.
Conclusions. The study showed that the systems has developed significantly in the last years and the usability is high, however there are still some parts that needs more work and development, such as offline support and a solution to the slow growth rate of the user base.

Keywords: Tokenization, Contactless payment, Comparison model

List of Figures

List of Tables

Contents

Chapter 1

Introduction

The development of contactless payment is still in its early stages. Nonetheless it is a field that has attracted a lot of big companies, such as Google, Apple and Samsung.
So far, the road has been tough for contactless payment systems, and the user base has not grown as large has predicted. However, the development is still going rapid, and with the possibility to use a smartphone instead of a regular credit card, interesting new solutions are released in fast pace. The latest significant new solutions is Samsung's "Magnetic Card Emulation"-solution, which enables a smartphone to emulate a magnetic field in the same way as an ordinary credit card. Magnetic Card Emulation is a substitution to the commonly used Near Field Communication.
Another new solution was adopted by Google in their operative system, Android, and it is called "Host Card Emulation". This is a solution to replace the hardware chip in the smartphone that handles sensitive information, with a software solution which enabled a large number of the current phones used today to support contactless payments.
However, there are also negative aspects of contactless payment systems that use a smartphone to conduct the payments. There is now a larger risk that the device will be infected with malicious code with the use of downloadable apps. Since most devices are connected to the internet as well yet another field of attacks emerges. On the other hand, a smartphone has more computational power that can be used to counter these kind of attacks in a more effective way than a credit card.
In conclusion, contactless payment systems for smartphones is a new and rapidly developing field that is still in its infancy. This thesis is presenting the current state of contactless payment solutions for smartphones, as well as a comparison between the current systems, and an analysis of the implemented solutions in order for the reader to get a better understanding of the field. This thesis is important in that aspect, since currently there is not a lot of gathered information regarding those systems. In the future, it is likely that many people have to make a choice on what contactless payment system that they want to use, therefore it is important to get an overview of both the advantages as well as the disadvantages

of these solutions.
Three systems are chosen to analyze in depth in order to get a better understanding of what technical solutions that are applied today. The three systems are: Samsung Pay, Android Pay, and Apple Pay.
Those three specific systems were chosen to analyze since they are developed by large actors of the contactless payment systems for smartphones. They are also currently adopting new technologies in order to enhance the systems.

1.1 Research question

The goal of this thesis is to answer the following research question:

> "What is the status of currently used contactless payment methods for smartphones regarding functionality, security and privacy compared to each other and what possible enhancements could be applied to the methods?"

1.2 Road Map

In chapter 2 - Background, the general functionality of contactless payment systems is presented, along with some deprecated functionality as well as some ideas that are yet in the development phase. Chapter 3 - Analysis and Comparison Model, is an analysis of each element found in the background, a comparison model is presented with the intention to make it possible to compare different systems in order to determine what solution that fits the current purpose the best. Chapter 4 - Analysis and Discussion presents the final model developed in chapter 3, along with a comparison between three of the largest contactless payment systems for smartphone currently used. The three systems are: Samsung Pay, Android Pay, and Apple Pay. Three scenarios are examined in order to see what system that will fit each scenario the best.

Chapter 2

Background

2.1 Literature Study

To conduct the literature study snowballing was used. This involves finding a start set of suitable papers that will be used, the next step is to go though all the references and citations of the articles connected to the start set. The same procedure will be conducted for each of the found articles until there are no more new related articles to be found[1]. To conduct the start set Engineering Village was used for articles as well as Apple's, Google's, and Samsung's web pages for white papers regarding their contactless payment systems. Google scholar was also used to find patents on contactless payment methods as well as articles. The reasoning behind using Engineering Village and Google Scholar is that Engineering Village shows results from several of the suitable databases for this work, which makes it a convenient tool. Google Scholar was used since they have good information regarding patents, as well as some articles that are not scientifically published. In some cases, this is a bad thing, however, in this study, it was not possible to find some information in scientific articles, and therefore Google Scholar was of great use.

During the literature study all the articles analyzed are put into a database where they get tags and relations between different articles that have been identified. To find the last pieces of information, Google was contacted in order to confirm some facts that were not explained in the literature study or by reading information on Android Pay's website.

2.1.1 Limitations

In order to only find relevant information regarding the subject, the following limitations were used,

1. **Search string:** (contactless payment OR mobile payment OR m-payment) AND (nfc payment OR magnetic secure transmission OR mst) AND (smartphone or smartphones or iphone)

2. **Restriction 1:** Only articles written in English.

3. **Restriction 2:** No articles written before 2011. (The reason for this is that the first smartphone with the possibility to carry out contactless payments was introduced in 2011.)

2.2 Near Field Communication

The most commonly used communication technique for contactless payments with smartphone currently is Near Field Communication (NFC)[2].
NFC is a limited version of Radio-Frequency Identification (RFID) and communicates on 13.56 MHz with a proposed maximum range of approximately 20 cm[3, 4]

2.2.1 Communication mode

When NFC is used to communicate there are three different operating modes that may be used to do this, the modes are the following[5, 6],

1. Reader/writer
2. Peer-to-peer
3. Card emulation

Reader/writer

In this mode the NFC device may read or write to passive NFC tags. A passive NFC tag is a tag which does not emits its own magnetic field, but instead it is activated by another NFC device that emits a magnetic field[3]. Passive NFC tags are commonly used in for instance commercial posters that are possible to NFC scan.

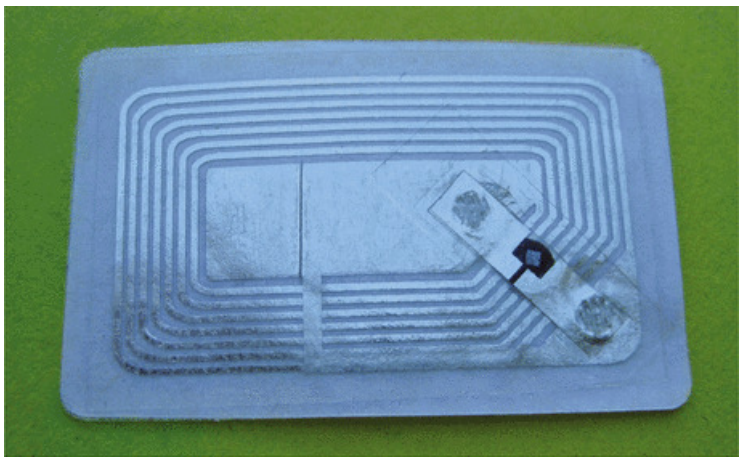

Figure 2.1: A passive NFC tag

Peer-to-peer

In peer-to-peer mode the NFC device may exchange data with another NFC device, which can for example be used to set up a secure communication line by doing key-exchanges with NFC, and then use Bluetooth to communicate afterwards[7].

Card emulation

In this mode the NFC device will emulate the behavior of a normal contactless smart card. This mode is the one that is used for all the contactless payment methods that use NFC in smartphones.
The way that this mode works is that a Point-Of-Sale (POS) terminal sends information to the smartphones NFC controller, the controller then communicates with both the application that is required to conduct the payment, as well as the secure element which has the task of securing the sensitive data, such as card number, the card security code, and expiration date of the card that has to be sent during the transaction. The card emulation method will return encrypted information regarding the payment. This information is handled by the card issuer[7].

Figure 2.2: An active NFC device and a payment terminal

2.2.2 Attacks

Relay Attack

Although NFC is expected to only work in near proximity, it has been proven that it is possible to eavesdrop communication for up to 10 meters with the correct equipment[3].
The fact that this is possible has resulted in that relay attacks have been successfully executed. To conduct a relay attack, the attacker needs the following:

1. A "mole" which is a NFC transceiver that is close to the victims NFC card/smartphone. The mole will also be able to use a communication protocol that can communicate over greater distances, such as WiFi, Bluetooth, or GSM.

2. a "proxy" which will emulate the victims smartphone with the credit card connected.

To conduct the attack the attacker will bring the mole in close proximity of the victims smartphone, and at the same time use the proxy to emulate a payment at a POS terminal. When the terminal sends a request to the proxy it will redirect the request to the victims smartphone via the mole. When the victims phone responds to the request it will be redirected from the mole to the POS via the proxy[8]
It is worth mentioning that the mole may be either hardware based or software based. It is important that users do not install applications from untrusted sources.

To counter a relay attack, suggestions have been made to lower the timeouts on communication, because when using a mole and relay via WiFi, Bluetooth or even mobile networks such as GSM, the response time will be significantly longer than with regular communication[8].

