NTNU
Det skapende universitet

Design av NFC betalingstjenester og -system som bruker en TSM

Kristoffer Rene Eckhoff

Master i kommunikasjonsteknologi
Innlevert: Mars 2013
Hovedveileder: Rolv Bræk, ITEM

Norges teknisk-naturvitenskapelige universitet
Institutt for telematikk

0.1 Problem description

MCP solutions are seen as a possibility to make money by a lot of players. To mention some that are actively trying to succeed at MCP: Mobile Network Operators(MNOs), Point of sales(POS), mobile phone hardware producers, financial institutions, payment network owners(Visa, MasterCard, Paypal etc.), internet corporations(e.g. Google) and possibly a new kind of player: A TSM. Some of these actors have already tailored their own variants of mobile and NFC payment systems where most solutions requires users to have a certain subscription with a bank, a MNO or bank card issuer(Usually a regular bank).

There is a need to create a service that allows different actors to connect to each other, a TSM. This service shall coexist with existing payment systems and their owners(Visa/MasterCard etc.), while also keeping or even extending the necessary functional and non functional properties of existing payment systems such as for instance accessibility and availability, security, usability, interoperability and dependability like the traditional wallet and payment systems have. The authors of [11] states that that overcoming such technical requirements while still delivering value to the key players will speed up replication of NFC payment systems.

An open and interoperable platform needs to be developed. It must be possible for different financial institutions and other peers to easily connect to and exchange messages in the system, while at the same time a requirement should also be that users should have the possibility to choose for instance their own mobile phone type, phone number, carrier and bank. Such an open platform where different key players are able to connect to each other will drive a more rapid adoption of NFC payments technology [11]. This is where the TSM comes in as a neutral third part allowing flexibility and acting as a platform that connects different financial institutions, end users with different devices and subscriptions, and other players wanting to join the network.

NFC could also be used in other ways than money transactions for buying services or items at a POS: The technology has potential for being used as a key for your home, office or car and ticketing for festival/concerts, cinema movies and public transportation with a lot of different other everyday authorized access based uses imaginable. POS's could also add value added services offering commercial electronic offers, vouchers, loyalty programs or coupons. Loyalty and couponing solutions for the NFC technology has been discussed in a lot of papers (Some of them discussed and presented in the related works section). These value added services may be what is needed in order to succeed with mobile contactless payment(MCP) solutions and will be studied in this thesis.

Even though there is a lot of interesting work in academia now presenting and trying to solve business aspects for NFC solutions, this will not be covered in depth. However some business models, business relationships and other business aspects will be studied in order analyze the domain and gaining an understanding of the NFC payment ecosystem in order to propose a TSM design solution.

This work will provide insight into the current state of art of NFC payment technology with a thorough analysis and comparison of current payment services and systems within these solutions. With this background a proposed design that specifically takes interoperability and openness in mind will be proposed. But will also be based on findings in the following:

- Analysis of the current and proposed future systems used for payments that in works now.
- The business needs.
- Actors and their relationships in current proposed business models
- Compatability to the existing systems.
- Functional and non-functional requirements needed in order to function and perform as least as good as current payment systems
- Business factors that are necessary in order to succeed in building a system that is at least as effective and efficient for all stakeholders compared to current payment systems.
- And finally existing proposed standards and guidelines.

In short this thesis will look into existing payment systems and services and how these services work in terms of architecture, system requirements, design or other relevant system development models/descriptions needed in order to describe the service and system in terms of the engineering research domain. It will try to propose design models for a TSM in the NFC payment systems based on different current standards, recommendations and academic work and on services and systems engineering methodologies. The research domain for this thesis will be in services and systems engineering. The goal is to add value to existing work in creating a TSM system design by specifying technical open APIs, architecture and designs. The system and service designs are presented in the main part of the thesis report.

Sammendrag

Near field communication(NFC) betaling er en ny teknologi som går igjennom mange standardiseringsinnsatser for å finne en fungerende helhetlig løsning. Denne oppgaven vil studere eksisterende løsninger i betalingsindustrien og vil også se på fremtidige foreslåtte betalingsløsninger innenfor mobil betaling og mobil betaling ved bruk av NFC og en Trusted Service Manager(TSM).

Adopsjonsraten til betalinsløsninger som bruker NFC teknologi har til nå vært treg. Denne masteroppgaven tar et grunnlag i at dette grunnes mangelen på interoperabilitet mellom systemer. Hvordan en TSM kan bli designet for interoperabilitet skal derfor bli studert. I tillegg så er det nødvendig å lage et åpent system som kan ta til følge at brukere vil ønske å kunne skifte bank, mobiloperatør og mobiltelefon. Samtidig så må det være mulig for ulike bankinstitusjoner, mobile nettverksoperatører og andre aktører å delta i nettverket.

Det finnes lite relevant arbeid som viser design og systemløsninger i detaljer for en TSM. Denne masteroppgaven vil derfor prøve å finne løsninger for design av en TSM med grunnlag i foreslåtte standarder, foreslåtte retningslinjer og relevant arbeid.

Abstract

Near Field Communication(NFC) payments is a new technology trend that is going through large standardization efforts in order to find a holistic solution. This work will study existing solutions in the payment industry and will also look at suggested proposed future solutions for mobile payment using NFC and a Trusted Service Manager(TSM).

The adoption rate of payment solutions using NFC has been slow. This thesis makes the assumption that this is because there is lack of interoperable systems between systems. In addition it is necessary to create an open system where end users are able to change their bank brand, mobile network operator(MNO) and mobile phone. At the same time it must be possible for financial institutions, MNO's and other actors to partake in the network.

There exists little State of the art work that shows design and system solution in details for a TSM. This thesis will therefore try to find design models for an interoperable and open TSM in terms of system and service engineering and taking a basis in existing proposed standards, guidelines and relevant work.

Preface

There has for a long time in the technology world been a trend that we are going towards cardless payment solutions.

I for myself have for a long time wanted to pay with a mobile phone thus eliminating my wallet. Now it is possible to pay with your mobile phone on Trondheim's Atb buses by using Mobilett. But there are still some issues of usability in that this kind of payment will delay the buses [1]. If a contactless payment solution using NFC was created this delay could be avoided.

Almost every other day while working on the thesis, someone would forget their access card to access the office. The card was not put in the wallet, but instead left on the work desk. However we would always bring our wallet and our mobile phones while leaving the office for a short while. If the card was stored in the mobile phone instead this would never happen.

In addition the process of getting the actuall card involved contacting the secretary at the institute, when she was available she would then sign a paper, which then again had to be delivered to the janitor at the house which would write the access privileges to the card. There is no doubt that a working card issuance process where users could download access cards to their phone using their university credentials would be time saving for everyone involved in the process.

This work started out to create a service implementation targeting NFC mCoupons. But studying current works and projects there are a lot of works in progress on developing different NFC applications, see related work for a reference for some examples.

In recent years there are a lot of news articles in media stating that NFC payments will become a new payment technology. However despite the hype and anticipation of NFC and a lot of pilot projects, the contactless technology NFC has not been established as a de facto way to perform payments. This thesis takes a basis that there is a problem that needs to be solved around these applications, that is there is presumably a need to look into the technological solutions for these systems. Specifically this thesis will look at payment systems and services using TSMs in order to achieve interoperability and openness across multiple players in a new proposed payment network.

A lot of effort in this thesis has gone into getting a broad overview of the subject and also the associated research domain in order to build theory around the existing solutions that will be presented in this report. From this basis a design is developed. This report will therefore also heavily include how this design is deducted using Software and Service engineering design models and methodologies within this scientific domain.

This master thesis is to be submitted to be the Norwegian University of Science and Technology (NTNU) for partial fulfillment of the requirements for the degree of Master of Telematics

This project was performed at ITEM, NTNU, Trondheim in Norway, with Professor Rolv Bræk as responsible Professor from ITEM and supervisor Mr. Thomas Jelle from Trådløse Trondheim and ITEM.

The work performed in this report was solely performed by me but would not have been developed in the direction it did had it not been for the advice I got from advisors mentioned in the acknowledgement section.

Kristoffer Rene Eckhoff, NTNU

Acknowledgements

I first want to say my thanks to Professor Rolv Bræk at Institutt for Telematics(ITEM, NTNU) for assisting me in specifying the problem statement for the thesis work. I also want to thank Professor Bræk for assisting me in the final finishing of the report.

I want to thank you Thomas Jelle from Trådløse Trondheim(NTNU based company) for mentoring and supervising me. Specifically in guiding me on finding a thesis problem.

Thanks also go to Associate Professor Harald Øverby for our discussions around my thesis problem.

Finally I want to say thanks to Laurent for our short discussion and email exchanges around NFC technology and the thesis, and for managing parts of the project. It really encouraged me to focus and finalize my work in time.

I want to dedicate this work to my family and especially my mum who has always encouraged me to go for higher education.

Contents

List of Figures

Abbreviations

API	Application Programming Interface
CA	Controlling Authority
CCM	Card Content Management
EPC	European Payments Council
FeliCa	Felicity Card
GSM	Global System for Mobile Communications
GSMA	GSM Association
ITEM	Institutt for Telematikk
MCP	Mobile Contactless Payment
MCPA	Mobile Contactless Payment Application
MHz	Mega Hertz
MNO	Mobile Network Operator
NFC	Near Field Communication
NTNU	Norges Teknologiske og Naturvitenskapelige Univsersitet
OTA	Over the air
POS	Point of sale
RFID	Radio Frequency Identification
SD	Secure Digital
SD	Secure Domain
SE	Secure Element
SIM	Subscriber identity module
StoLPaN	Store Logistics and Payment with NFC

TSM	Trusted Service Manager
UICC	Universal Integrated Circuit Card

Chapter 1

Introduction

The society is heading towards a cashless world of payments, most payments today are performed by using credit or debit card that has replaced our traditional coins and bills. But now there is a trend that we are going towards wallet free solutions using a mobile wallet instead: With the increasing amount of always online smartphones and with the new Near field communication(NFC) technology that can enable Mobile Contactless Payment(MCP) and that comes with some newer phones, one can envision a future where we use our phones as a mobile wallet for money transactions, getting a bus ticket, for utilizing coupons or for replacing other cards/coupons and receipts in the traditional wallet. These payment solutions are seen by developers, mobile phone hardware producers, telecoms, banks as well as other players as a possibility to make money. This thesis will look into payments using NFC technology and especially a backend service that enables this service, a Trusted Service Manager(TSM) .

A lot of time in this project has gone to researching the current systems within the payment industry, and specifically look into payment solutions that exists in mobile payments using NFC and TSMs and its connected peers. Specifically a focus has been on the current proposed guidelines, current work and proposed standard work for NFC and a TSM that can be used for Mobile contactless payment(MCP). A TSM is a business contracter/connector service between a business, a consumer or another actor wanting to perform a NFC transaction. The main role of a TSM is to issue cards to an end user, e.g. for payment, loyality/couponing/offers, public transportation or any other card in the range of different cards available today. See figure 1.1 for a picture of the concept of downloading and storing cards in a phone instead keeping physical cards. The end user, the consumer, still pays with a card, but the card is virtually stored within a secure storage location called the Secure Element(SE).

While studying current work it became clear that there is a lack of concrete proposed holistic system and service design models for an interoperable and open TSM systems. See the related works and the state of the art section for references to some of this work. The NFC technology domain, and especially the concept of a TSM, is going through a research phase and specific standards for different requirements have not yet gained

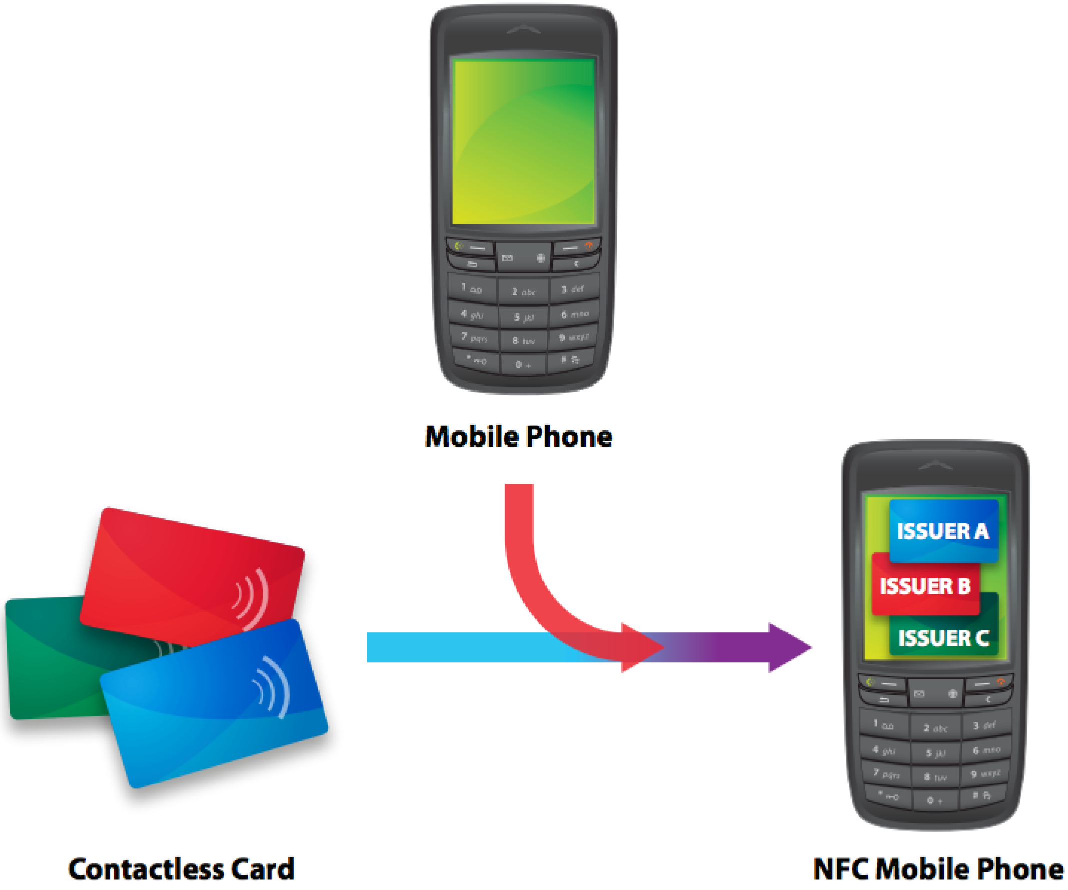


Figure 1.1: TSM concept adopted from [25]

dominance. There are however a lot of standardization works discussing business models and the NFC ecosystem, but few address and discuss the actual TSM creation by system development through design.

And although there exists several privately and governmental held live projects, these projects often do not reveal the design details and such systems will often also be proprietary systems. There is possibly a great potential for growth if one where to look into the best practices and proposed guidelines and try to build a report around how to build a TSM system that is interoperable and open for all vendors, thus also creating a common acceptance infrastructure for all operators. This thesis will try to understand and learn from the best practices and try to propose a design from these different systems and their offered service.

In addition Near field communication(NFC) payments has not yet had a mass adoption. Even if NFC technology has been anticipated for a long time to breakthrough as an adopted technology. NFC technology and NFC payments is in the Gartner's 2012 Hype Cycle graphed to be on a downwards trend in terms of expectations, see figure 1.2 for details. The NFC technology has matured a lot and is ready to be deployed in handset devices, however there is a need for infrastructure that can enable and help different industrial actors to cooperate in the competition. A common and available infrastructure could lead to more services being developed which could again lead to a higher adoption rate because service providers(SPs) could produce systems with cost and time efficiency through this reuse by using a service. There is possibly a great potential for growth if a common specification for a standard NFC TSM payment system is established as it can lead to interoperation between systems that again can lead to the customer having more services available. An assumption is that more services available for the customer will lead to more users, and therefore a TSM will enable growth.

1.1 Problem description

MCP solutions are seen as a possibility to make money by a lot of players. To mention some that are actively trying to succeed at MCP: Mobile Network Operators(MNOs), Point of sales(POS), mobile phone hardware producers, financial institutions, payment network owners(Visa, MasterCard, Paypal etc.), internet corporations(e.g. Google) and possibly a new kind of player: A TSM. Some of these actors have already tailored their own variants of mobile and NFC payment systems where most solutions requires users to have a certain subscription with a bank, a MNO or bank card issuer(Usually a regular bank).

There is a need to create a service that allows different actors to connect to each other, a TSM. This service shall coexist with existing payment systems and their owners(Visa/MasterCard etc.), while also keeping or even extending the necessary functional and non functional properties of existing payment systems such as for instance accessibility and availability, security, usability, interoperability and dependability like the traditional wallet and

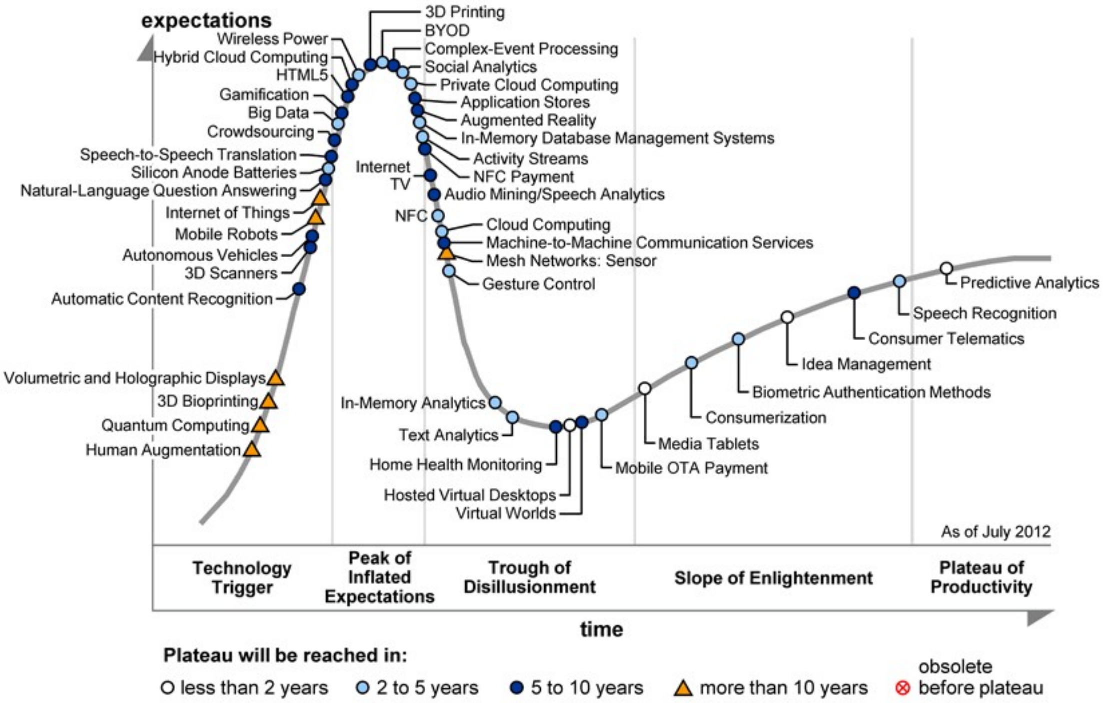


Figure 1.2: Gartner 2012 hype cycle

payment systems have. The authors of [11] states that that overcoming such technical requirements while still delivering value to the key players will speed up replication of NFC payment systems.

An open and interoperable platform needs to be developed. It must be possible for different financial institutions and other peers to easily connect to and exchange messages in the system, while at the same time a requirement should also be that users should have the possibility to choose for instance their own mobile phone type, phone number, carrier and bank. Such an open platform where different key players are able to connect to each other will drive a more rapid adoption of NFC payments technology [11]. This is where the TSM comes in as a neutral third part allowing flexibility and acting as a platform that connects different financial institutions, end users with different devices and subscriptions, and other players wanting to join the network.

NFC could also be used in other ways than money transactions for buying services or items at a POS: The technology has potential for being used as a key for your home, office or car and ticketing for festival/concerts, cinema movies and public transportation with a lot of different other everyday authorized access based uses imaginable. POS's could also add value added services offering commercial electronic offers, vouchers, loyalty programs or coupons. Loyalty and couponing solutions for the NFC technology has been discussed in a lot of papers (Some of them discussed and presented in the related works section). These value added services may be what is needed in order to succeed with mobile contactless payment(MCP) solutions and will be studied in this thesis.

Even though there is a lot of interesting work in academia now presenting and trying to solve business aspects for NFC solutions, this will not be covered in depth. However some business models, business relationships and other business aspects will be studied in order analyze the domain and gaining an understanding of the NFC payment ecosystem in order to propose a TSM design solution.

This work will provide insight into the current state of art of NFC payment technology with a thorough analysis and comparison of current payment services and systems within these solutions. With this background a proposed design that specifically takes interoperability and openness in mind will be proposed. But will also be based on findings in the following:

- Analysis of the current and proposed future systems used for payments that in works now.
- The business needs.
- Actors and their relationships in current proposed business models
- Compatability to the existing systems.
- Functional and non-functional requirements needed in order to function and perform as least as good as current payment systems
- Business factors that are necessary in order to succeed in building a system that is at least as effective and efficient for all stakeholders compared to current payment systems.
- And finally existing proposed standards and guidelines.

In short this thesis will look into existing payment systems and services and how these services work in terms of architecture, system requirements, design or other relevant system development models/descriptions needed in order to describe the service and system in terms of the engineering research domain. It will try to propose design models for a TSM in the NFC payment systems based on different current standards, recommendations and academic work and on services and systems engineering methodologies. The research domain for this thesis will be in services and systems engineering. The goal is to add value to existing work in creating a TSM system design by specifying technical open APIs, architecture and designs. The system and service designs are presented in the main part of the thesis report.

1.2 Hypothesis

It is possible to design an interoperable and open MCPA payment system by using a TSM and by taking a basis on current proposed standards, guidelines and academic/commercial work as well as system engineering methodologies.

1.3 Purpose of study

Existing commercial payment systems are slowly being extended by newer solutions by companies such as for instance financial institutions and MNOs. One hype that has been around is the extension to mobile payments, and now also MCPs using NFC technology. There is a lack of State of the Art work in this field of study, and Gartner 2012 states that NFC as a technology is going through a trough of disillusionment. There is not much academic work that addresses the creation or design of NFC payment systems. Most work, academic and other work, will address the surrounding business models or try to define the NFC ecosystem. The purpose of this study is therefore to find system and service designs, that is holistic models that can extend the current payment/transaction solutions and at the same time conforms to the standards/protocols of standardization bodies, recommended guidelines and other current work. In the end a goal is that this thesis could act as a guideline for vendors wanting to implement a TSM system.

1.4 Methodology

A system specification will be created based on literature for instance the information found on current TSM solutions and current or future MCP or other payment systems.

From the system specification we can generate a system design using system development methodology.

There are also some standards proposed by standardization bodies that gives guidelines and protocols for how to design the system and further interoperate with other systems. These standards and guidelines will be presented in the main part, and then further analysed.

The following approach is used

1.4.1 Approach

The approach for developing the design models involved four steps:

1. The first step was researching and gathering of existing TSM material and information from commercial, academic and standardization work. The goal was to put together a broad and representative sample of existing design and architectural models.

2. A background and terminology around what the technology is used for, goals, objectives, characteristics and key elements was built for the TSM domain.

3. Thirdly an examination and analyzation of the state of the art designs and architectures to better understand existing concepts was done. The goal for this step was to find best best practices and more knowledge about the design of a TSM.
4. Finally a development of a requirement specification and description and a TSM design including an abstract interface and a logical design of the system was created from the analyzation and then presented.

1.5 Research Questions

- In what ways can a TSM be designed using current proposed standards/protocols, guidelines and work in academia/commercial work(Best practices etc.)?
- What other NFC mobile contactless payment applications are proposed or are live today? How are they designed? How do they work? Are there something to learn from best-practices?
- What non-functional and functional requirements are required in order to build a TSM service providing properties at least as good as current payment systems? How can non-functional requirements be achieved in the system and service design?

1.6 Thesis Structure

The thesis is structured as follows

Chapter 1: Introduction

Chapter 2: Background

Chapter 2: Related work

Chapter 3: State of the art

Chapter 4: Main work

Chapter 5: Results

Chapter 6: Evaluation and Discussion of Results

Chapter 7: Conclusion

Appendix

Chapter 2

Background

Payment solutions and their services nowadays range from cash to Automatic teller machines, to Debit and credit cards and also online banking, but is now presumably going towards also including a new cashless solution where NFC technology is used to enable payments.

This background chapter will outline on how some of the current payment system and the future MCP systems using NFC are connected in terms of actor/stakeholder relationships.

In addition this chapter will outline the current NFC technology and introduce current NFC Trusted Service Management(TSM) solutions.

A section defining some terms and building terminology will be presented. A short version of these terms can also be found in the glossary.

Finally a section of a Service Manager design pattern is presented.

Some of these sections may present well-known facts for the reader. However this chapter will in addition to introducing a background for the reader try to build some terminology and history of payments in order to clearly have definitions and anchor points to build upon later.

2.1 The current payment systems

Most adults of today have used an ATM where we as users insert a card, give the ATM our credentials and can then withdraw money from our bank accounts. These machines save money indirectly to banks by lowering queues and personnel required to give access to teller transactions and nowadays some ATMs are also extended to provide other automatic services.

However nowadays most transactions are done electronically using only a credit or debit card instead of ATMs. This means of payment has existed since the early 80s and is the

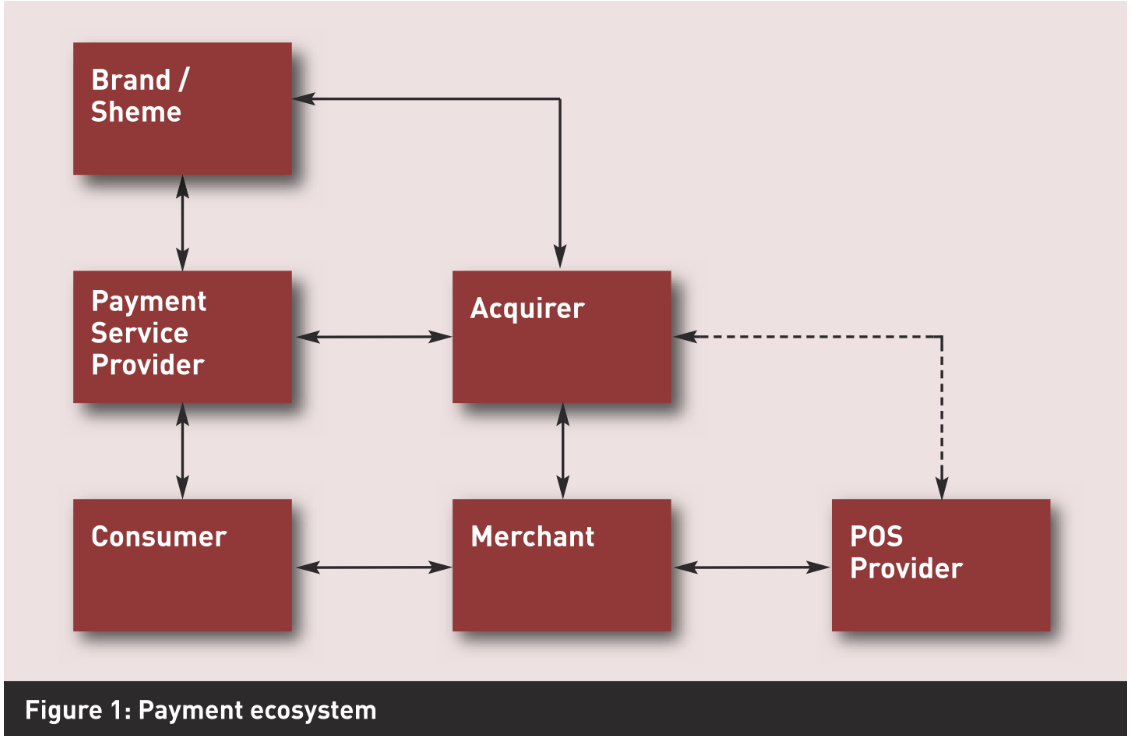


Figure 2.1: Traditional payment ecosystem adopted from [24]

most widely adopted paying medium. Where the card in some process is connected via the POS to perform transaction in the customers' bank account. This kind of payment where the user uses a physical plastic card will be referred to as the current or traditional payment system in this thesis.

See figure 2.1 for a graph of the relationships in the traditional ecosystem, that is how the ecosystem is operating today without a TSM. The brand/scheme in this figure will be payment networks such as Visa and MasterCard while the payment service provider will be the users bank.

In [12] the author Avila identifies and analyses different current and possible future payment systems. Avila identifies 3 different current payment systems used for debit and credit cards. Where mainly a payment network is in the core of these systems. These different system types are referred to as n-party systems. Where the number n, refers to the number of actors participating in the system. In Avila's descriptions the brand/scheme and the POS provider are left out of the description, as they are not part of the payment process but a process that happens before the actual payment:

1. User goes to the bank to get a credit or debit card.
2. The bank orders a bank smart card from the brand/scheme or other manufacturer.
3. The card is sent to the User through mail.

Two-party payment systems

Functionality: “A POS issues a card that gives credit to the customer. The POS controls the credit and is the only part that the customer relates to” [12]

This is identified by Avila as how the initial credit and debit cards was created, but it can also be found in some stores today as gift vouchers and vouchers for exchanged wares

Actors:

- Customer
- POS/Merchant

Commercial relationship: Customer <–> POS(Merchant)

Three-party payment systems

Avila states that this is how the credit card brands “American Express” and “Discover” works. “American Express” or “Discover” will issue a payment card, and will then operate a network for payments. An example shown in [12] is:

Functionality:

1. A customer delivers his or hers card to a POS
2. The POS sends transaction data to the card issuer(For instance AmEx or Discover)
3. The card issuer accepts or rejects the transaction in a response message to the POS.

Actors:

- Customer
- POS
- Card issuer/Payment network

Commercial relationship:

Customer <–> POS <–> Card issuer/Payment network

Avila also calls this a closed loop payment network, which means that the card issuer owns the network and offers payment service directly to the POS and the cardholder.

Four-party payment systems

To give comparison Avila states that this is the system that the debit card brands Visa, MasterCard and Star uses. This system is defined by Avila as an open loop payment network. Where an open loop is consisting of “multipart" institutions in order to perform transactions between two parts [12], usually an end user and a POS. The four-party payment system will "usually not have a network operator issuing cards" [12], but instead banks or other financial institutions will issue cards used for payments.