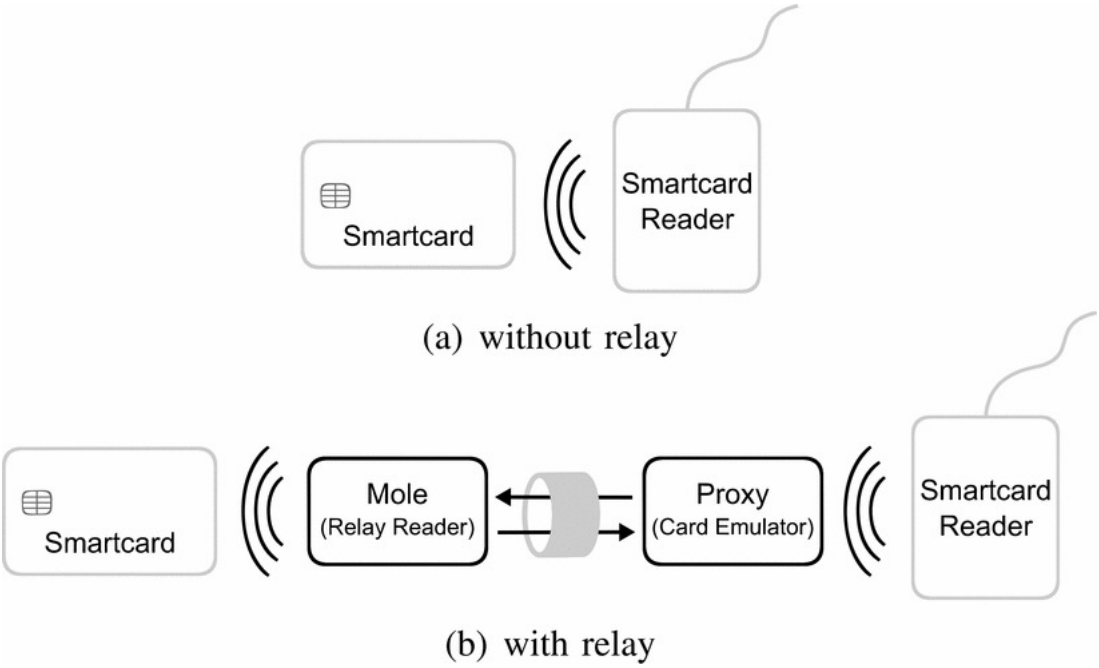

Figure 2.3: An illustration of how a relay attack is conducted

Denial of service - Jamming

An attack that has been known for a long time in RFID communication is "Jamming". Jamming is performed when an attacker sends out lots of fake messages to the victims who are trying to communicate. This will make it difficult for the victims to determine what data that is of actual importance, and what is just useless data. If the victims system does not have any countermeasures to jamming, the system will most likely stop working as long as an attack is ongoing. It is worth mentioning that it is harder to conduct this attack against a NFC system compared to most of the regular RFID systems since NFC has a much shorter range, but since it has been proven to be possible to transmit and receive NFC for ten meters, it is still a realistic threat.
A solution to jamming is for the POS terminal to measure the signal strength of all incoming transmissions, if the signal strength is abnormally strong, the device will ignore this transmission. When jamming, the signal strength is most likely going to be higher than for normal communication and the reason is that the attacker wants to be sure that the signal will reach the victim[9].

Denial of service - Terminated Secure Element

Another Denial of Service (DoS) attack that is possible to perform is to infect the victims phone with malicious software that has permission to communicate with the secure element, and the only task this program has is to try and authenticate itself to the secure element software ten times. When there have been ten unsuccessful authentication attempts in a row, the secure element will set itself in a state called "TERMINATED", and this means that the secure element will not be able to communicate with other hardware anymore. This state is irreversible, which means that the secure element will not be functional again[10]. The attack is also possible to conduct on application level, which means that instead of attacking the secure element directly, one may attack a specific application and only putting that specific application in TERMINATED-mode. The study stating this facts is from 2013, which means that there is a possibility that newer systems have mitigated this risk. However, no information for either Samsung Pay or Apple Pay was found regarding this.

To counter this type of attack, it is important that the user is aware of what dangers different permissions might result in. In this case, the user should never allow an application that is not trusted to communicate with the secure element. This awareness is important for other applications and permission levels as well. Another solution mentioned in [10] is to redesign the secure element access control in such a way that the described attacks would be impossible to conduct.
If the attack was against one specific application, it will be sufficient to only re-install the application in question.

Eavesdropping

In all wireless communications there are risks of eavesdropping and NFC is no exception. It has been claimed to be possible to eavesdrop NFC communication up to ten meters away from the victim[3]. In the case of payment systems that uses NFC, the information that is sent is likely to be confidential and might therefore cause the victim great problems if leaked. To conduct an eavesdropping attack, all the attacker has to do it so build a transmitter device that has an antenna that is strong enough to pick up signals from as far away as possible.

Since the attacker does not transmit any data when eavesdropping, it is impossible to detect when an attack is conducted, and therefore it is impossible to defend during an attack. Therefore countermeasures for this kind of attacks has to be taken before the data is transmitted. The countermeasure used today is to set up a secure channel with the help of an encryption protocol between the two devices that wants to communicate without the risk of someone eavesdropping the messages. Another solution is to implement a tokenization process in order to make the information sent less sensitive. Tokenization works the such a way that the actual smartphone does not store the card information, but rather stores a token, which is sent to the payment terminal in order to fetch the card information. Tokenization is described more in depth in chapter 2.5.

2.3 Magnetic Secure Transmission

A major issue with NFC is to convince retailers to install new POS terminals that support the NFC technology. Therefore a company named LoopPay developed Magnetic Secure Transmission (MST), which is a component that emulates the magnetic field of a card's magnetic strip[11, 12]. In 2015 Samsung bought LoopPay[13] and has since then continued the development of MST[13].
The main advantage of MST compared to NFC is that the retailers are not required to get new equipment and therefore the adoption speed of smartphone payment systems is expected to increase.

2.3.1 Attacks

Skimming

The largest issue with the magnetic cards used today is how easy it is for attackers to perform a skimming attack in order to steal the card information. This is solved in MST with the help of mobile tokenization and each token is only valid for one transaction. The token is generated with a cryptography function that uses a private key, which makes it very difficult for an attacker to generate a valid token[14].

A skimming attack is when an attacker reads the magnetic field generated by a magnetic card in order to later emulate the same magnetic field and thereby use the victims card information to make the payment.
To counter skimming attacks, reversible hybrid tokenization is used to handle the sensitive information and hence make it hard for an attacker to conduct a successful attack. A reversible hybrid tokenization is a token that stores information which can be retrieved by decrypting the token[15, 14]. More information about tokenization can be found in chapter 2.5.

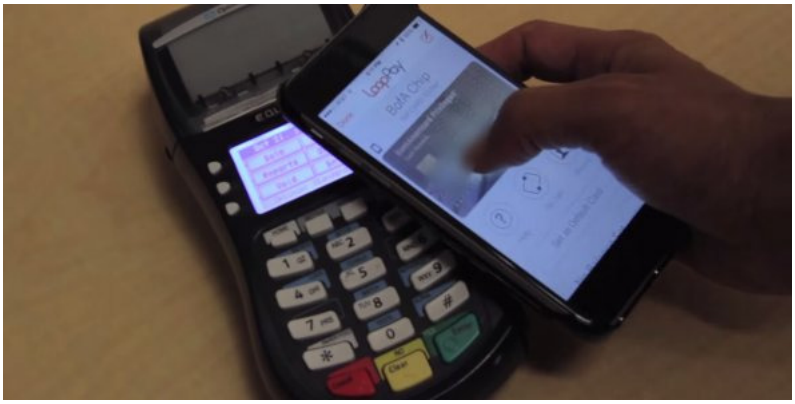

Figure 2.4: A MST payment at a
point-of-sales terminal without NFC support

2.4 Card Emulation

It is of great importance that the part of the smartphone that handles the sensitive information regarding card number and other personal information has a high grade of security in order to prevent attackers from stealing that information.
This information can be handled either by the hardware, with a Secure Element (SE) or in the software, with Host Card Emulation (HCE).