Functionality:

1. A customer uses his card to perform a purchase at a POS.
2. The POS sends transaction data to its own bank or other financial institution/Acquirer
3. The POS financial institution asks the payment network for the customers bank information.
4. The network operator validates the transaction and submits it to the cardholders financial institution/Payment Service Provider(Usually a bank)
5. Cardholders i.e. the customers financial institution accepts or rejects the transaction.
6. The operator sends the accept/reject back to the POS bank.
7. The POS bank sends an accept/reject of the transaction to the POS.
8. The POS terminal receives the accept/reject, displays a message and prints a receipt for the transaction.

Actors:

- Customer
- POS
- POS' Bank/Financial institution of POS
- Customer's bank

Commercial relationship:

Customer <–> POS <–> POS Bank/Financial institution <–> Customer bank

2.2 NFC MCP Payments

2.2.1 NFC Technology introduction

NFC is an emerging technology that is currently going through "many standardization efforts and tries to find a suitable ecosystem." [16] Most of the device technology is already standardized and developed. And NFC technology is already being distributed to POS's, mobile phone owners and other early adopters. This section will introduce how

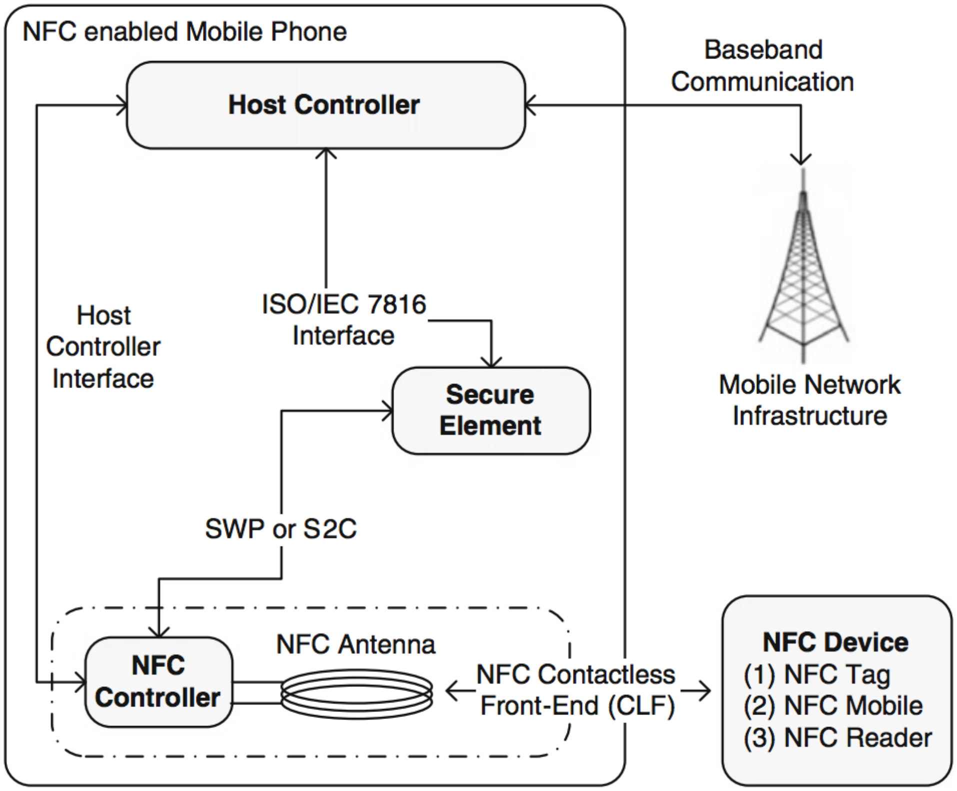


Figure 2.2: NFC mobile phone device architecture with SE adopted from [43]

these different functionalities within the NFC chip works as well as introducing other established technology standards and implementations as well as giving an introduction to NFC terminology.

The NFC technology is based upon the ISO 14443 RFID [35] technology with added protocols, NFC protocols, to enable communication to other NFC devices. The technology is designed to operate in short distances, approximately up to 10 cm with the low range frequency of 13.56 MHz. In addition the technology has evolved to also include a range of different modes: Peer to peer exchange of data using NFC pairing, NFC card emulation and NFC reading or writing. These different modes are defined by standards and also implemented by some vendors. NFC has with the different modes a potential for a lot of uses. One trend is NFC payments where a user is identified by using credentials and an application, a Mobile Contactless Payment Application, within a secure element(SE) stored inside the NFC device.

A figure of the NFC technology architecture can be found for reference in figure 2.2. The architecture modules will be presented in the following sections. But first active and passive NFC devices will be defined.

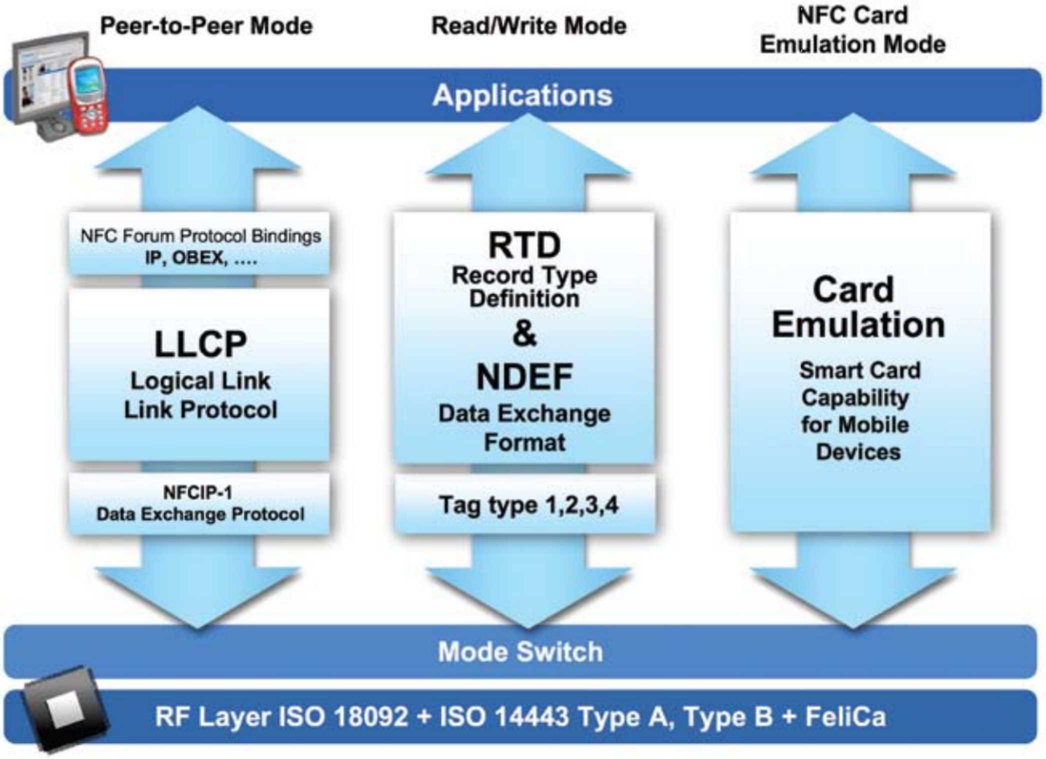

Peer-to-Peer Mode
Read/Write Mode
NFC Card Emulation Mode
Applications
NFC Forum Protocol Bindings IP, OBEX, ...
LLCP Logical Link Link Protocol
NFCIP-1 Data Exchange Protocol
RTD Record Type Definition & NDEF Data Exchange Format
Tag type 1,2,3,4
Card Emulation Smart Card Capability for Mobile Devices
Mode Switch
RF Layer ISO 18092 + ISO 14443 Type A, Type B + FeliCa

Figure 2.3: NFC modes adopted from [5]

Active and passive devices

An active device is defined to be an iniator device capable of communicating without any other iniator, that is an active device will create and communicate their own generated signals. The active devices will have their own battery or other power source to communicate with other NFC devices. An active device can iniate communication with both an active and passive NFC device.

A passive device will be controlled by an active device and will then act as a responder. The passive device will take read/write or other instructions from the active device and perform them. An example of a passive device is the NFC tag described in the NFC read/write mode section below. A passive device can in conclusion only be activated by initiation from an active device and cannot communicate with other passive devices.

NFC secure element(SE)

Most active NFC technology chips are now including the newly standardized secure element(SE) allowing secure use of credentials in order to authenticate users at point of sales or other NFC endpoints.

The SE is used to store application credentials, virtual smart cards/mobile contactless payment applications(MCPA) and other sensitive data in a secure storage. The level of security is at least as high as in smart cards [43]. In smartphones SE is integrated into the mobile phone and cannot be removed [43], see figure 2.2 for a figure showing how the SE is combined with the rest of the NFC architecture.

In a mobile phone NFC device the phone manufacturer will be the provider of the secure element, or in NFC terminology will be the SE issuer. But the secure element could also come in other forms, for instance in a active NFC tag, stored in the SIM card/UUIC, embedded in a SD card or as a module in the battery to mention some different forms of SE. The manufacturer of the SE will in any case be the SE issuer holding keys for the secure storage. More on SE issuer can be found in the NFC ecosystem actors section below.

The following three sections will present different NFC Modes. Some applications that will use these different modes are referenced in the related works section. See figure 2.3 for an overview of the different modes.

NFC peer-to-peer mode (ISO 18092)

Putting two active devices together can activate this mode. The two active devices are then linked together and can exchange data or communicate other instructions/operations using NFC protocolls. Data Exchange Format(NDEF) is used to transfer the data. An example of one such service could be a dating app where the user gets an instant percent metric for how well they match. Or just plane file transfer, for instance sharing of pictures or other media.

This mode could be used for NFC payments if the payment terminal and the active NFC device communicates with a protocol to exchange information needed in order to perform the payment. The terminal then proceeds to send the data as in a n-party payment model. The payment terminal will however be required to differentiate between normal smart cards and a MCPA.

Figure: NFC DEVICE <–> NFC DEVICE

NFC card emulation mode (ISO 14443)

In this mode the mobile handset will emulate a smart card. An external reader(Active NFC device) can then not distinguish between a physical and the virtual emulated card [26]. This mode can be used for MCP and ticketing [26] where the user would use a virtual card stored inside the SE instead of a traditional plastic card.

Figure: NFC DEVICE EMULATING CARD <– INTERACTION POINT CONTAINING ACTIVE NFC DEVICE

NFC read/write mode

In this mode an NFC reader, for instance a NFC enabled mobile smartphone, will induce power into a passive NFC device. The smartphone, or another other compliant NFC device inducing power to the batteryless passive tag, can then read/write and also lock the NFC tag for alteration. Depending on the data structure the NFC device then takes the action and performs it without user interaction, except for the user's initial interaction with the tag. Such NFC devices, also commonly referred to as NFC tags, could be included in coupons/vouchers and as tags in posters/magazines enabling the user to store offers and deals electronically on their phones When the users touches the tag, the tag could for instance contain an URL that opens in a browser or a code for any other smartphone app action like for instance calling a phone number stored within the tag.

Figure: NFC DEVICE –> TAG

Two-part application

NFC payments or other NFC applications can on the device be divided into two parts: One to be stored on the SE and one to be stored in the phone operating system. This means that the server may need to handle two applications types. [25] introduces and defines the two parts and some terms for describing them. For an overview of functionalities contained within these applications see 4.3

- Application Execution Environment(AEE): An actual software application running on a NFC device. This could for instance be an app store like application where users could download a lot of different NFC applications in order to activate electronical smart cards and utilize value added services, such as for instance how [10] and [2] operate. Or it could be vendor specific applications utilizing a TEE.
- Trusted Execution Environment (TEE): A SE application where secure applications such as payment applications can run.

2.2.2 Value added services

As later shown in the related works there are some services that can be added on top of the MCP payment as a service.

- Loyalty programs.
- Coupons/Vouchers.

Certified developers could also be enabled to connect to a TSM to create other services/applications. This will require an open API, but should not compromise the SE.

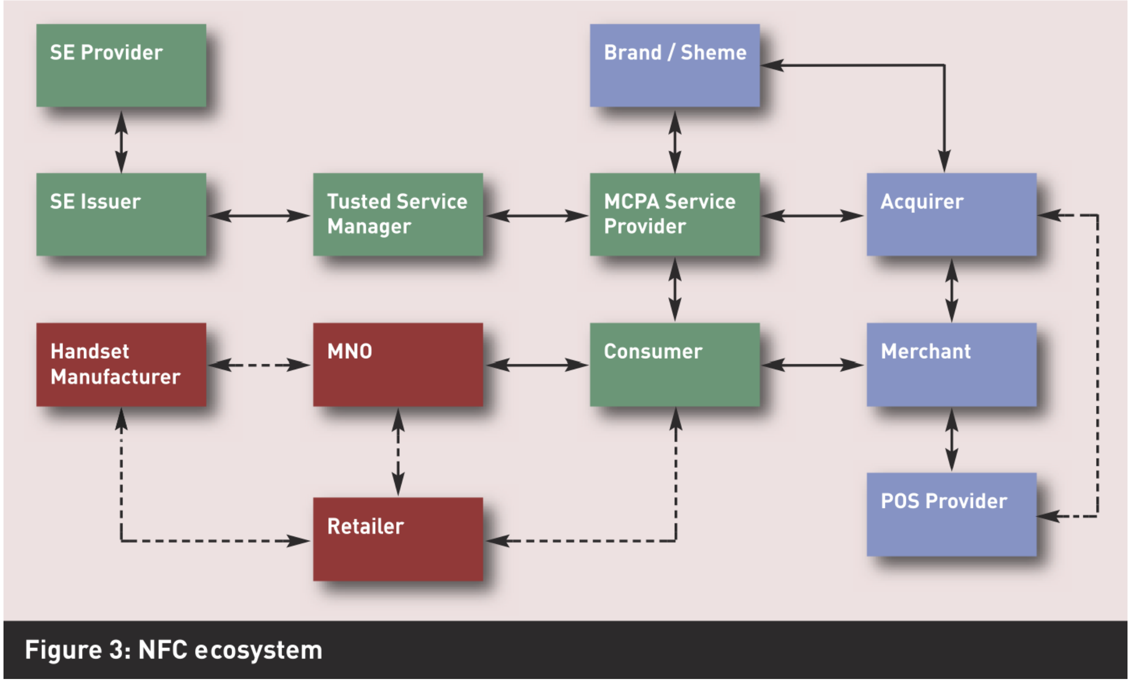


Figure 2.4: NFC payment ecosystem adopted from [24]

2.2.3 Actors and relationships

In literature the environment in which NFC payments could be realized is called the NFC payment ecosystem. The systems consist of actors or certain stakeholders that are considered to be partaking in a future payment ecosystem.

The stakeholders are mostly adopted from [24] [40].

See figure 2.4 for an overview of how the actors are related. The red colors in the figure show the mobile phone side, where the Consumer, the end User, could either acquire a mobile phone from a MNO or a retailer. The green colors shows the addition needed in order to establish an ecosystem where a TSM is used. And the blue colors show the actors in the traditional ecosystem as depicted in figure 2.1.

Trusted service manager(TSM)

In recent years a new service has been proposed by numerous organizations: For instance NFC forum, StolPaN and Global Platform are all working to define a payment service infrastructure called a Trusted Service Manager(TSM). The TSM is a third party in a payment ecosystem and delivers payment-, loyality- and voucher- card manufacturing services to users and banks. The service that will be discussed most in this thesis is where the user downloads and personalizes a card. That is the User requests a card from the bank/MCPA SP, and then the card is downloaded with the users personalized information and stored in the MCPA. To give an analogy, the card manufacturer would also personalize a card by printing the card number on a physicall card. More technically described the main role of the TSM is to manage the different MCPA lifecycle functionalities. The downloading and personalization of the MCPA described above are part of the lifecycle functionalities. These functionalities are presented in the State of the Art from different works. In addition a sorted functionality list of a TSM including the lifecycle functionalities are included and presented in the main part.

[40] splits the TSM's role into two roles: A TSM role for the MCPA SP and a TSM role for the User. The TSM's MCPA SP roles are most importantly to manage the MCPA SP's applications. While the TSM's User roles are mainly to manage the lifecycle of the application within the Users device. Whether or not the SP should handle User requests(e.g. request for registration of a MCPA) or the TSM should do it directly depends on the SP's needs. In some cases the SP may want to use a TSM but handle parts of Card management itself. For instance at least be the User's point of interaction for these services. In other cases the whole process could also be taken care of by contacting a TSM directly. In either case the TSM would have a MCPA Lifecycle process. [25] also adds that the TSM needs to communicate with the SE issuer because the SE issuer will hold the keys needed to install the SE. More on SE issuer can be found below.

A TSM could also be useful for adding value added services, discussed previously in this chapter, that are considered as a possibility with MCP solutions to add business value for the POS [40]. The cards are then produced with different personalization data. But would still be virtual contactless cards.

More about the TSM will be presented throughout the report. A short description can also be found in the glossary.

Consumer/Customer/End User

This is the end user which holds a NFC device. Usually the user would own a plastic card, but a virtual card stored in the SE within the NFC device replaces this. With this virtual card a user could perform payments, pay for ticketing or gain access to their office, to start their car or other access based services

In an ideal NFC environment the system should be open so that a user is able to download any certified NFC application to their secure element in their NFC device. The user should also be able to change brand and bank, change mobile phone and mobile service provider [40]

[40] also remarks that the user is central because the user will always be the originator of the request being partaken by ubiquitus touch interaction and that this is important to avoid unsolicited pushed service offerings.

MCPA Service provider

Issues the MCPA application to the consumers wanting to use a NFC application [24]. This is typically a bank or could for instance a public transport service that issues a card or any other organization that would issue a smartcard.

A bank will also be contacted when the user is using the MCPA for payments as described in the four-party payment model.

Acquirer

"The acquirer is responsible for handling financial acquisitions in payment ecosystems. It will initiate the clearing and settlement of payment transactions through payment schemes and banks." [24]

Point of sale(POS)

The part selling a service or some kind of goods to the consumer. This is the point of interaction for the consumer, where he or she would usually use a credit or debit card, but would instead in the NFC payment scenario use the NFC device to initiate and then perform a payment. [24].

POS provider

Provides the POS with NFC enabled payment technology such as NFC terminals [24].

ISO/IEC 14443 type A and B standard, can function as NFC terminals in public transport [27]

Handset manufacturer

The handset manufacturer manufactures and sells NFC enabled devices. This will often also include adding a SE in the manufacture process [24].

MNO

The MNO can be the provider of the underlying network for TSM to issue MCPA's [24]. In a scenario where the a MCPA uses the UICC/SIM card as SE the MNO will have a stronger role in the ecosystem because it will be SE issuer.

Retailer

This is the seller of the handset devices. Keep in mind that this could also be the MNO [24].

SE issuer

The SE issuer provides a Secure Domain(SD) and keys to the user's SE inside the NFC device. The SE issuer could for instance be SE provider: the Handset Manufacturer or the MNO. Or in another thought out scenario the SE provider could also outsource the SE issuance role to a third party, for instance a TSM. This scenario would however require the TSM to have the access right to create SD and keys. In any case, whether the TSM acts as an SE issuer, or the SE provider remains the SE issuer the SE issuer manages Secure Domains and SD keys. The application is stored within the SD so that only the keyholder can use the application. [24].

Developers

Parts of the TSM or SP services could also be available for certified developers as long as it does not compromise the SE. Developers could connect through an API to be able to create new innovative services. For instance developers could request their own security domains to store applications.

OTA provider

The OTA process is to manage the SE securely and remotely over the air(OTA). That is to perform the lifecycle processes securely and remotely. An OTA provider is the service holder performing this process. This process is transparent to the actual implementation [40]. In other words handling OTA just means to handle the remote upload and download of MCPA applications to the SE securely. The OTA process could be performed by the TSM or the MCPA SP.

Brand/Scheme

The brand or scheme holds the existing underlying payment network, and "is responsible for handling agreements with scheme participants, setting fees and establishing technical, functional, branding and certification policies for scheme participants." [24]. Visa is a good example of this. Banks will usually issue cards using the Visa (or another brand/scheme) and then the underlying Brand/scheme payment network will be used when payments are perfomed. The brand/scheme has to cooperate with the MCPA SE in order to create a MCPA to be stored in the SE. Most likely the cards will be of a format that can be reused by multiple Brands. So the TSM could offer standard cards, and then get personalization information from the MCPA SE.

It should be remarked that the brand/scheme owners would most likely require the branding logo to be shown in the AEE in the same way credit and debit cards are branded with a logo.

2.3 Google wallet example

Google wallet is an SP that utilises a TSM in order to add cards to its wallet. This example is therefore presented here in order help giving understanding of the involved functionality.

The initial version of Google's "Google Wallet" was launched in May 2011. With the release of this "App" they also released a smartphone with added built in NFC technology: The "Nexus S". And Google added support for NFC chips and operation in the Android Operating system. Later the added Android operating system support has been adopted among others by Samsung and their "Samsung Galaxy S3" smartphone. In order to provide Google wallet Google has partnered with Citi Bank to provide specific bankcards and they also offer a Google prepaid card that can be loaded into the users phone in order for the user to perform payments. Google has also partnered with MasterCard PayPass with their technology as a payment network provider. Google also uses a TSM service called First Data where Google acts as a MCPA SP. First Data provides over the air provisioning of payment card credentials to Google wallet. Thus Google wallet adopt the existing payment system in their solution by letting user add their current cards and banking credentials to use for payments.

When Google uses their TSM from First Data users can download and personalize different cards provided by the TSM. The download and personalization process has to be performed before a "consumer can buy something with his or her phone, the device must be "personalized" with appropriate payment application and account information. In some ways, this is similar to the process of personalizing or provisioning a plastic credit or debit card." [20]. The TSM manages the download and personalization process as well as other MCPA application lifecycles processes and then replaces the traditional physical Card manufacturer. While the MNO's mobile network or Internet replaces the traditional means of delivering the card through a postal service or by collecting it at your bank. More on this actuall process will be presented in the main part as these processes are the main focus in this report.

In August 2012 Google released a new version of its Google wallet popularly referenced as Google Wallet 2.0 that extends the functionality of Google Wallet 1.0. In this version Google states that any credit card can be added to the secure element. They do this by preloading a PayPass MasterCard inside the secure element that is used to forward the payments performed by this electronical wallet. The PayPass card is connected to the

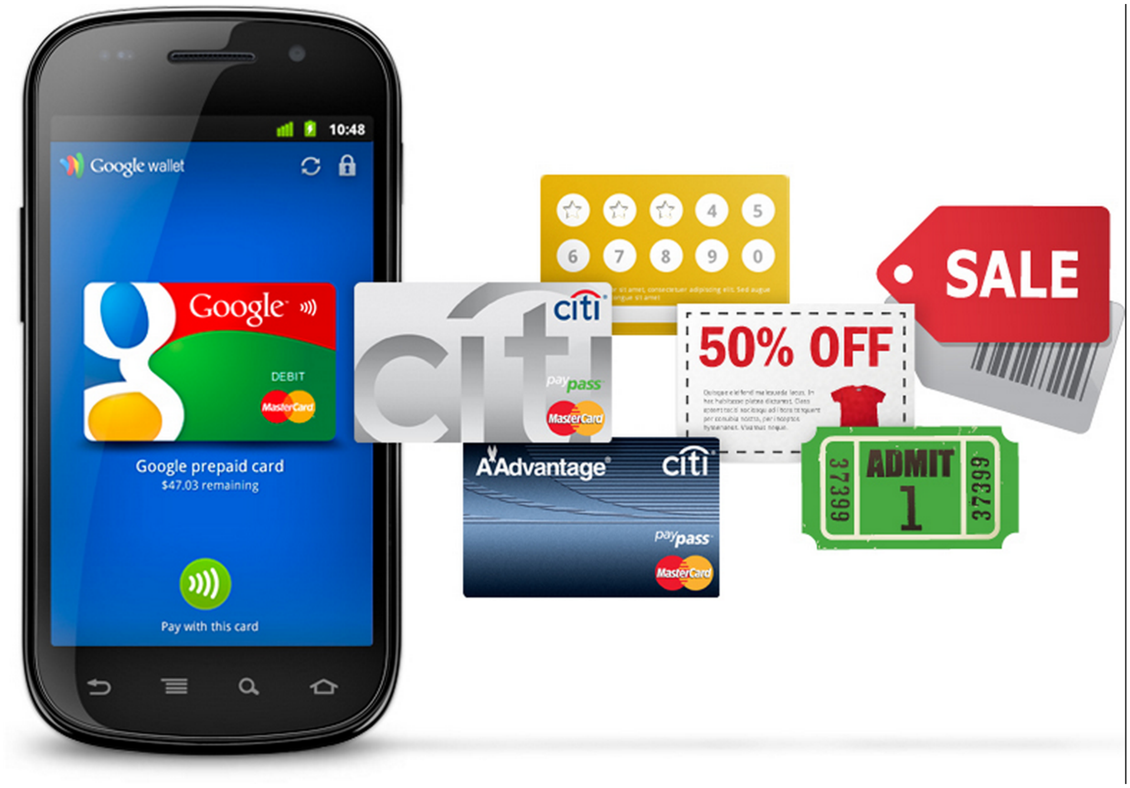


Figure 2.5: Google wallet vision from [34]

MasterCard payment network, which is widely accepted throughout the world.

Whenever a user wants to perform a payment with his or hers personal credit or debit card loaded into Google Wallet 2.0 it will go through the preloaded MasterCard card with the following procedure:

1. A card is preloaded in the secure element from MasterCard(credit card), while the actual virtual card used is stored on Google servers(After an end user adds it).
2. MasterCard performs the payment with the preloaded MasterCard in the payment network as if it was the Customer in the four-party payment model.
3. MasterCard then proceed to deduct the amount from the users card.
4. When the users looks at his or hers transaction records the payment will state “Google” in the beginning of the transaction and then the POS name. For instance “Google* Sony Store”.

Google also plans on extending payments with value added services such as couponing and loyalty programs as described in the background section.

See figure 2.5 for an overview of Google’s vision of the the future wallet.

2.4 Short notice on parallels to the telecom industry

A TSM can in a lot of ways be compared to the way the telecom industry has worked through history. It is a requirement that any phone can call any other phone, no matter where you are in the world. Standardized interfaces are used to enable this interoperability. In the same way most payment cards today can be used to pay anywhere in the world with the added flexibility that comes with collaboration.

[40] also gives this analogy and is adding that an environment in which the NFC community acts as one will improve NFC business conditions dramatically. This can be achieved through a common standardized TSM.

2.5 Relevant terminology definitions

Some of vocabulary definitions and abbreviations will be presented throughout the text and are also listed respectively in the glossary and the abbreviation list. But in order to present a clear thesis the definitions of interoperability, openness and open systems will be presented here.

2.5.1 Interoperability

The IEEE Standard Glossary [6] definition of interoperability: “Ability of a system or a product to work with other systems or products without special effort on the part of the customer. Interoperability is made possible by the implementation of standards.”

While the IEEE Standard Glossary of Software Engineering Terminology [13] defines interoperability to be: “The ability of two or more systems or components to exchange information and to use the information that has been exchanged” The glossary also refers to compatability when looking up interoperability. Where compatability is defined to be: “(1)The ability of two or more systems or components to perform their required functions while sharing the same hardware or software environment. (2) The ability of two or more systems or components to exchange information.”

[32] which discusses technical architecture aspects defines interoperability to be: “Building blocks from different vendors should be allowed. This ensures that each building block has predictable, well-defined behavior”.

These definitions define interoperability to be the ability to work with other systems, across vendors. The IEEE Standard Glossary of Software Engineering Terminology definition is however more specific in terms of system and service engineering and will mainly be the definition to be used when referring to interoperability in this thesis. But the definition from [32] is also relevant.

Finally it will be added that interoperability in telecom is the ability of systems to work together and this is what is wished to be investigated in this thesis work.

There exists a lot of work seeking to make NFC technology interoperable, that is that it should for instance work with Smart card standards, as well as function across different NFC devices. This thesis will not focus on NFC device interoperability, but on how an interoperable TSM can be created with the multiple services/systems and NFC devices it needs to work with.

2.5.2 Openness/Open system

The IEEE Standards Glossary [6] definition of openness is as follows: "Participation in the standard development process shall be open to all persons who are directly and materially affected by the activity in question, and the committee's activities are publicly available."

In [28] openness is defined to be "Openness is a measure of the extent to which a system comprises components that are built to Open Standards. The Openness of a system can then be defined by the extent to which the components from which it is built implement Open Standards."

While [28] defines an open system to be: "An Open System is a modular construction where the components are built to Open Standards. The standards will normally be the responsibility of Standards Bodies or otherwise be publicly available."

[32] defines openness in a technical architecture to be: "The network must be open and able to support appropriate principles of competition" in terms of network requirements.

In [19] openness is defined to be achievable for a system by "adding emphasis on connectivity" meaning that the system should be connectable for different actors wanting to use the system's functionality or have access to data in the system.

In [18] it is stated that negotiation is a fundamentally important mode for open systems. An example for why this is important, which is also an example that can relate to TSM infrastructure and a negotiation protocol is: "For example each bank will offer similar services that will differ in detail from the services of its competitors. [These bank] systems will need to negotiate the terms and conditions of their transactions." [18] This means that the systems need a common language in order to communicate the negotiation [18].

In addition the following definition from [3] will be used: "Vendor-independent, non-proprietary, computer system or device design based on [. . .] standards. It allows all vendors (in competition with one another) to create add-on products that increase a system's (or device's) flexibility, functionality, interoperability, potential use, and useful life. And enables the users to customize and extend a system's (or device's) capabilities to suit individual requirements."

This thesis will therefore use the definition that an open system is a system that has some extent of measurable openness, is a system that follows open standards, and is open to all actors or stakeholders that are directly or materially affected by the system to access required functions or data.

From the definitions defined above for openness/open systems and interoperability it can be said that open standard specifications is created in order to get interoperable systems and open standard specifications are used to build open systems.

Chapter 3

Related Work

This chapter will shortly outline some academic work and current projects that are related to NFC technology.

3.1 Survey on mobile commerce(M-Commerce) academic work and pilot/live projects

A commonality for these services are that they build their solution from the ground up where they could have used a TSM to provide management of NFC related services like couponing/ticketing, access to an office, a home or to start a car or another service or application based on contactless authorization using the secure element in the NFC chip.

There exists too many examples to list them all here. But it shows that there is already established academic work and some working examples of live projects using the mobile as a wallet.

3.1.1 mCoupons: An Application for Near Field Communication(NFC) [22]

This paper is discussing distribution of electronic coupons in traditional mediums like newspapers and posters with a NFC chip inside the paper. When a user touches the tag with his or hers NFC device a link or application is activated. It also is discussing security around electronic coupons.