2.4.1 SE

There are several different types of secure elements, each one of them has their advantages and disadvantages but they all have the same goal: "securely store data and to carry out cryptographic operations."[5].
A secure element never communicates with the smartphones Operative System (OS) or directly with the CPU, it rather communicates through the SE, see Figure 2.5[4].
Both Samsung Pay and Apple Pay use a SE chip[11, 16], but their way of using the SE differs.
Apple Pay uses a coprocessor inside the CPU called "Secure Enclave" to handle

communication with the SE in a encrypted and secure fashion with the help of a tokenization process, as well as communicating with Apples data servers[17]. The secure enclave is also responsible for authenticating the user if the fingerprint scanner is used[16].
Samsung pay on the other hand uses the SE chip to fetch tokens from the token service provider (normally a bank) which is then used right away together with some public data, such as the price of the transaction[18].
A more in depth description of how the Secure Element is used in Apple Pay and Samsung Pay is presented in Chapter 2.5.5.

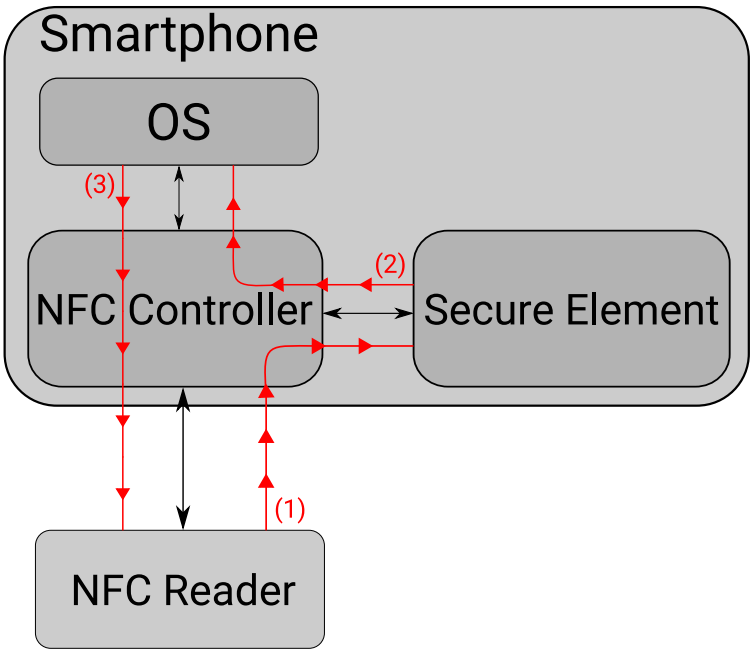

Figure 2.5: NFC communication with SE

SIM

Several mobile network operators (such as Bell, and Telus) offer SIM cards with NFC SE support. This means that the phone is not required to support HCE or have an integrated circuit for SE, but instead the SIM card acts as the SE.
The sensitive information regarding card number and such are then stored encrypted on the SIM cards SE which is only available for communication through the NFC controller[5].

Advantages

- Works on all smartphones that are using a SIM card and supports the use of NFC.

- The phone manufacturer does not need to add specific hardware to support the system except NFC.
- Removable - Makes it easy for the user to change phone.

Disadvantages

- Not compatible with CDMA phones, since they do not use a SIM card.
- It becomes harder for the user to change operator.

Chip

A chip is what both Samsung Pay and Apple Pay use. The chip is soldered onto the smartphone at the manufacturing process. This part of the smartphone is only accessible via the NFC controller. When using a integrated chip, the risk of an attacker that manages to steal the SE is also reduced compared to a removable SE[19].

Advantages

- High level of security.
- No requirement on the user to buy specific SIM/SD-card.
- Not bound to any specific operator.

Disadvantages

- Higher manufacturing cost.
- Not possible to use the SE in another smartphone when the user is switching phone.
- If the chip is broken (by e.g a DoS attack as described earlier), it is difficult to repair the damage.

Since manufacturers like Apple integrate an SE chip in all their new smartphones, one can argue that there are no disadvantages in that the SE is not removable, since the user gets a new chip in each new phone from Apple. But if the user wants to change to a phone from another manufacturer, it is not guaranteed that the new phone supports a SE chip.

SD-card

SD-card SE was greeted as a promising technology with a bright future in the early days of NFC. But with the development of the other types of SE, and when more new smartphones dropped support for SD-card's, the alternative solutions gained larger portions of the market[19].
Despite the fact that the market has lost a lot of interest in SD-card SE, the SD Association is developing a standard called "smartSD Memory Cards" which focus on the SE capabilities of the SD-card[20].
Because of the current situation on the contactless payment market, and that smartSD memory cards are not available for customers to buy, it was decided that sd-card as SE was excluded from this thesis.

2.4.2 HCE

HCE is a software based solution in the regard that the smartphone user is not required to have any dedicated hardware to handle the sensitive information, but rather the hardware that handles the sensitive information is located in a cloud, normally at the card issuer. Therefore HCE is in some cases called "Cloud based SE". In 2012 Blackberry released the first smartphone that supported HCE. Some time later HCE was adopted by Google in the Android OS since android 4.4 (KitKat). Since April 2014 Google migrated to HCE, and it is now the only accepted card emulation method for Android Pay and their other payment solution called Google Wallet[4].
For the end user there is no difference between HCE and SE, but the greatest advantage of HCE is that the phone manufacturer does not have to develop a phone to support anything else than a NFC chip and an Android version of 4.4 or higher.

HCE is constructed in a way so that the OS has libraries and APIs that will be used to communicate with the POS terminal via the smartphones NFC controller and hence the POS will communicate with the OS via the NFC controller. See figure 2.6.

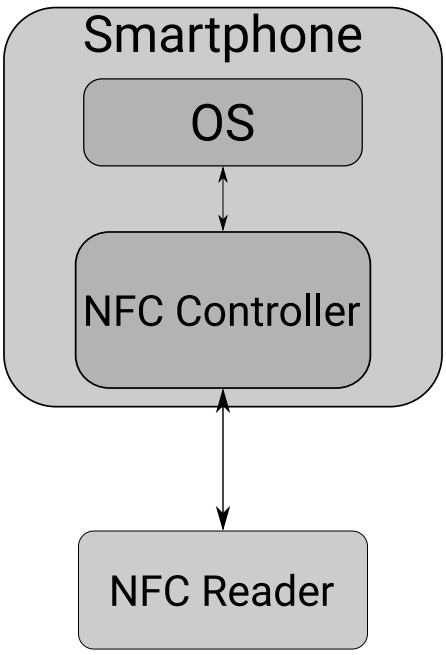

Figure 2.6: NFC communication with HCE

Advantages

- Does not require the phone manufacturer to create a phone that has an integrated SE.
- Computing and storage capacity is higher than in SE.
- Development complexity and cost is lower than with a SE.
- HCE is independent of what service provider the chosen.

Disadvantages

- Puts a higher demand on the OS and the APIs that communicate with the HCE to limit the risks of malicious software that exploits the system.

Full Cloud based HCE

This is a proposed solution to decrease the amount of sensitive information that can be eavesdropped by the public and it is achieved by handling the card emulation in a secure cloud which the smartphone authenticates against for each transaction that is going to be made.
The advantage with this solution is that very little information can be stolen from the phone. But the risks are that if there is a successful attack against a cloud that is hosting the sensitive information, the amount of leaked sensitive information

might be tremendous. There is also a great drawback of this system, and that is that the user is required to have fast internet access each time a transaction will be conducted. It is suggested that 4G or 5G is used for sufficient speed[21].

2.5 Tokenization

To further increase the security of contactless payment, tokenization was developed. Tokenization is a solution to reduce the amount of sensitive information that is being sent and also decrease the sensitivity of the information sent.

2.5.1 Tokenization use case

Figure 2.7 shows a theoretical use case scenario for contactless payment with tokenization[15, 22].

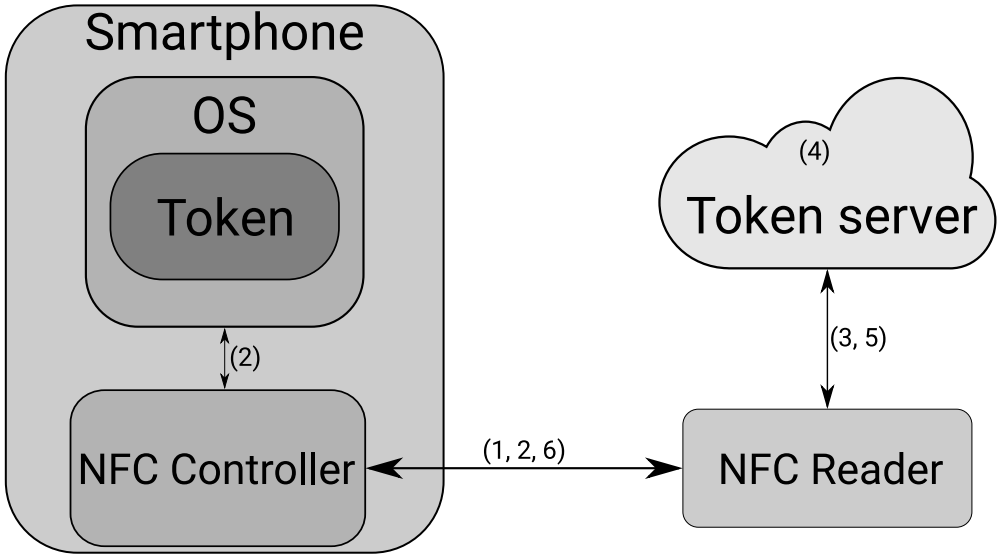

Figure 2.7: Contactless payment with tokenization

1. The smartphone gets in near proximity of the NFC reader.
2. The NFC controller fetches a token from the OS and sends it to the NFC reader.
3. The NFC reader sends the token to the Token Service Provider (TSP).
4. The TSP check the token mapping to find if and where the card information is stored.

5. The card information is fetched from the Card Data Vault (CDV) and is sent back to the NFC Reader.
6. The NFC Reader reports back the complete status of the transaction.

2.5.2 Security Domains

In order to achieve a secure tokenization process, it is suggested in the PIC tokenization guidelines[15, 22] that a tokenization service treats the following security domains:

1. Token Generation
2. Token Mapping
3. CDV
4. Cryptographic Key Management

Token Generation

A process that creates a token that the card owner may send to the POS terminal. The token generation is conducted by the TSP, which often is the card issuer.

Token Mapping

Token mapping is used to keep track of what tokens that are connected to which card information. This domain will also include access control and logging for tokenization and de-tokenization requests.

Card Data Vault

The CDV is in charge of encryption and the Card information is stored here. Access control is implemented to restrict user permissions.

Cryptographic Key Management

In this domain the cryptographic principles are declared and it is defined how the encryption and decryption will work.

2.5.3 Token types

irreversible tokens

Tokens that are irreversible can not be used to retrieve any sensitive information, but only to verify transactions, or to connect a user to a non-sensitive unique data string.

reversible tokens

It is possible to retrieve sensitive information from a reversible token either having access to the cryptographic key for decrypting if the token is encrypted, or by sending the token to the CDV to fetch the data bound, if it is a non-cryptographic token.

2.5.4 Attacks

Eavesdropping

If only the tokenization process was conducted, and no other security measures, it would still mean that an attacker could eavesdrop the token transmission and then use the stolen token again. This can be countered by setting a limit on the tokens, either by a limited validity time on the token, or by a limited transaction amount for one token[21].

2.5.5 Practical use

Samsung Pay

When a user initially registers a new card to Samsung Pay, a request containing the card information is sent to the TSP. The TSP communicates with the card issuer in order to validate the card information sent. If the card information is valid, the TSP returns a token to Samsung Pay.

When the user tries to make a payment with Samsung Pay, he is required to either enter a text-based password or complete a biometric scan. Then a request is sent to the POS terminal from the smartphone. In that request all the payment information along with the token data is sent. The POS terminal forwards the token and other relevant data, such as token requester ID, expiry date and cryptogram to the merchant acquire (The merchants bank). The merchant acquire sends the data to the TSP, which will answer with the actual Card information. Finally, the card information is sent to the Card issuer of the users card in order to validate the card information. If the information is valid, the transaction is successfully conducted, if the information is not valid, the transaction will not be conducted[18].

No information regarding offline support has been found, although on the support page for Samsung Pay, it has been stated that Samsung Pay may return the error "No network connection" or "Network problem occurred"[23]. Which strongly indicates that Samsung Pay requires internet access in order to maintain required functionality. Hence it is also likely that between each transaction a new token is requested from the TSP.

Android Pay

When a new credit card is connected to Android Pay the card information is sent to the TSP, which will return a token to the smartphone that will be encrypted and stored on the device.

When the user tries to make a payment with Android Pay, he is required to either enter a text-based password or complete a biometric scan. Then the token will be sent along with some non-sensitive information, such as the time of the transaction, and what items that is brought, to the POS terminal. The POS terminal will send the token to the merchant acquire (the merchants bank) which will identify the TSP of the token and send a request to get the card information given the token received. The TSP will respond with card information and information regarding which bank has issued the card. The transaction information is sent to the card issuing bank, which will authorize the transaction and send a response back. The merchant acquire returns the response regarding if the transaction was successful or not to the smartphone[24].

There is no information regarding offline support in the case either, although Google was reached for comments and an employee confirmed that Android Pay is not supporting offline transactions, and that a token is only valid for one transaction.

Apple Pay

Apples iPhone uses a secure element chip called the "Secure Enclave". The Secure Enclave is used to validate the user by biometric scan or password. When the authentication has succeeded, the Secure Enclave gathers the payment information, such as total sum to pay, a device unique identifier for the iPhone, as well as a cryptogram that is only available to use once, along with this the merchant information is fetched as well. When the information is gathered, the Secure Enclave creates an encrypted token.
The token is then sent to a server hosted by Apple, and this server's task is to yet again encrypt the token, but this time the merchants public key is used to encrypt it. This encryption is to prevent attackers from reading any sensitive information if the token is stolen. The token is then sent back to the iPhone, which then sends the token to the POS terminal. The terminal decrypts the token and carries out the transaction[16, 17].

2.5.6 Offline compatibility

With the help of tokenization it is possible to handle transactions where the smartphone is not required to have internet access when making the payment.

The offline support may be added by either make the token only usable during a given time or by installing a spending limit. If e.g a token is usable for 24 hours, the user is required to have internet access once every day to refresh the token. This would mean that an attacker only had a maximum of 24 hours to try to use the token. The solution containing a spending limit means that the token is only valid to use until the point where the limit is reached. With this solution even if the attacker manages to steal and exploit the token, he would only be able to steal a limited amount of money. If either of those two solutions were combined with a geographical proximity checking, it would be possible to make the process rather safe.
However none of the contactless payment systems analyzed has offline support.

2.6 POS time

When using contactless payment the execution time is decreased compared to card and cash payments, and according to a study conducted by American Express the contactless payments are up to 63% faster than cash payments and 50% faster than card payments[25]. The speed up of contactless payments is a huge selling point, but there is a trade-off between speed and security. In the case of contactless payment some of the early systems had no authentication, such as pin-code, password, or biometric authentication. This resulted in a faster execution time, but greatly decreased the security.

When comparing Samsung Pay, Android Pay and Apple Pay, both Android Pay and Apple Pay run fully in the background when the smartphone is unlocked. This means that as soon as the smartphone gets in close proximity to a POS terminal, the payment application will open up and the user may start the authentication process. Samsung Pay, on the other hand, requires the user to manually start the app, which is done by swiping upwards from the bottom of the screen. This results in a little longer execution time for a Samsung Pay user, but on the other hand it is an extra layer of defense against attacks that execute without the victims knowledge.

2.7 Privacy

In payment systems the level of privacy is of great concern for some users, while other users do not value their privacy highly in comparison to other factors and features, such as getting suggested product in regard of your shopping behavior. Regarding contactless payment systems it is a trivial task to gather and store user information that intrudes on the user's privacy, since all the purchase and transaction information is passed through the payment application. This information

can then be used by the payment service provider to send targeted advertisement to the user, send coupons, or to send other advertisement related messages to the user[26].

2.8 Demographics

During this study, it has been difficult to find official number of users, transactions and the current state of geographical spread. Hence some of the numbers in this section are fetched from internet pages. However citations in this section were considered to be unbiased since the companies behind the sources are companies that work mainly with statistics and analytic work.

2.8.1 User base

The smartphone industry is a rather new field. Despite that, the user base has grown enormously in the last couple of years. The number of smartphone users are expected to pass 2 Billions during 2016 [27]. Out of all these users, chart 2.1 shows the monthly users base of the following three systems: Samsung pay, Android pay and Apple pay[28].