3.1.2 Paper Ticketing vs. Electronic Ticketing Based on Off-Line System 'Tapango' [35]

This article presents a partial solution that bases itself on a user carrying a NFC chip for instance in a bracelet/card etc. The user or a POS/ATM can write and/or read the chip to exchange services or sales. This could for instance be used for ticketing on a concert where a user wears a bracelet as a means to access the festival.

3.1.3 Mobile sales assistant [37]

Discusses NFC tagging of articles in a store, for instance tagging of clothes in a clothing store. The idea they give is to replace the traditional barcode with NFC tags, which also extend the traditional usage with for instance scanning a tag to get availability and stock information.

3.1.4 Do you talk to each poster? Security and Privacy for Interactions with Web Service by means of Contact Free Tag Readings [39]

This article discusses the interaction between physical tagged objects(Like posters with a NFC tag inside like mentioned earlier) and a Web service backend. This article also states that NFC based applications are on their way from the technology research stage and going towards the system development phase.

3.1.5 Near field communication network services [44]

Presents a general solution for implementing a backend NFC service for instance to be used with a NFC terminal and NFC chips. In future work they mention a creation of a standard service language for different service aspect within the NFC ecosystem. For network based communication services this paper also suggest using a lightweight binary protocol in order to save CPU and memory on the user device. The paper also states that there is a lack of "operator scale NFC service creation and delivery".

3.1.6 From Implicit to touching interaction: RFID and NFC approaches [15]

This paper discusses ambient intelligence and ubiquitous computing. The article gives an example where NFC tags/readers are distributed at different locations in our daily life. For instance the user carries a tag that can identify the user or the user carries a reader in the mobile phone. Some examples given are that a user uses NFC technology to gain access to the office and where a user uses a NFC device to control a PC using a “tagging board”

3.1.7 Identity Verification Schemes for Public Transport Ticketing with NFC phones [41]

Discusses and proposes security and performance within NFC technology specifically targeted for a public transport service solution.

3.1.8 An NFC-Based Solution for Discount and Loyalty Mobile Coupons [38]

Describes a solution where mobile coupons are used using NFC technology and a backend service. This paper also describes loyalty programs and discounting to add value to the user.

3.1.9 Near field communication-based secure mobile payment service [33]

Describes a NFC payment service where the focus is on security.

3.1.10 Offline NFC Payments with Electronic Vouchers [42]

In addition to discussing NFC vouchers this paper concludes that it is possible to create a offline version of a NFC payment service without compromise to security, but that it is difficult in regards to limitations in todays CPUs, memory sizes and security functionalities.

3.1.11 Remittance services

In some undeveloped countries people do not use banks but instead utilize mobile phone credit as a mean for payment. An example is how the Orange telecom provides remitance services with their service Transfert [9]. International interoperability is therefore naturally required also for a NFC payment service.

3.1.12 Singapore example

In Singapore the 3 biggest telecoms has together with the government, banks and the public transportation system created a national NFC service that users can utilize for public transportation or for payments [4].

3.1.13 Japan example

“In Japan, it was effective for one trusted third party to lead the whole NFC Mobile Ecosystem in the early stage of business development.” [25]

3.1.14 Mobile and online banking

Norwegian banks are introducing mobile versions of their net banks, following the online banking trend, naturally calling it mobile banking. Most big Norwegian banks have at least an Android and iPhone Mobile bank App. These applications could with a bank being a MCPA SP and using a TSM as a backend also extend these Apps to also include functionality where users could download their credit or debit card. Such an App can be called an AEE Application, whereas when the users download the credit or debit card it is downloaded to the TEE and physically stored in the SE.

At the same time the banks are improving their current online bank services by introducing users an overview of their result(personal finances terminology). One example is how Sparebank 1 has created a Business Intelligence like dashboard showing the results of the last month when the user enters his/hers online bank. The user can then the next month set a budget in order to get an alert when he or she goes over a certain limit making personal finances more easier.

Chapter 4

State of the Art

Some new payment systems using a TSM system have already emerged or are being defined by standardization bodies. These systems will be presented here in detail in terms of system and service engineering to show current knowledge and development. A commonality for a lot of these frameworks is that they strive to eliminate functionalities of the physical wallet.

This survey shows that different standard bodies or organizations are working on specifying a TSM.

4.1 StolPan proposal

The StoLPaN organization is an organization that is by their own definition "contributing to the establishment of an open, interoperable, technologically transparent service environment for the dynamic post issuance operation of NFC applications" [7]. The StoLPaN organization wants to establish a next generation euro wide NFC management service using NFC technology and a TSM for communication between businesses and consumers.

According to [40] a basic requirement for the NFC environment is to provide technical compatability. The underlying systems should have openness so that users can have the flexibility to choose between brands, mobile phones, mobile service providers and have the possibility to download any MCPA they may want.

[40] also states that there is a need for interoperability. They say there is still a need for interoperability for a more complex NFC environment where there is now dominance in both proprietary service applications and logistical solutions.

[40] presents a "standard dynamic card content management process". With this they aim to create a NFC service environment that are capable of managing the creation/deletion of new security domains and applications as well as application personalization. A deletion can be requested from either the MCPA service provider or the user owning the

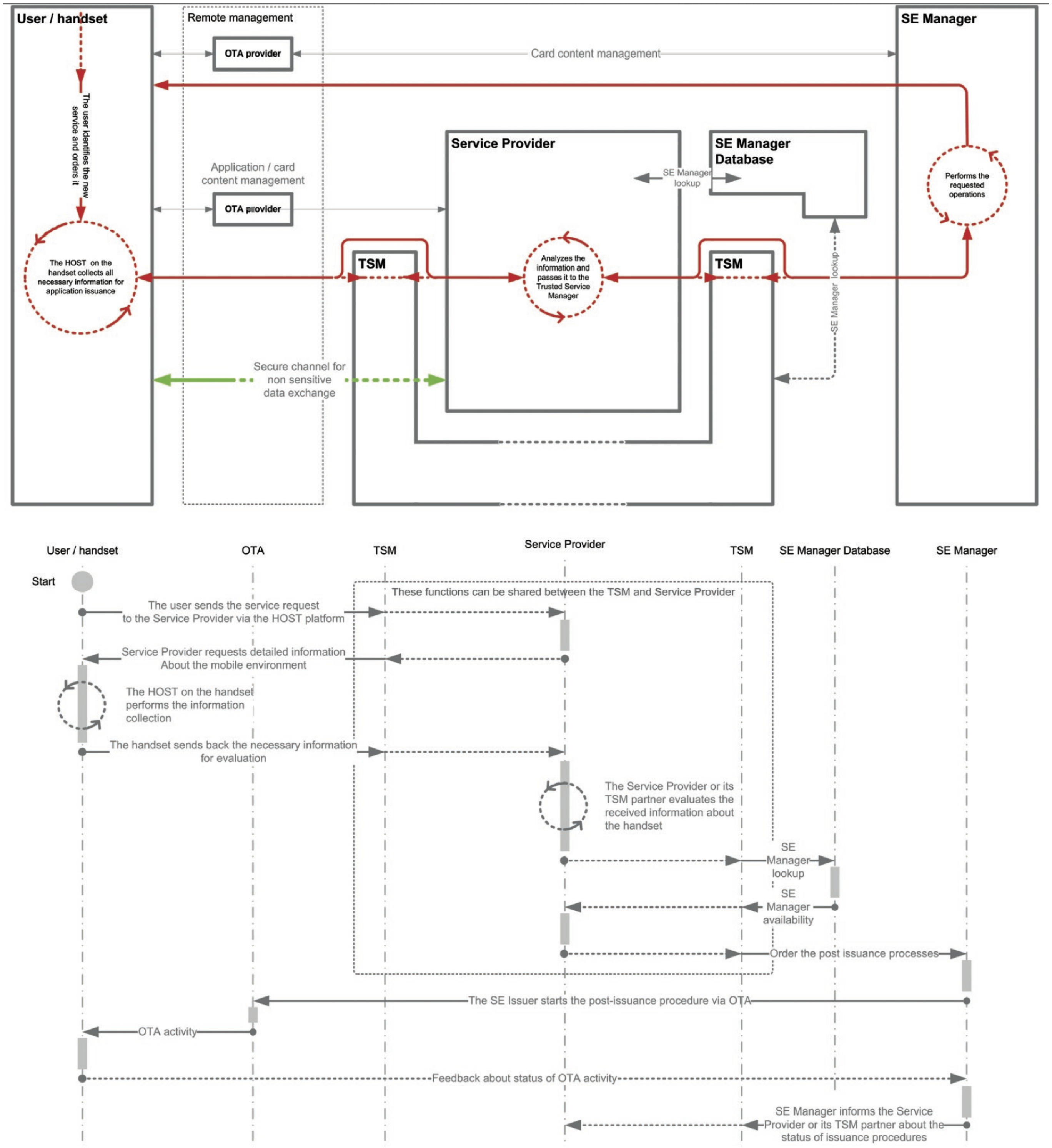

User / handset
Remote management
SE Manager
OTA provider
Card content management
The user identifies the new service and orders it
Service Provider
SE Manager Database
SE Manager lookup
Application / card content management
OTA provider
Performs the requested operations
The HOST on the handset collects all necessary information for application issuance
TSM
Analyzes the information and passes it to the Trusted Service Manager
TSM
SE Manager lookup
Secure channel for non sensitive data exchange
User / handset
OTA
TSM
Service Provider
TSM
SE Manager Database
SE Manager
Start
These functions can be shared between the TSM and Service Provider
The user sends the service request to the Service Provider via the HOST platform
Service Provider requests detailed information About the mobile environment
The HOST on the handset performs the information collection
The handset sends back the necessary information for evaluation
The Service Provider or its TSM partner evaluates the received information about the handset
SE Manager lookup
SE Manager availability
Order the post issuance processes
The SE Issuer starts the post-issuance procedure via OTA
OTA activity
Feedback about status of OTA activity
SE Manager informs the Service Provider or its TSM partner about the status of issuance procedures

Figure 4.1: StoLPaN remote post issuance procedure adopted from [40]

application. In addition the application content management process manages the service provider portfolio.

The StoLPaN proposal in [40] divides the technical process into different parts that will be shortly described here. This process is also presented visually in figure 4.1 The process describes which information is needed and how messages are exchanged in order to establish loading a security domain and an application onto the SE. The TSM is central in the process.

4.1.1 1. The start

The user initates the NFC process by performing an interaction that initiates one of the three possible NFC modes.

4.1.2 2. Information requirement, data exchange

A request is sent to the Service provider. The service provider then proceeds to collect information about the users NFC device, which SE is embedded in the NFC device and information about the SE issuer. The information comes from a generated message from the user's device.

4.1.3 3. Data check and SE selection

After receiving the information about the users NFC environment the service provider will assess if the data is satisfying the requirements needed based on "technical, security and financial considerations" [40].

SE selection will happen if the users carry multiple SEs in the NFC device. The users may indicate which SE they want to store the application in. Or the service provider may decide which SE to use based on requirements.

Finally after checking the data and choosing a SE the SP will continue to proceed with the card content management procedure, or alternatively inform the user that the NFC service application cannot be downloaded and loaded into the NFC device.

4.1.4 4. Card Issuer determination

The SP now has a selected target SE. The SP or its connected TSM can then proceed to identify the chosen SE issuer. The SE issuer identification information is delivered in the initiating message sent to the service provider from the users mobile phone containing the NFC device and the SE. The SP or the TSM proceeds to collect identification information about the SE issuer.

4.1.5 5. Post issuance process

After identifying the users SE, the SE issuer and collecting information about the users device the information is sent to the SE issuer. The SE issuer proceeds to generate security domains, and will perform requested application loading or alternatively deletion if this is requested. The issuer also generates security keys for the SP to be able to access the security domain and application.

The SE issuer will deliver keys, generate security domains and the loading of applications through a process that will either happen by itself, or by using another controlling authority(CA) or a TSM.

After data is loaded onto the card in the SE the SP or its connected TSM receives the generated keys from the SE issuer. This could also be exclusive access keys, if the service is to be managed exclusively by the SP.

4.2 NFC forum proposal

NFC forum is a consortium that tries to work with a lot of partners in order to build interoperable NFC solutions. They want to try to build an all around solution as can be seen in figure 4.2. They also detail some relevant use cases for NFC payment and couponing that is directly referenced in Appendix A, or could also be found with other user cases and in a full report in the source document.

See figure 4.3 for a visual overview of some of the functionalities.

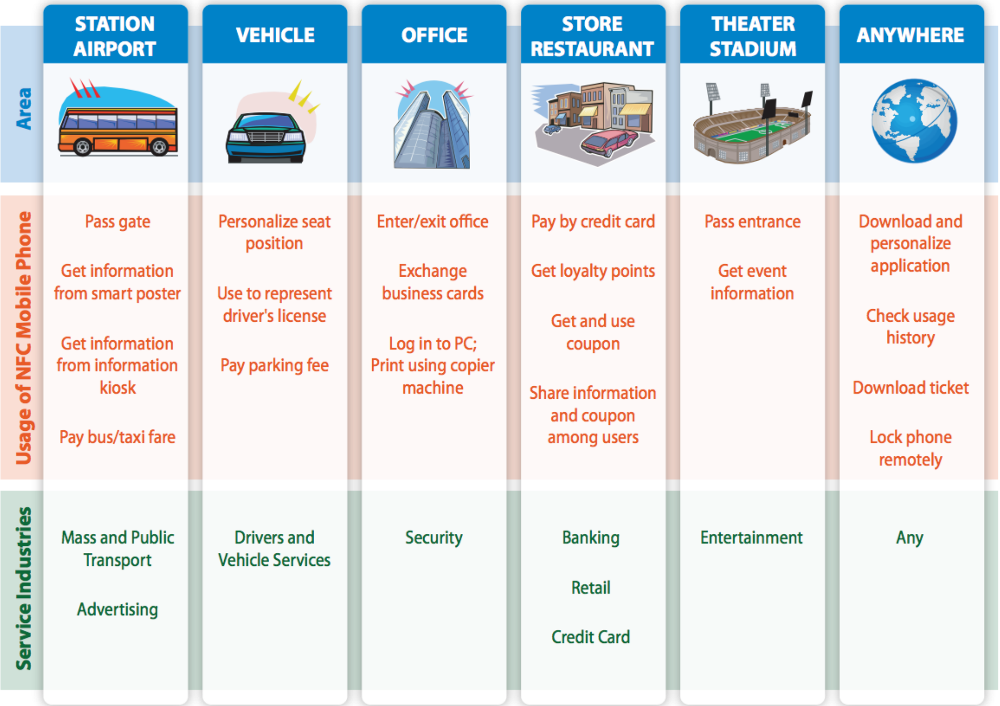
In [25] different functionalities needed in order to manage an ecosystem is also described

Download and update NFC applications

“Download functionalities are utilized to download a mobile application securely to an NFC Mobile Phone. Some applications may be stored in the AEE (for example, a UI application) and others in the TEE (for example, a smart card application).” [25]. See figure 4.3 for an overview.