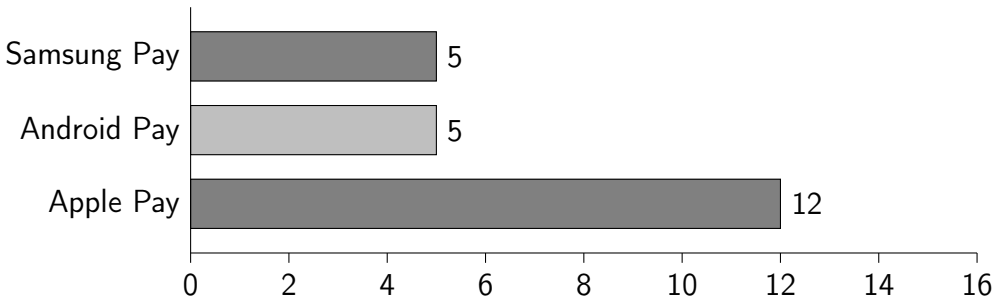

Chart 2.1: Million of users worldwide, March 2016

2.8.2 Adoption

During the period between November 2014 and October 2015, the amount of people that have tried Apple Pay has increased with approximately 85%[2].

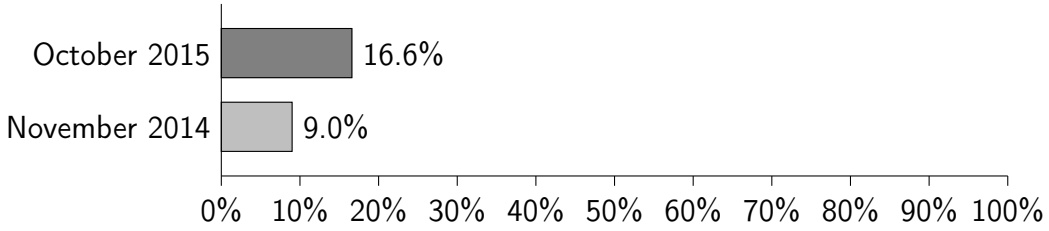

Chart 2.2: Percent of iPhone 6 and iPhone 6 plus that have tried Apple Pay

Given chart 2.1 and 2.2, almost 2.000.000 users had tried Apple Pay in October 2015. However, only 5.1% of the users of the statistic collection in [2] said that they used Apple Pay in order to make the payment connected to the study. The reasons given for this were mainly that they either forgot to use it, or that they were not sure if Apple Pay was accepted at the payment terminal.

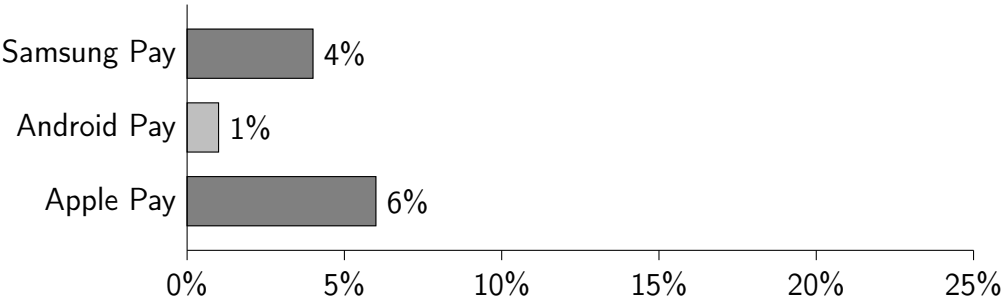

Chart 2.3: % of customers using Samsung/Android/Apple Pay

Chart 2.3 shows how many of the currently used products from Samsung, Android and Apple that are used to conduct contactless payments[28]. For Apple devices, it requires that the device has the Security Enclave as well as the NFC chip. For Android and Samsung devices, the requirement is that the device is able to use NFC or MST.

Global NFC market revenues

In 2013, the company "MarketsandMarkets" showed the current revenue of NFC payments, as well as a prediction on how the market would develop in the years to come, up until 2016, the following graph shows the development and prediction[29].

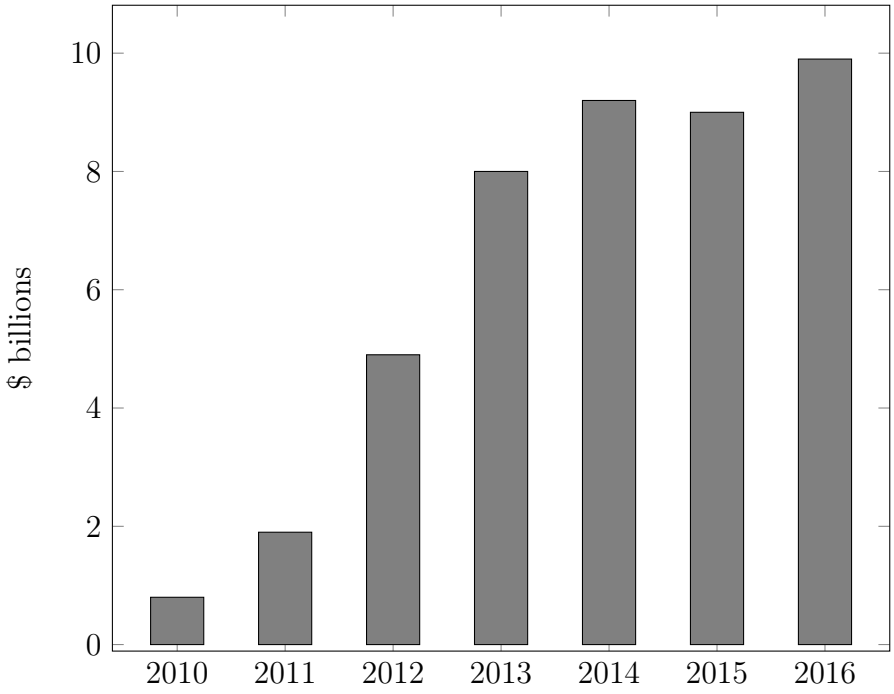

Table 2.1: Market revenue of NFC payments
Newer statistics were not found publicly available from any reliable source.

2.8.3 Geographic spread

Samsung Pay

Samsung pay is currently available in USA, United Kingdom[30], South Korea[31], China[32].

Android Pay

Android Pay is currently only available in the USA[33].

Apple Pay

Apple Pay is currently available in USA, United Kingdom, Canada, Australia, China, and Singapore[34].

Chapter 3

Analysis and comparison model

3.1 Introduction

In the sections below, each element presented in the background will be discussed in order to determine what degree of importance it has got when comparing there payment systems.

3.2 Element value

In order to make a comparison model that is versatile, a value-system is created. With the value-system it is possible to evaluate contactless payment systems in regard of what scenario that are currently present. in the chapter "Analysis and Discussion", three scenarios of interest is presented, and the model will be used to conduct the comparison in regards of the scenario. The value grading goes from 0 to 5, where 0 means that the element is not worth anything in the given scenario, and 5 means that the element is of greatest importance. A scale from 0 to 5 was chosen because with a scale that has too many steps, it will be difficult to determine between two close values, and if the scale would have less steps, it would in some case mean that two elements would get the same grading, even if they actually should differ.
In order to construct the comparison model for contactless payment systems, all the elements from the chapter "Background" have been analyzed and evaluated regarding how each will fit into the model.

It is also worth mentioning that even though the element value set in each scenario is generated by analyzing information from previous work, the grading will run the risk of being subjective by the person that makes the grading. Which in this case is the thesis author.

3.3 Communication method

Regarding the communication method there are currently two solutions, NFC and MST. MST is patented by Samsung and hence only Samsung Pay has implemented MST. The advantage of MST is that it does not require the POS terminals to be upgraded, and therefore the adoption rate of contactless payment methods is likely to increase.
Although, in a future scenario where contactless payment methods are the standard way to make payments, and all POS terminals have integrated hardware and software to handle NFC, which new terminals today support, the need for MST will most likely disappear over time. This would mean that the hardware required in the smartphone to support MST would be an additional cost for the manufacturer, and finally the customer.
For these reasons, the communication method is considered an important part of the model as of the current state of the systems.

3.4 Card Emulation

In order to keep the manufacturing cost down, as well as to handle availability and security, the card emulation method is of great importance. An HCE solution does not require additional hardware, while SE does. Hence manufacturing cost and availability will differ between these two. However previous researchers do not fully agree on what solution is the most secure[4, 21, 9].
Full cloud based HCE has been mentioned in[21], however, this solution is currently not used by any contactless payment service that has been found during this study. The reason for this is most likely that the high requirements on internet speed and stability can not be met with the currently available networks.
It is important to take into account that HCE is a rather new technology which in all forms relies heavily on the cloud. This is a new potential risk zone that has not yet been examined fully in the case of contactless payment systems.