Service provision

“Provision functionalities are utilized to initiate a TEE and assign a trusted area within a [TEE] to a specific service. These functionalities could be delegated by the original issuer of the TEE to a third party.” [25]



Area	STATION AIRPORT	VEHICLE	OFFICE	STORE RESTAURANT	THEATER STADIUM	ANYWHERE
Usage of NFC Mobile Phone	Pass gate Get information from smart poster Get information from information kiosk Pay bus/taxi fare	Personalize seat position Use to represent driver's license Pay parking fee	Enter/exit office Exchange business cards Log in to PC; Print using copier machine	Pay by credit card Get loyalty points Get and use coupon Share information and coupon among users	Pass entrance Get event information	Download and personalize application Check usage history Download ticket Lock phone remotely
Service Industries	Mass and Public Transport Advertising	Drivers and Vehicle Services	Security	Banking Retail Credit Card	Entertainment	Any

Figure 4.2: NFC forum's mobile NFC service vision adopted from [25]

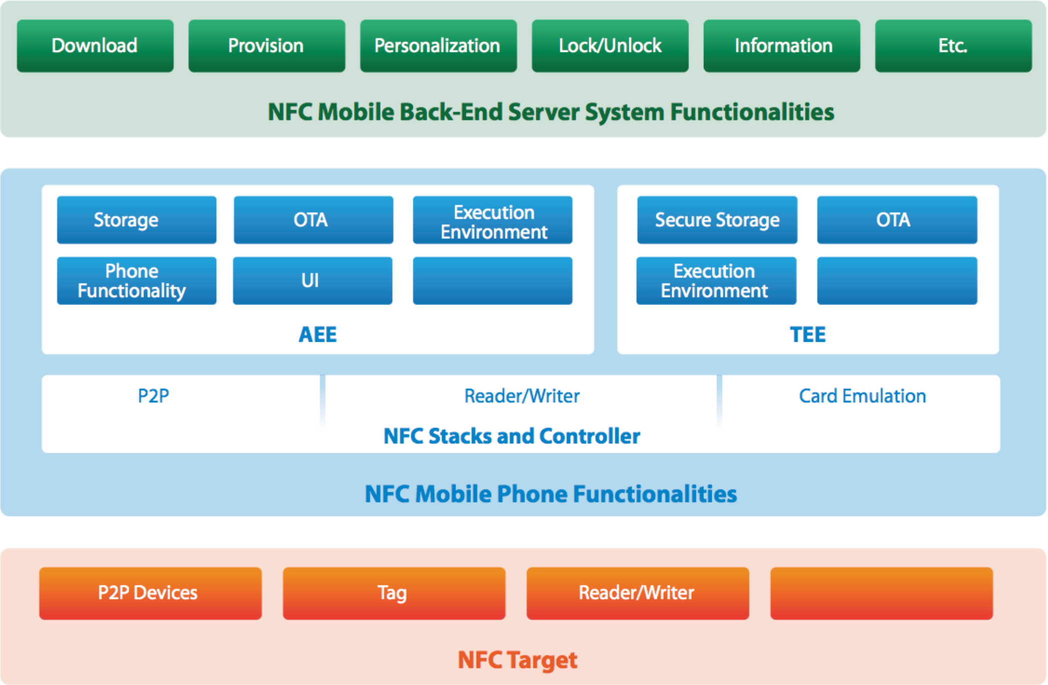


Figure 4.3: NFC functionalities figure adopted from [5]

Personalization

“Personalization functionalities are utilized to configure application- or user-specific data to an application. These functionalities could be delegated by the service provider to a third party.” [25]

Lock/Unlock

“Lock/Unlock functionalities are utilized to lock, unlock, and delete previously provisioned applications corresponding to the request from a user or a Service Provisioning.” [25]

Lifecycle management

All the functionality above is often referenced as lifecycle management in literature.

Information

“Information functionalities are utilized to provide information to or get information from an[sic] NFC Mobile Phone. Typical examples are an[sic] NFC Mobile Phone’s browser accessing Web servers and its mailer receiving information by email.” [25]

4.3 EPC/GSMA Trusted Service Manager proposal

[23] describes the Issuance process where the MNO using a UICC as SE acts as a TSM. See figure 4.4 for an overview.

[23] lists a number of requirements for a MCPA lifecycle.

- Eligibility Request: Whether or not the mobile phone is able to perform payment service
- Installation of MCP Application/TEE
- Installation of MCP Application User Interface/AEE
- Update of MCP Application Parameters
- Deletion of MCP Application
- Deletion of MCP Application User Interface
- Block MCP Application by the Issuer

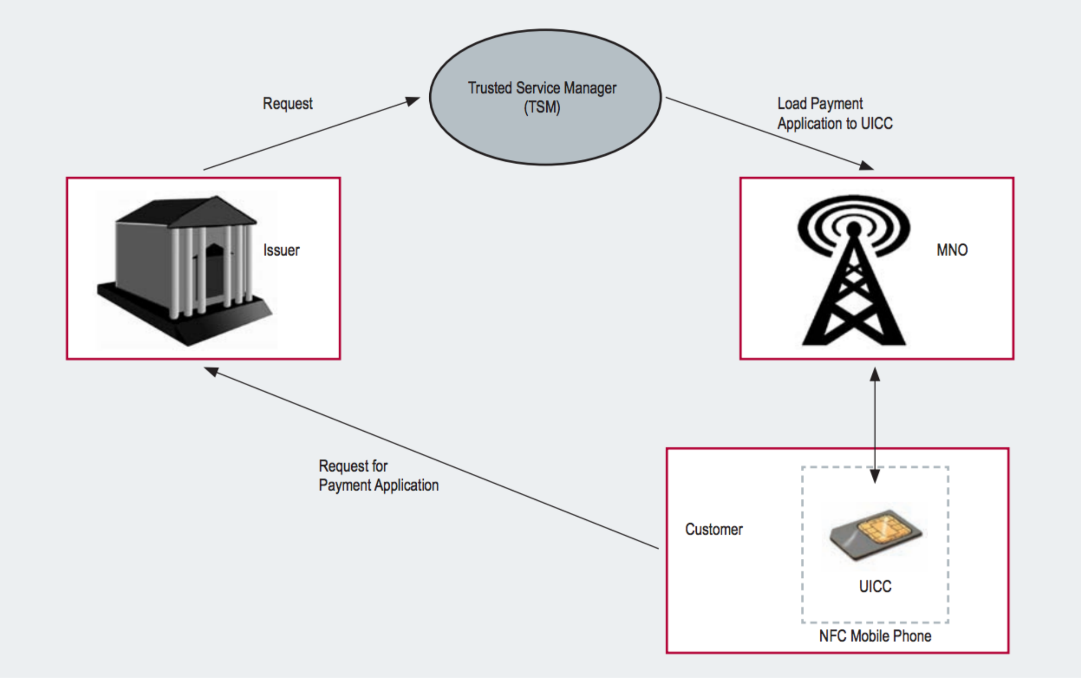


Figure 4.4: EPC/GSMA's card issuance process overview adopted from [23]

- Unblock MCP Application by the Issuer
- "Block Mobile Network Connectivity" Notification in case the phone is lost.
- "Unblock Mobile Network Connectivity" Notification
- Audit MCP Application
- Audit UICC(SE)

The auditing involves checking the application from the SE issuer or the SE itself for security concerns. The whole lifecycle can be summarized in figure 4.5

4.4 Global Platform standard

Global Platform has created a standard for a SE Card Content Management(CCM) process and a Messaging Specification in [29] [30]

[30] describes some uses cases from a technical NFC service side and the users side.

Use cases related to a NFC lifecycle management:

1. Mobile service deployment
2. Mobile service activation

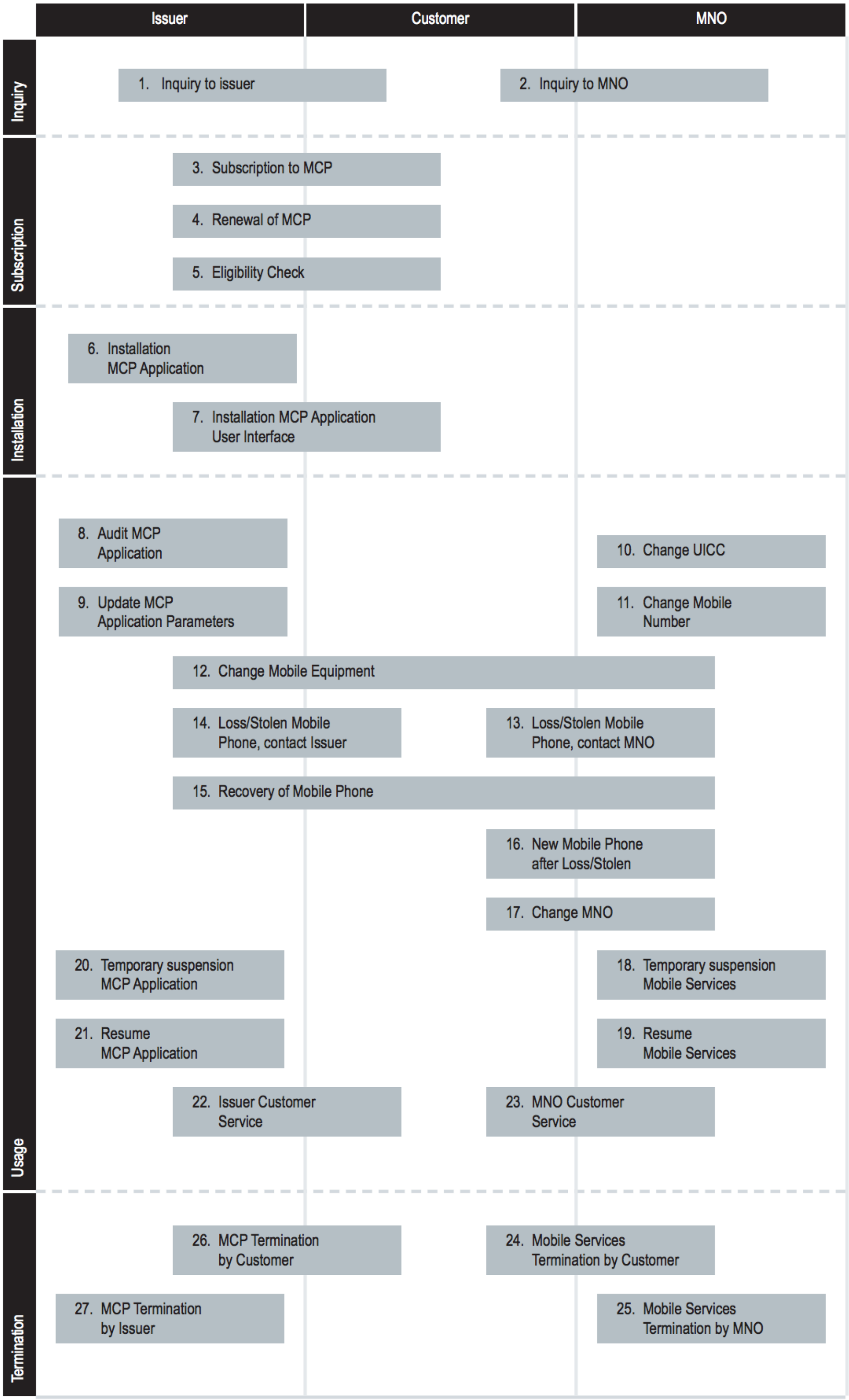

Issuer
Customer
MNO
Inquiry
1. Inquiry to issuer
2. Inquiry to MNO
Subscription
3. Subscription to MCP
4. Renewal of MCP
5. Eligibility Check
Installation
6. Installation MCP Application
7. Installation MCP Application User Interface
Usage
8. Audit MCP Application
10. Change UICC
9. Update MCP Application Parameters
11. Change Mobile Number
12. Change Mobile Equipment
14. Loss/Stolen Mobile Phone, contact Issuer
13. Loss/Stolen Mobile Phone, contact MNO
15. Recovery of Mobile Phone
16. New Mobile Phone after Loss/Stolen
17. Change MNO
20. Temporary suspension MCP Application
18. Temporary suspension Mobile Services
21. Resume MCP Application
19. Resume Mobile Services
22. Issuer Customer Service
23. MNO Customer Service
Termination
26. MCP Termination by Customer
24. Mobile Services Termination by Customer
27. MCP Termination by Issuer
25. Mobile Services Termination by MNO

Figure 4.5: EPC/GSMA's MCP lifecycle overview adopted from [23]

3. Mobile service lock
4. Mobile service unlock
5. Mobile service upgrade
6. Mobile service data update
7. Mobile service undeployment

Use cases related to a user

1. SE changed
2. Mobile phone number changed
3. Mobile device changed
4. Lost or stolen mobile device
5. Recovered mobile device after a loss
6. Get a new mobile after a loss
7. Mobile subscription termination
8. MNO swap
9. Temporary suspension of NFC services

[29] also proposes a messaging model used for MCPA management. The message includes a header and a body.

The header should at a minimum contain:

- Message Identifier
- Message Type
- Message Source
- Message Recipient
- Message Security

The message itself contained within the message body is further categorized into two different types:

- Card, application and key management interchange messages.
- Card customization messages. "These messages focus on personalization data preparation and personalization enablement, including post issuance delete, load, install and personalization." [29]

The messages follow a request-response message(Two-way communication) flow or Notification message flow(One way communication) [30]

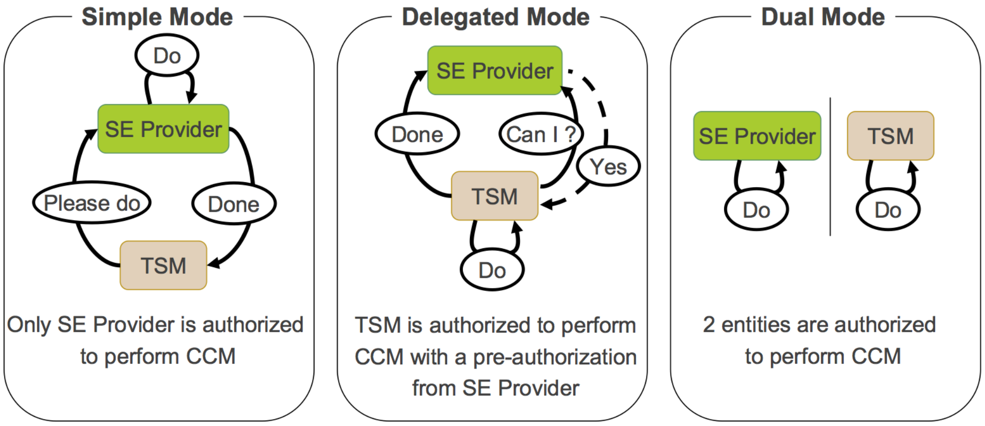

Simple Mode
Do
SE Provider
Please do
Done
TSM
Only SE Provider is authorized to perform CCM
Delegated Mode
SE Provider
Done
Can I ?
Yes
TSM
Do
TSM is authorized to perform CCM with a pre-authorization from SE Provider
Dual Mode
SE Provider
TSM
Do
Do
2 entities are authorized to perform CCM

Figure 4.6: Deployment models overview adopted from [30]

[30] identifies and categorizes different deployment modes. See also figure 4.6:

- "Simple Mode: an Issuer-centric model, where the TSM requests the SE Provider to perform a Card Content Management operation and return the execution result to the TSM."
- "Delegated Mode: Card Content Management is delegated to the TSM. Each operation requires preauthorization from the SE Provider. The execution result of the operation is optionally sent to the SE Provider."
- "Dual Mode: Card Content Management is fully delegated to the TSM on a dedicated area of the SE. Dual mode is characterized by the presence of at least two Security Domains with the Authorized Management privilege in the Secure Element."

4.5 Other mobile wallet related applications or services

- TrustNorway has launched a Norwegian based TSM [8] [10]
- An organization called ISIS is trying to create a TSM service [2].