3.5 Tokenization

In order to protect a wireless communication, tokenization is the most promising technique at the moment. If tokenization is combined with a good encryption and tokens with either time limitations or spending limitations, the system will reach an adequate security state given the currently known threats today[8, 7].
A system without tokenization would make it a trivial task for an attacker to eavesdrop transaction data and steal victims credit card information. If an encryption method was used to hide the credit card information one could potentially protect this information, however the system would still be vulnerable to malicious software. For a system that has an integrated tokenization process, the

credit card information is only located on the smartphone device until the first token is requested, hence the sensitive information is considerably more challenging for an attacker to steal.
Given what has been stated, tokenization is an essential part of the comparison model.

3.6 Offline compatibility

In section 2.5 it is mentioned that tokenization opens up the possibility to create a rather secure transaction without having internet access on the smartphone conducting the payment. Even though this is the case, offline support is not implemented in any of the systems tested in this study. In the future, the offline support might not be relevant since the internet coverage becomes greater every day, but as of today, there are cases when smartphones do not have internet access. The current solution to this is for the store to install a public WiFi which the customers may use to conduct their payments. However, this solution defeats the purpose of contactless payment systems, since the idea is to make a more convenient payment system and to decrease the POS time. This would only work if the user is a regular visitor of the store, and has already stored the WiFi details so automatic connection is established.
Given the potential value of offline compatibility, it was integrated in the comparison model.

3.7 POS time

In order to convince store owners to invest money in a new POS terminal that is compatible with NFC, one must be able to argue that there is a financial gain in implementing the new technology. One valuable aspect to argue would be to show that the POS time would decrease in comparison to currently used systems. As mentioned in the Background, there are reports claiming that contactless payments are significantly faster than both cash payments and credit card payments. In regard of the current state of contactless payment systems, it is important to focus on how to enhance the systems in a way that will increase the number of users. Hence, POS time is an important aspect.
However, the POS time is a complex variable which is difficult to grade considering the fact that the POS time should be graded in comparison to other available solutions. However it is still suggested that POS time is taken into consideration since it is important for the user experience, but it will be almost impossible to do with a comparison model that only handles true/false grading.
In regard to the the aspects mentioned, POS time was excluded from the comparison, since it would be almost impossible to make a fair evaluation.

3.8 Privacy

For some users, privacy is one of the most important factors of a system. On the other hand some users value other elements higher and because of this the privacy aspect might be forgotten.
Regarding privacy, both Samsung and Apple clearly state in their privacy policy that their payment systems do not store more privacy sensitive information than required about a customer[35, 36]. Google on the other hand states the following in their privacy policy for payments with Google[37]:

> "When you use Google Payments to conduct a transaction, we may collect information about the transaction, including: Date, time and amount of the transaction, the merchant's location and description, a description provided by the seller of the goods or services purchased, any photo you choose to associate with the transaction, the names and email addresses of the seller and buyer (or sender and recipient), the type of payment method used, your description of the reason for the transaction, and the offer associated with the transaction, if any."

In conclusion privacy is an important aspect in some scenarios, where in other scenarios it is of no interest. Hence it is added as a part of the comparison model.

3.9 Model

Table 3.1 presents a suggested comparison model given an analysis of the findings from the background. The model can be used in order to compare different systems against each other.

Value	Element\Service	service
Communication method		
0-5	NFC	
0-5	MST	
Card Emulation		
0-5	Secure Element - Chip	
0-5	Secure Element - SIM card	
0-5	Host Card Emulation	
0-5	Full cloud based HCE	
Tokenization		
0-5	Token	
0-5	Offline compatibility	
Miscellaneous		
0-5	Privacy	

Table 3.1: Comparison model

Chapter 4

Analysis and Discussion

4.1 Model

Table 4.1 shows the suggested comparison model implemented without any values on the elements, but only the true/false marking on each element factor.
Android Pay, Samsung Pay and Apple Pay have been inserted and the information regarding which element that each service uses has been fetched from previous information in the thesis, as well as: [11, 12, 38, 8, 17, 16].

Value	Element\Service	Android Pay	Samsung Pay	Apple Pay
Communication method				
0-5	NFC	x	x	x
0-5	MST		x	
Card Emulation				
0-5	Secure Element - Chip		x	x
0-5	Secure Element - SIM card			
0-5	Host Card Emulation	x		
0-5	Full cloud based HCE			
Tokenization				
0-5	Token	x	x	x
0-5	Offline compatibility			
Miscellaneous				
0-5	Privacy		x	x

Table 4.1: Comparison model with Samsung Pay, Android Pay, and Apple Pay

In the following sections, three scenarios will be presented with an introduction, followed by an analysis of how important each element is in the given scenario. After this, the score is is calculated and followed by a conclusion on the scenario

and results.

It is important to note that the following scenario-sections element analysis are not fully objective since it is the author of the thesis that has set the values. However the scores are set given information collected form the information presented in the background section.

4.2 Scenario 1 - Uprising technology

Currently the contactless payment systems for smartphones have a limited user base, hence it is of great importance to find new ways to recruit new users in order for the companies behind the solutions to make a profit worth the development costs that is involved.

4.2.1 Element analysis

1. NFC - NFC is the most commonly used communication method for contactless payments today. However the big issue with NFC today is that there are very few POS terminals that are equipped with a NFC reader. Since NFC is still a usable element, it should have a value larger than 0, however, the drawbacks are great. With this in mind, the value of NFC was set to 1.

2. MST - MST reduces the current requirement on the merchants to invest in new POS terminals, and it enables most of the currently used POS terminals today to support contactless payments. Given the positive effects, MST value is considered highly important, therefore the value is set to 5.

3. Secure Element - Chip/SIM card - The use of SE in order to enable contactless payments has made it much more difficult for the market to adopt to this new solution. The reason is that each SE will cost the manufacturer extra money, which will then increase the price of the product. With this in mind, SE is likely to have harmed the adoption speed, and therefore the value is set to 0 for both types of SE.

4. Host Card Emulation - A system that supports HCE lowers the production cost for smartphones compatible with contactless payment systems. HCE also allows smartphones that is not equipped with a secure element to conduct contactless payments. The value of HCE is set to 4 since it makes a large number of smartphones currently used to support contactless payments. The reason for why it is not set to 5, is because MST is considered a more important aspect, since the largest issue right now is that the POS terminals lack the support.

5. Full cloud based HCE - Since it is an HCE solution, the positive aspects mentioned regarding HCE can be applied on Full cloud based HCE. However Full cloud based HCE put tremendous requirements on the users internet connection speed. Hence in the current scenario where the internet speed is not sufficient in the majority of locations, this element is not as highly valued as regular HCE, therefore the value is set to 2.

6. Token - In order to recruit new users, one selling point is to show the users that the service is secure and safe to use. This is especially the case in regard of services that handles sensitive bank information. Therefore the token process is of interest. However the token process is yet not as important as for instance HCE since tokenization is not a total necessity for the system to work, therefore the value of the token was set to 3.

7. Offline compatibility - In order to recruit more users, it is important to increase the level of convenience. To support offline transactions would increase the convenience by making the payment process smoother, and possibly faster as well. This is not a crucial functionality, however a highly desirable one. Because of this, the value is set to 3 - which is the middle of the scale.

8. Privacy - The privacy aspect is of very little interest in the "Uprising technology", because it is a new system and the users often wants to see the full potential of the product with no regard of how it works. The privacy aspect will often be overlooked in this state. Hence the value of privacy is set to 0.

Given the element evaluation, Table 4.2 shows the evaluation with element values inserted regarding this information.

Value	Element\Service	Android Pay	Samsung Pay	Apple Pay
Communication method				
1	NFC	x	x	x
5	MST		x	
Card Emulation				
0	Secure Element - Chip		x	x
0	Secure Element - SIM card			
4	Host Card Emulation	x		
2	Full cloud based HCE			
Tokenization				
3	Token	x	x	x
3	Offline compatibility			
Miscellaneous				
0	Privacy		x	x
	Score:	**8**	**9**	**4**

Table 4.2: Comparison model - Scenario 1

4.2.2 Conclusion

In the "Uprising technology" scenario, Samsung Pay is suggested as the best suited solution for contactless payments. The one thing missing for Samsung Pay that is holding the system back from gaining a huge user base is the fact that it is only geographical available in a fraction of the world. However, Android Pay has almost as high score as Samsung Pay, Samsung gain the high score by supporting MST, Android gain the score by supporting HCE. Both those solutions are created with the idea of increasing the convenience for the user and merchant, but the approach varies.
One thing to take into consideration with this scenario, is that Apple Pay has the lowest score, and yet Apple Pay has the largest amount of users according to the statistics mentioned previously. There are several reason for this, since the supported services is not the only factor that comes into play. Apple Pay is the solution that is supported in the largest amount of countries. Hence the amount of potential users is significantly larger. It may also be because of the fact that the company creating the payment service has to make an agreement with each and every bank that they want to support. This could indicate that even though Apple Pay does not support all the highest suggested elements in this model, they do a better work in making deals with the banks, and spread the support better

geographically, which gives them a larger user base.

4.3 Scenario 2 - User trust

In order to maintain a high level of trust, any type of service is required to protect its users from attacks and in many cases emphasize on the fact that they value the customers security and privacy. In order to maintain a high user base, the trust of the users is required.

4.3.1 Element analysis

1. NFC & MST - There have not been found reports regarding if NFC or MST is more secure. Given this, the communication method is of no interest in this scenario, hence both NFC and MST is set to a value of 0.

2. Secure Element - chip - The SE Chip has been proven to have a high level of security. The chip is considered to have a higher level of security than the SE SIM card since the SIM card is actually a removable part of the smartphone. The SE chip has been given the value 3 on the scale.

3. Secure Element - SIM card - The SE SIM card is mostly valued the same as the SE chip, although, the possibility to remove the SIM card result in that the SE SIM card value is set to 2.

4. Host Card Emulation - It has in some cases been stated that HCE is less secure than SE, however in other cases, the opposite has been said. Therefore the value of HCE is set to the same as SE chip, 3.

5. Full cloud based HCE - Currently Full cloud based HCE is just a theoretical solution and it is not possible to set a value on this card emulation solution, and the value is set to 0.

6. Token - In order to keep the sensitive information as secure as possible, tokenization is implemented. If this were not the case, the user would have to send the actual card information wirelessly to the POS terminal. The tokenization process is a core element in order to keep a high level of security and the token value is set to 5.

7. Offline compatibility - The offline compatibility was not considered to be able to have any compact on the user trust. The value was set to 0.

8. Privacy - In order to gain trust by the users, one solution is to focus on retaining a high grade of privacy for the users information. However the

privacy element is hard to grade in some way because different users may have their own opinion regarding privacy. Hence it was decided that the privacy aspect value should be set to 1. This results in that it does not make any major changes to the scores, but still not totally overlooked.

Given the discussed element evaluation, Table 4.3 shows the outcome with element values inserted.

Value	Element\Service	Android Pay	Samsung Pay	Apple Pay
Communication method				
0	NFC	x	x	x
0	MST		x	
Card Emulation				
3	Secure Element - Chip		x	x
2	Secure Element - SIM card			
3	Host Card Emulation	x		
0	Full cloud based HCE			
Tokenization				
5	Token	x	x	x
0	Offline compatibility			
Miscellaneous				
1	Privacy		x	x
	Score:	**8**	**9**	**9**

Table 4.3: Comparison model - Scenario 2

4.3.2 Conclusion

In the "user trust" scenario all three services have a very similar score, and it is not possible to determine a fair winner in the scenario. The one thing that made a difference was that Google's privacy policy is not as strict as Samsung's and Apple's. Hence Android Pay lost by one point. But overall, all three services applies almost the same actions in order to ensure a secure service.

4.4 Scenario 3 - Future system

A final important scenario, which is hard to predict, is how the systems will work in the future, and what elements that will be important in the future. This

scenario is an attempt to predict what will be important in the year 2025. The year 2025 will be nine years away from when this thesis were published, hence it is very likely that contactless payment systems has moved into the next phase, beyond the establishment phase.

4.4.1 Element analysis

1. NFC - It is very likely that NFC has become a standard on POS terminals, hence NFC is an important element. Although NFC is important, there are other elements that are more important. Therefore the value of NFC has been set to 3.

2. MST - MST is a patented technology owned by Samsung and currently no other manufacturer has implemented it, and other actors will most likely focus on promoting NFC instead. As mentioned in the NFC section, it will probably be standard for POS terminals to support NFC by 2025, and with this advancement MST will not be needed anymore. It is also worth taking into consideration that regular magnetic cards is already an outdated technology that is not supported by all POS terminals today, and magnetic card support will most likely be even less in the future. Hence the value of MST will be set to 0.

3. Secure Element - chip - SE chip is a tested solution that has high credibility and is thoroughly tested. Because of this it is predicted that SE Chip will still be present. However, the popularity of SE chip is likely to decrease when software based solutions emerge that is more cost effective. The SE chip value has been set to 2.

4. Secure Element - SIM card - SE SIM cards were a temporary solution in order to enable contactless payment systems to work on phones that does not have a SE chip. Although with the release of HCE, SE SIM cards will most likely be unnecessary, since HCE is much more convenient for the user. Hence the value has been set to 0.

5. Host Card Emulation - Since HCE is a new technology, it is hard to predict its future. But a software solution that is as secure and works the same way as a hardware solution is most likely going to be preferred, in both cost and convenience perspective. Hence it is predicted that HCE is a key element in the future and the value is set to 5.

6. Full cloud based HCE - This is yet only a concept and therefore it is hard to predict the future of it. But given the current development of network speed and connectivity, it is possible that a full cloud based HCE solution is possible to manage in 2025. With this information in mind, full cloud based HCE is valued the same as standard HCE, 5.

7. Token - The only reason for tokenization to be irrelevant is if it replaced with another solution that handles the same issue. Since there has been no alternative suggestions found during this study, it is likely that tokens will be used in this scenario as well. Hence the value is set to 5.

8. Offline compatibility - As mentioned in "full cloud based HCE", it is likely that internet connection will not be as big of a problem as it is today. However, it is very difficult to guarantee a 100% network connection rate, therefore offline compatibility is likely to still be of a certain value. Therefore the value is set to 1.

9. Privacy - There is often discussion regarding privacy, despite this, services that does not value the users privacy grows larger every day, and there are currently no signs indicating that this trend is about to change. Therefore privacy will most likely be of very little interest in the future as well. Hence, the value is set to 1.

Given the discussed statements, table 4.4 shows the evaluation with element values inserted regarding this information.

Value	Element\Service	Android Pay	Samsung Pay	Apple Pay
Communication method				
3	NFC	x	x	x
0	MST		x	
Card Emulation				
2	Secure Element - Chip		x	x
0	Secure Element - SIM card			
5	Host Card Emulation	x		
5	Full cloud based HCE			
Tokenization				
5	Token	x	x	x
1	Offline compatibility			
Miscellaneous				
1	Privacy		x	x
	Score:	**13**	**11**	**11**

Table 4.4: Comparison model - Scenario 3

4.4.2 Conclusion

In the "future system" scenario, Android Pay scores the highest, however both Samsung Pay and Apple Pay has a high score as well, and the difference is small. Therefore it is not fair to say that Android Pay will be guaranteed to best fit a future scenario. However, Android Pay supports new technology that is likely to fit a future solution very well.

4.5 Enhancement

The most surprising fact found was that none of the systems supported offline transactions. Given the found information regarding how tokenization works, it should be possible to create a solution that could support offline transactions by for instance have an option that let the user create a custom token that is valid until it has been used for a given sum. That would mean that the user would be able to spend up to that sum before internet access would be required again.

A suggest solution to the problem with relay attacks which has been mentioned would be to do a geographical comparison of where the POS terminal that is used is located, and compare that to where the smartphone connected to the credit card that is used is located. If the results of these two does not match up, the transaction should be aborted. Since the GPS data is not totally reliable when inside, some proximity margins would be required.

Another surprising fact is that the geographical spread is not larger. Since NFC is the most commonly used communication method in contactless payment, the cost of installing POS terminals is likely to be the case for the slow growth. With the entrance of MST the spread rate will hopefully increase. Having that said, it is also important to remember that in order for this kind of systems to work, a cooperation with the banks are required as well, hence MST will not solve all the problems, but it is certainly a step in the right direction.

Chapter 5

Conclusions and Future Work

The thesis handles the primary aspects of contactless payment systems that are used today. Each aspect is analyzed and put into perspective regarding several different scenarios. A presentation of the current state of contactless payment systems is shown in regard of different scenarios. Each element that is found important in a contactless payment system is discussed in order to determine in what extent the specific element matters, and why it matters.