Chapter 5

Main work

From the proposed standards studied and best practices suggested it is possible to build at least abstract design models for TSM systems that will be presented in this chapter.

The background chapter and the related works chapter shows that there are a lot of possible uses for a TSM. And the State of Art chapter presents functionalities needed that will be taken into account when presenting a design for a TSM.

For the understanding of the design it is important to note that TSM is used before the actuall payment or voucher/loyalty card usage takes place to issue Mobile contactless cards to be stored in the User's SE. Or in other words if the TSM where to handle only payments the TSM would issue MCPA cards to a User before the User can perform payments with the card. So the advantage of the TSM is that the User can download the card instantly and does not need to wait for the Card to arrive by mail. More technically described before the user can perform a payment the TSM's main objective is to install the MCPA in a card issuance process.

During the lifetime of the application the TSM will handle different processes referred to as lifecycle management. An example is for instance a request from the user to delete a MCPA that will result in the application being deleted. In this case both a TEE and an AEE application may need to be deleted, as well as applications or application references residing in the MCPA SP, TSM and in a SE issuer service depending on who holds data. Other lifecycle management processes will also be detailed in this main part, for instance the downloading and personalization processes as mentioned earlier. The installation of a MCPA onto the User's device from the TSM will be described in detail. See figure 5.1 for an overview of the MCPA lifecycle management process for requesting and installing a MCPA in the users NFC device.

Because the participants in NFC ecosystem have not come to full agreement some assumptions are made that will be noted throughout the presentation of the design. Some initial assumptions are presented in the next paragraphs.

The NFC mode that will be used for NFC MCP payments is the card emulation mode.

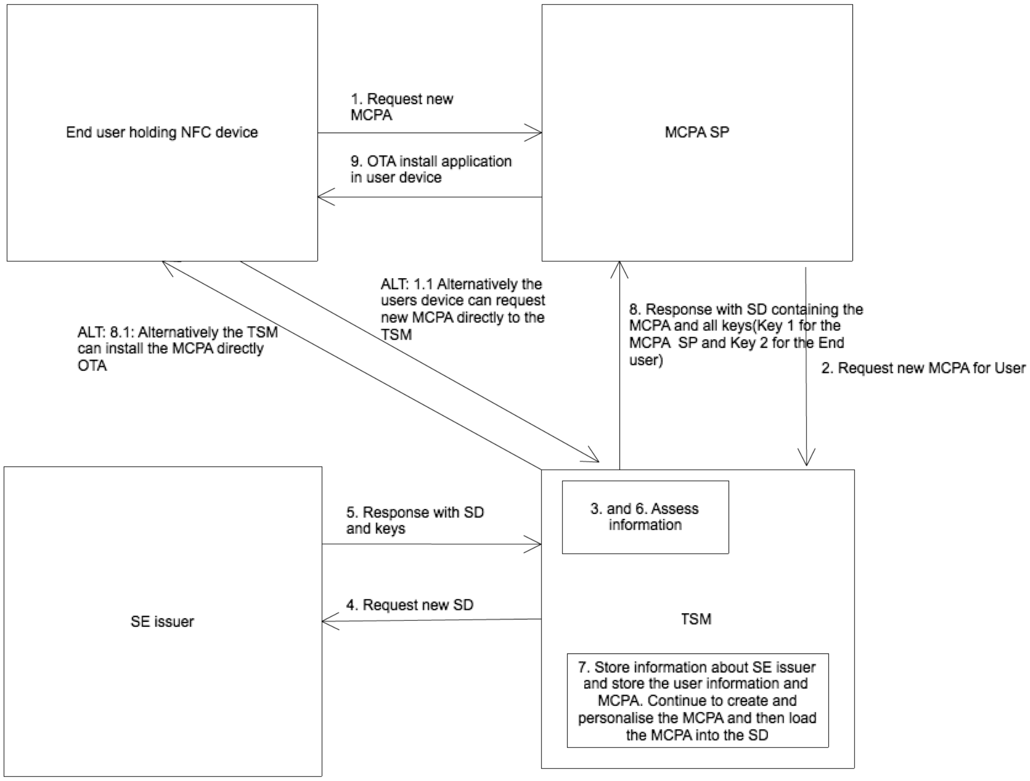

End user holding NFC device
1. Request new MCPA
9. OTA install application in user device
MCPA SP
ALT: 1.1 Alternatively the users device can request new MCPA directly to the TSM
ALT: 8.1: Alternatively the TSM can install the MCPA directly OTA
8. Response with SD containing the MCPA and all keys(Key 1 for the MCPA SP and Key 2 for the End user)
2. Request new MCPA for User
5. Response with SD and keys
3. and 6. Assess information
4. Request new SD
SE issuer
TSM
7. Store information about SE issuer and store the user information and MCPA. Continue to create and personalise the MCPA and then load the MCPA into the SD

Figure 5.1: MCPA lifecycle management process overview

The payment terminal then needs to be an active device that communicates with the NFC emulated card. The payment workflow could then work in three different ways: The user first enters his or her pin code on the mobile device. Alternatively the user can tap the phone, enter the pin, and then tap the phone again(For instance for large values). Finally for small amount the user could perform the payments with no credentials. In either case the User performs a payment by ubiquitously putting his or her device near the terminal, which then proceeds to do the payment as in the n-party models without the TSM being involved.

The processes described will mostly take a basis in the four-party model. But in theory both two-party(Vouchers) and three-party(Credit cards) models could also work. The Voucher model would then require the same functionalities as the value added services, and the credit card would need to be issued in the same way as a debit card.

The MNO's part is not described in detail. A MNO may have a role delivering the application over a dedicated network. Or may take a role as a CA. However the goal is to present designs that are independent of MNO's. The card issuance delivery could then for instance be performed over Internet or any Mobile network as long as the right security and remote management means are performed. This would compromise the reliability of the application, but is a trade off to gain more openness and interoperability.

5.1 Analysis of state of the Art

All State of the Art work studied suggest building NFC payment infrastructure as an extension to the traditional payment systems. Where the TSM replaces the traditional way of issuing cards.

Most State of the Art(not [40]) work studied suggest building a MCPA service that uses the card emulation mode and then managing a card issuance process with a TSM.

Most State of the Art work studied suggests an OTA process to handle both the TEE and the AEE lifecycle.

The SE issuer may be the MNO, the phone producer or even an SD card producer(Although not discussed much) in literature. This report will try to stay neutral to who the SE issuer actually is. But instead have a focus on which interfaces and associated methods is needed. The idea is that the TSM itself stands outside the scope of who the SE issuer actually is.

Whether or not the MCPA SP should be the access point for handling the User requests or the TSM should be used directly is unclear. In this thesis we assume the MCPA SP is contacted directly from the different User devices, and then redirected to the TSM. This gives the MCPA SP the advantage of being in control of which TSM it will use.

None of the state of the art except [14] envisions scenarios where the TSM communicates with another TSM. But scenarios in which a MCPA SP would change TSM provider or scenarios where the TSM grow so big that they need redundant TSM systems can be thought of.

5.1.1 StoLPaN analysis

A small analysis section is added here specifically for the StoLPaN case: The StoLPaN proposal describes some parts of the process to happen either in the SP/SE issuer(CA) or in a TSM. So several scenarios may need to be supported in order to support different SPs needs and wants. The TSM should therefore be able to support multiple scenarios in order to support different implementations.

[40] suggests a SE Manager Database to handle the problem of handling multiple SE issuers.

[40] also loosely defines the difference between the MCPA SP and the TSM, while the designs presented in this thesis will try to clearly define the different functionalities and in which system they are found.

5.2 Requirements specification

This section combines some of the State of the Art work's proposals for requirements. The goal when this requirement specification list was created was to get a full overview of the requirements needed for a TSM in order to later be used in a design model. A minimum requirement for a TSM is that it should be able to handle the MCPA lifecycle process.

5.2.1 Functional requirements

5.2.2 Functionalities overview

- Information functionalities.
- Lifecycle management over OTA functionalities
- Configuration functionalities
- MCPA SE Applications Lifecycle Management functionalities:
  - Assessment Process
  - Establish Secure Domain(SD)
  - Personalize MCPA
  - Deployment: Load/Install/Upgrade
  - Activate/Deactivate
  - Update
  - Undeployment: Deletion/Removal
- Users MCPA Lifecycle Management functionalities:
  - Change SE
  - Change mobile phone number
  - Change Mobile device
  - Change Mobile subscription
  - Swap MNO: Change from one MNO to another while keeping the same telephone number.
  - Terminate Mobile Subscription
  - Suspend mobile NFC services
  - Blocked/Unblocked e.g. the MCPA SP or the MNO blocks the Application.

  - Lost/Unlost/Lost and user gets a new mobile phone
- Value added services
  - Couponing: Offers/Discount
  - Loyalty programs

Information functionalities

Messaging to and from customer/user. Information Messaging is a trivial problem and will not be discussed more from here on in order to focus on the Lifecycle Management process.

- Informational Messages shall be able to be sent to the users device.
- Informational Messages should be able to be sent from the users device

Lifecycle management over OTA functionalities

In regards to the lifecycle functionalities it will be assumed that the TEE and AEE are installed either near simultaneously or a TEE is installed via an AEE over an OTA channel. Either way an OTA channel needs to be established

- There shall be an OTA application loading/updating/deletion/locking process.
- There shall be an OTA personalization process.

MCPA SE Applications Lifecycle Management functionalities

The lifecycle functionalities are adapted mostly from [25] and [23]. If the OTA is to be handled from the MCPA SP the TSM will deliver the MCPA to the MCPA SP. But a TSM should also handle OTA processes. In any case these functionalities will be nearly the same. It is assumed that security and remote management is handled by the OTA functionalities. The Lock/unlock functionalities are described in [30] but are left out as they are defined as Activate/Deactivate in this thesis.

- Assessment Process: Check if the requested card is able to created based on information gathered from the Users request and the SE issuer.
- Establish Secure Domain(SD): Request a secure domain and forward it to the MCPA SP or the requesting NFC device.
- Personalize MCPA: Create a MCPA that is personalized with user and application specific data.

- Deployment: Load/Install/Upgrade of a MCPA into the SE from the TSM or deliver the MCPA to the requesting client for it to handle OTA itself.
- Activate/Deactivate: Remotely activate or deactivate the MCPA e.g. Lock/Unlock the application from executing
- Update: Update personalization data.
- Undeployment: Deletion/Removal: Remove the MCPA from the user NFC device and in any other system keeping reference to the MCPA.

Users MCPA Lifecycle Management functionalities

These functionalities are adopted from [23] and [30]. The functionalities are related to actions performed by end-users. e.g. the user changes a SE. These functionalities enables the TSM to have flexibility in order to be open for different scenarios as discussed earlier. The functionalities here are self describing.

Configuration functionalities

In order to be able to do an assessment of applications, and then produce MCPA's that fits the user's NFC device configurations should be gathered and kept in a database. These configurations could be accessed or updated from for instance a MCPA SP sending a request for changes in the MCPA's to happen for all users. After a MCPA SP send such a request the MCPA's stored in the Users device would need to be upgraded. The configuration database could also be used to store information about the different SE issuers and SE types. Or the TSM could update the Configuration manager with information about different new NFC devices.

- Virtual SmartCard configuration management functionalities.
- Device configuration management functionalities.
- SE configuration management functionalities.
- Eligibility/Assessment Request functionalities.

Security functionalities

- MCPA/User/POS authorization.
- SE issuer authorization.
- Authentication for all actors in the system

Value added services

These services will have the same lifecycle services as the MCPA applications. But these virtual cards will contain different data compared to a MCPA when being personalized and updated.

As a suggestion the loyalty cards could contain user identification as well as a counter. And vouchers would need some identification for the item to give discounts for or just a decoded barcode identifying the voucher.

5.2.3 Non-functional requirements

Interoperability

A way of getting interoperability is to create a service interface for communication where all parts involved with the system agree on the design, or in otherwords that an API follows a standard specification. In addition a common language or more specifically a common messaging specification that defines a service language and the data structures to be exchanged between the systems should be established Different systems will then be interoperable to one another.

Content negotiation comes out of the box with some service frameworks today(e.g. ServiceStack) and could be implemented in order to give clients the possibility to choose from different Content types. The data structures needs to be consistent however.

In order to establish technical interoperability a service interface and a common messaging specification should be established.

Openness

Users should have the possibility to choose their own mobile phone type, phone number, carrier and bank. In addition it should be a platform that is open for different financial institutions issuing cards, SE Issuers(e.g. MNO's with UICC, Manufacturers and Secure Digital card producers handling keys for the SE) and other players wanting to join the network(e.g. Certified developers creating innovative services).

Security

The payment transactions will consist of private and sensitive data exchanges. The TSM therefore needs to give guaranteed end-to-end security. With the extension to NFC technology there is a new platform with opportunity to do mischievous tasks that exploits the integrity of the traditional payment service, like for instance eavesdropping and data tampering in order to perform illegal activities like fraud and theft. So in order for a TSM to be a trusted third party a high level of security is required. The OTA channel should have end-to-end security. Security around NFC security has been covered by multiple works [17].

A definition of roles needs to be established in order to control authorization and authentication. The roles define what access the user has. For instance the User role will have access to lifecycle functionalities, while an SE issuer/CA role will have access to SE issuer/CA specific functionality like uploading CA keys.

An authentication scheme needs to be created in the TSM: The roles needs to be authenticated before they perform only authorized actions. Where a role can be a User/a MCPA SP on behalf of the User or an SE issuer. And an Action could be to respectively download a MCPA, or to upload a key from CA. This could be done in the traditional manner of authenticating the user in the service layer and then performing authorization on methods in the service layer and the data access layer

An authorization scheme should give access to the MCPA and keys for a user, but to nobody else. The security domain downloaded from the SE issuer with the appropriate keys secures the MCPA itself. But it should still not be possible for anybody to access the MCPA or especially the keys. So authorization in the TSM to gain access in order to for instance re-download a MCPA is necessary. In addition different Actions called from an End user should be authorized. A suggestion as shortly mentioned above is to do role specific authorization on methods in the service layer, for instance by using authorization by annotation. And also controlling authorized access to resources in a data access layer.

Availability and accessibility

The TSM issuance functionalities should never be down and has to have a high availability which could technically achieved in the TSM with redundant systems and other availability measures such as hearthbeat, downtime alerts etc. Actors external to the TSM such as the MCPA SP/CA should also be required to sign a SLA with the TSM.

Usability

Usability should mostly be covered by the AEE App. However the API should also be easy to use and well documented for external implementers.

Performance

During the actual payments the end user does not go via the TSM. But users still would expect this payment means to be at least as good as the plastic card payments so the system needs to perform in real-time even if it is initated from a mobile phone.

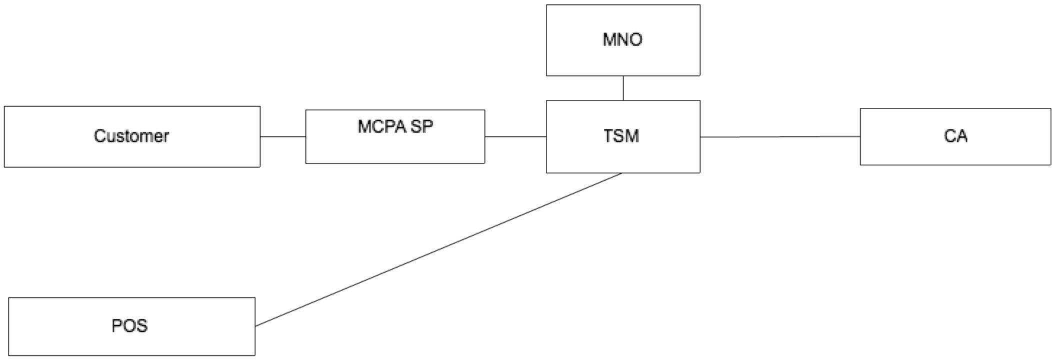


Figure 5.2: MCPA lifecycle management collaboration diagram

While performing the Lifecycle functionality the TSM Server should have a high upload rate in order to give Users satisfying download rates. Most likely the Card file size will be in magnitudes of some Megabytes or even less. The links should at least have some performance management in order to look for and alert congestion in the traffic.