The study has shown that the maturity of contactless payment systems has increased significantly in the last years. When the possibility to use a smartphone to conduct a contactless payment opened up, some large companies with high budgets became actors in the field, that is likely to be the most significant reason to why the development rate has increased.
However, the study has also shown that even though the field has grown a lot in popularity, and the user base is becoming larger and larger, the predicted amount of users has time and time again been higher than the actual values.

The field of contactless payment for smartphones is a new field in which there is still lots of work to be done. The largest gap that was found during this study is the lack of reliable statistics regarding almost all the aspects of contactless payments.
As mentioned in the thesis, it is surprising that none of three analyzed services supported offline payments. Hence it would be interesting to see work in the field of offline compatibility for contactless payment systems in order to find out what possible limitation there is, and if there are any security flaws that is not solved.
A final suggestion for future work is to thoroughly compare a SE solution to HCE regarding the security, usability and capability. The current information that is available differs in regard of which solution is best fitted for contactless payment systems.

References

[1] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering*, p. 38, ACM, 2014.

[2] "Apple Pay Adoption." <http://www.pymnts.com/apple-pay-adoption/>, June 2015.

[3] E. Haselsteiner and K. Breitfuß, "Security in near field communication (NFC)," *Workshop on RFID security*, pp. 12–14, 2006.

[4] M. Alattar and M. Achemlal, "Host-based card emulation: Development, security, and ecosystem impact analysis," in *2014 IEEE International Conference on High-Performance Computing and Communications (HPCC), 2014 IEEE 6th International Symposium on Cyberspace Safety and Security (CSS) and 2014 IEEE 11th International Conference on Embedded Software and Systems (ICESS), 20-22 Aug. 2014*, 2014 IEEE International Conference on High-Performance Computing and Communications (HPCC), 2014 IEEE 6th International Symposium on Cyberspace Safety and Security (CSS) and 2014 IEEE 11th International Conference on Embedded Software and Systems (ICESS), pp. 506–9, IEEE Computer Society, 2014.

[5] T. Zefferer, "A survey and analysis of NFC based payment solutions for smartphones," in *International Conference e-Society 2013, 13-16 March 2013*, International Conference e-Society 2013. Proceedings, pp. 275–82, IADIS Press, 2013.

[6] "Alliance Activites : Publications : Host Card Emulation 101 » Smart Card Alliance." <http://www.smartcardalliance.org/publications-host-card-emulation-101/>, Aug. 2014.

[7] M. Roland, "Software card emulation in NFC-enabled mobile phones: great advantage or security nightmare," *Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use*, pp. 1–6, 2012.

[8] M. Roland, J. Langer, and J. Scharinger, "Applying relay attacks to Google wallet," in *2013 5th International Workshop on Near Field Communication (NFC), 5 Feb. 2013*, Proceedings of the 2013 5th International Workshop on Near Field Communication (NFC), p. 6 pp., IEEE, 2013.

[9] V. Coskun, B. Ozdenizci, and K. Ok, "The Survey on Near Field Communication," *Sensors*, vol. 15, pp. 13348–405, June 2015.

[10] W. Anwar, D. Lindskog, P. Zavarsky, and R. Ruhl, "Redesigning secure element access control for NFC enabled Android smartphones using mobile trusted computing," in *Information Society (i-Society), 2013 International Conference on*, pp. 27–34, IEEE, 2013.

[11] G. Wallner, "System and method for a baseband nearfield magnetic stripe data transmitter," Aug. 26 2014. US Patent 8,814,046.

[12] E. Huang, W. W. Graylin, and G. Wallner, "METHODS, DEVICES, AND SYSTEMS FOR SECURE PROVISIONING, TRANSMISSION, AND AUTHENTICATION OF PAYMENT DATA," Dec. 24 2015. US Patent 20150371234.

[13] Samsung, "SAMSUNG to Acquire LoopPay, Transformative Digital Wallet Platform." <`https://news.samsung.com/us/2015/02/18/431-2/`>, Feb. 2015. Accessed: 2016-04-05.

[14] G. Wallner, "Stronger Security and Mobile Payments - Dramatically Faster and Cheaper to Implement." <`http://www.pymnts.com/wp-content/uploads/2014/03/Loop-MobileTokenization-final4.pdf`>, 2014.

[15] P. S. S. Council, "Tokenization Product Security Guidelines." <`https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf`>, Apr. 2015.

[16] "iOS Security Guide." <`https://www.apple.com/business/docs/iOS_Security_Guide.pdf`>, Sept. 2015.

[17] G. Chesler, A. Bakir, and M. d. l. Torriente, *Program the Internet of Things with Swift for iOS*. DE: Apress, 2016.

[18] Samsung, "Samsung Pay Will Transform the Mobile Wallet Experience." <`http://www.samsung.com/hk_en/business-images/insights/2015/Samsung_Pay_Will_Transform_the_Mobile_Wallet_Experience-0.pdf`>, 2015.

[19] M. Reveilhac and M. Pasquet, "Promising secure element alternatives for NFC technology," in *2009 First International Workshop on Near Field Communication - NFC '09, 24 Feb. 2009*, Proceedings 2009 First International Workshop on Near Field Communication - NFC '09, pp. 75–80, IEEE, 2009.

[20] S. Association, "smartSD - SD Association." <https://www.sdcard.org/developers/overview/ASSD/smartsd/>. Accessed: 2016-04-07.

[21] B. Ozdenizci, V. Coskun, K. Ok, and T. Karlidere, "A Secure Communication Model for HCE based NFC Services," Aug. 2015.

[22] P. S. S. Council, "PCI DSS Tokenization Guidelines." <https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf>, Aug. 2011.

[23] Samsung, "When I try to use Samsung Pay, I receive a "No network connection" error message.." <http://www.samsung.com/us/support/answer/ANS00045324/997424667/1>. Accessed: 2016-05-04.

[24] Google, "NFC payment flow - Android Pay Merchant Help." <https://support.google.com/androidpay/merchant/answer/6345242?hl=en>. Accessed: 2016-05-11.

[25] S. C. Alliance, "The what, who and why of contactless payments," *November*, vol. 3, p. 150, 2006.

[26] J. Vincent, V. Alimi, A. Plateaux, C. Gaber, and M. Pasquet, "A mobile payment evaluation based on a digital identity representation," in *2012 International Conference on Collaboration Technologies and Systems (CTS), 21-25 May 2012*, 2012 International Conference on Collaboration Technologies and Systems (CTS), pp. 410–18, IEEE, 2012.

[27] eMarketer, "2 Billion Consumers Worldwide to Get Smart(phones)." <http://www.emarketer.com/Article/2-Billion-Consumers-Worldwide-Smartphones-by-2016/1011694>. Accessed: 2016-03-31.

[28] Bloomberg, "Samsung Gunning for Apple in Race to Dominate Mobile Payments." <http://www.bloomberg.com/news/articles/2016-03-01/samsung-gunning-for-apple-in-race-to-dominate-mobile-payments>.

[29] A. Bodhani, "New ways to pay," *Engineering & Technology*, vol. 8, pp. 32–5, Aug. 2013.

[30] Samsung, "Which banks and credit cards are compatible with Samsung Pay?." <http://www.samsung.com/us/support/answer/ANS00043884/997408820/Y/>. Accessed: 2016-04-28.

[31] Samsung, "Samsung Pay Continues Global Momentum in 2016." <https://news.samsung.com/global/samsung-pay-continues-global-momentum-in-2016>. Accessed: 2016-04-28.

[32] Samsung, "Samsung Pay is Now Available in China with China Union Pay." <https://news.samsung.com/global/samsung-pay-is-now-available-in-china-with-china-union-pay>. Accessed: 2016-04-28.

[33] Google, "Android Pay - Supported Networks." <https://www.android.com/pay/supported-networks/>. Accessed: 2016-04-28.

[34] Apple, "Apple Pay participating banks and store cards." <https://support.apple.com/en-us/HT204916>. Accessed: 2016-04-28.

[35] Apple, "Apple Pay security and privacy overview." <https://support.apple.com/en-us/HT203027>. Accessed: 2016-05-02.

[36] Samsung, "Samsung Pay – Privacy Notice." <http://www.samsung.com/us/support/answer/ANS00045961/997435235>, Sept. 28 2015. Accessed: 2016-05-02.

[37] Google, "Privacy Notice." <https://payments.google.com/legaldocument?family=0.privacynotice>. Accessed: 2016-05-02.

[38] Google, "Payment Token Cryptography." <https://developers.google.com/android-pay/integration/gateway-processor-integration>. Accessed: 2016-04-05.