Reliability

The payments themself need to be atomic, either they occur or not at all. Most of this reliability is covered by the traditional payment systems. But it is important that this reliability should kept.

The lifecycle functionalities also needs to have high reliability. The card must be downloaded correctly, with no errors. This could for instance in an implementation be done using a checksum scheme.

Dependability

The system shall work and be available at all times for users. And should be reliable.

5.3 Design Models development

5.3.1 Collaboration diagrams

Collaboration diagrams that show the different roles and how they are related can be found in figure 5.2

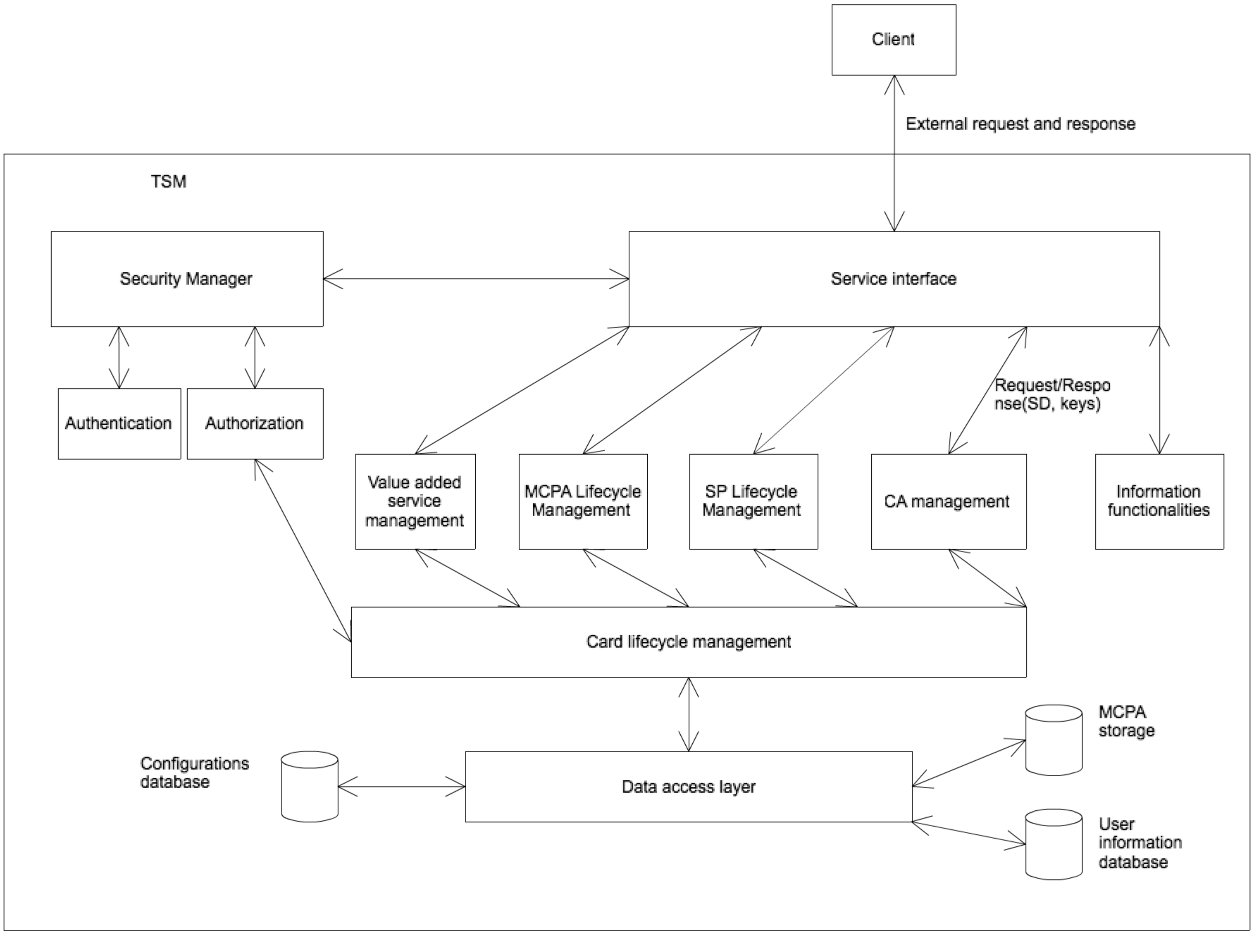


Figure 5.3: MCPA lifecycle management software architecture diagram

5.3.2 Software Architecture

An overview of the software architecture for a TSM depicted in 5.3 shows which modules a proposed TSM solution should contain. This also gives a pinpoint on what needs to be served in a service interface: Different actors should have access to different methods in the service interface.

The software architecture design includes the following:

- Security Manager
- Service Interface
- Lifecycle functionalities modules for different roles.
- CA functionalities module

- Information functionalities module
- Data access layer

It should be added that a TSM could possibly also be acting on behalf of the MCPA SP. This does not however change the software architecture, the Client would in this case be the End-user. And the TSM needs to perform OTA management in the users device. In this case the Users could connect to the TSM directly or be redirected via the MCPA SP.

5.3.3 Service Interface

Further in order to get a unified service language an API specification for the TSM is presented here. This specification also helped in the creating further designs as it separated the concerns. This API can also be looked upon as a proposed OTA communication standard. Both incoming and outgoing messages are defined in this API proposal. The messaging structure is defined in the next section.

A web service with content negotiation is proposed for an implementation.

API:

The API should mainly consist of methods for the User, the SE issuer and the MCPA SP:

The User should have an API for lifecycle functionalities as well as user specific functionalities: A general pattern can be applied here: LifecycleFunctionality(Message: Information), where for instance a lifecycle functionality would be Update(Message: Information). This general pattern does not however apply the for Assessment Process or the Establish Secure Domain(SD) which are respectively an internal eligibility process and a Request/Response to the SE issuer.

Regarding user changes the user could either send a notification upon changes. Or the TSM could poll for changes. After the TSM gains knowledge about a change it would need to perform necessary actions, for instance updating the MCPA.

- Request(Message: Information)
- Response(Message: SD(MCPA))
- or Poll(Message: Information)

The MCPA would in some cases want to get MCPA's produced by the TSM. The TSM would then need to deliver the MCPA to the MCPA SP in the same way it would deliver a MCPA OTA to a NFC device. In addition the MCPA SP would need to configure the cards in a process.

- Request(Message: Information)
- Response(Message: SD(MCPA), KEYS)

The SE issuer needs to be requested for issuing SD and keys:

- Request(Message:Information)
- Response(Message: SD, KEYS)

Example of messages for loading of SE from TSM.

- Request(Message: User information), see sequence diagram 5.5 for an example. This message will be sent from the user for instance to download and personalize a MCPA.
- Request(Message: User information, SE issuer information), again see sequence diagram 5.5 for an example. This message goes to the SE Issuer.
- Response(K1, K2, SE(MCPA)), 5.5, this message can be used to create the SD the first time it is requested
- Response(SE(MCPA)), 5.5, this message can be used to get the SD the first time it is requested

There may be some variations in the use of the message structure that should be detailed in an implementation design.

5.3.4 Message structure

The data exchanged between the different actors is suggested to be as follows: According to the standard defined in [30] the messages exchanged between systems should be have a header/body format. See figure 5.4 for an overview. The header should as a minimum contain:

- Message Identifier(E.g. GUID)
- Message Type
- Message Source
- Message Recipient
- Message Security

Whereas the body could contain:

- Card, application and key management interchange messages.
- Or card customization messages. “These messages focus on personalization data preparation and personalization enablement, including post issuance delete, load, install and personalization.” [29]

Example of usage of the message structure for installation request from a client would be:

- Message:
  - Header:

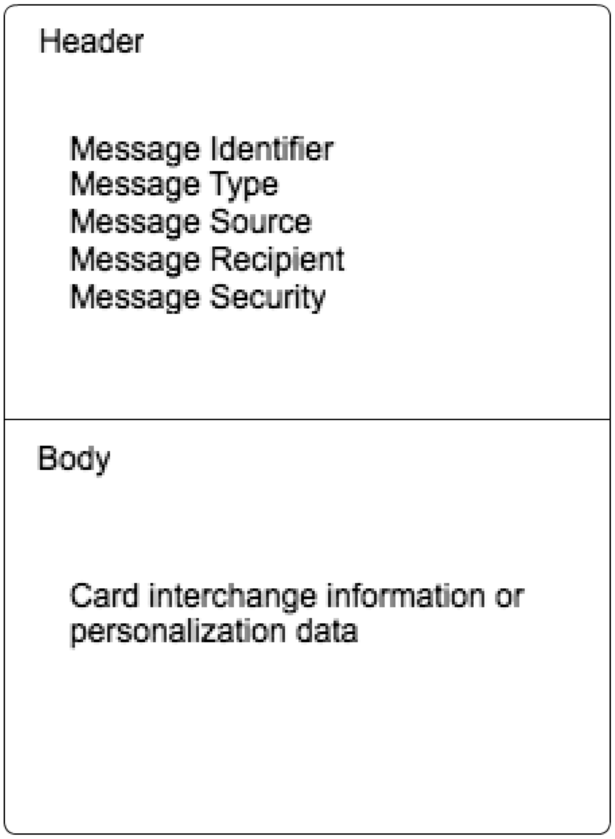


Figure 5.4: MCPA lifecycle management messages structure

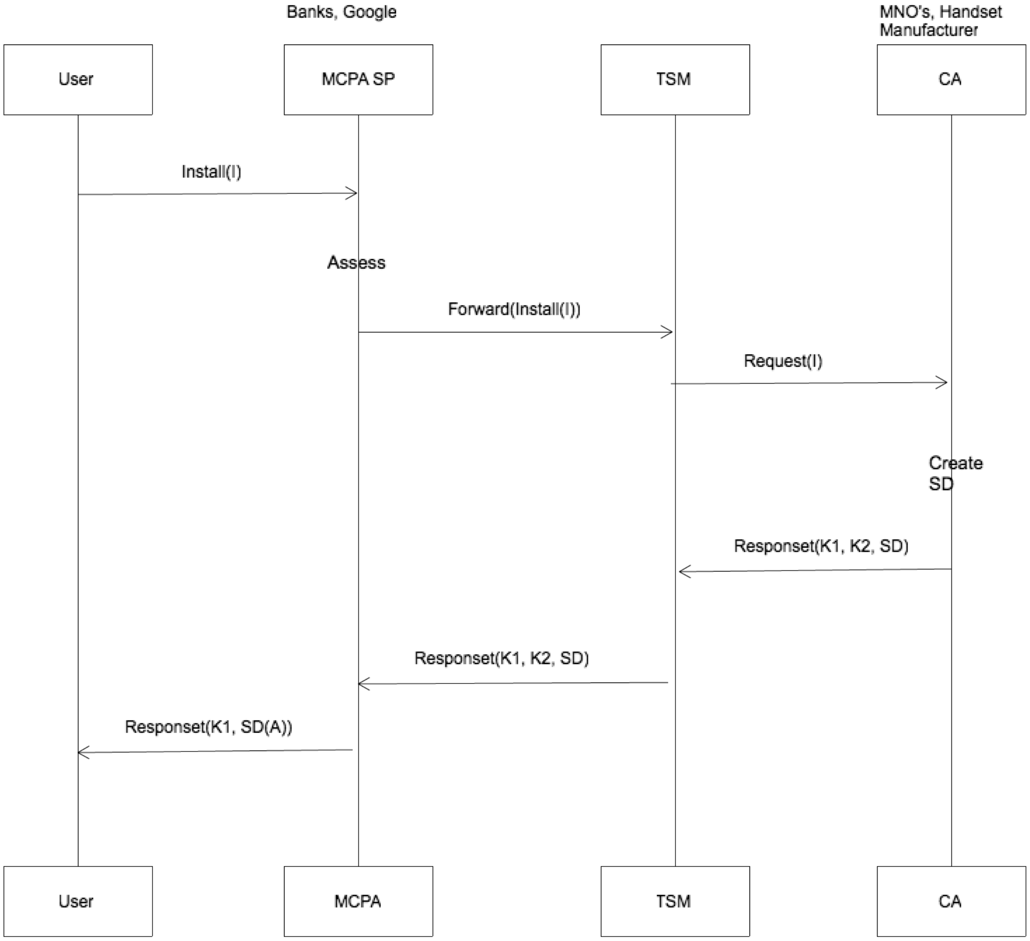


Figure 5.5: MCPA lifecycle management installation sequence diagram

  - Identifier: [GUID]
  - Type: Install
  - Source: MCPA SP1 address
  - Recipient: TSM1 address
  - Message Security: Top secret
- Body:
  - Information about the User

An example of the MCPA lifecycle management installation process is described in the sequence diagram in figure 5.5

It should be noted that in the Sequence diagram the TSM could also as noted before perform tasks directly on behalf of the MCPA SP and that the SE issuer could also certify or give rights to the TSM to create security domains. This is up to business agreements.

Both binary and XML data [29] formats has been discussed in literature. The advantage of binary format is that it has smaller overhead in parsing the messages. Since the goal for this thesis is to propose design models this implementation details is left for the implementation phase to figure out.

Different stakeholders and different concerns about and around the data

The different stakeholders will handle the data differently and have different concerns about the data being exchanged:

- SE issuer will be concerned about the available resources(For the Security Domain to be stored in the Users storage)
- TSM will want to hold the user data and domains so that it does not need to be set up again for instance if the user switches phone. The user data includes personalization data and user MCPA and User/SE issuer domain.
- The banks will possibly be concerned about owning the keys exclusively and that the data is exchanged securely. Some banks are also likely to not wanting to use an external third party TSM, but would want to be their own TSM.
- The users are concerned about the data security; Whether or not this payment means is as secure as the traditional plastics. The data should be securely stored in the SE and securely transferred over OTA channels from the TSM/MCPA SP. The banks may use similar Card structures that may be reused but will need different personalizations.
- When considering the POS they would also require security to be as of todays standards.

5.3.5 Post Issuance Process Design

The installation process from the users request until the process is stored and activated in the NFC device will be presented in this section. [30] also describes this process by listing the following.

1. Eligibility/Assessment process
2. Create SD
3. Personalize SD
4. Load SE application
5. Install SE Application

6. Personalize SE application
7. Activate SE application
8. Install UI application

By further elaborating on the presentation in [30] the different parts are running in different locations 1. is a compliance check performed by the TSM. 2. through 3. is done by the SE issuer or another CA. 4. through 5. is done by the TSM's Lifecycle Manager. 5. through 7. is performed by the TSM down to the users NFC device. While 8. is done either by the Lifecycle manager or could already be performed by the end user from an App store as assumed before.

See also figure 5.6 for figural overview of the process. The other Lifecycle processes will follow a similar flow.

5.3.6 Challenges

The domain is quite broad and complex and a lot of different players and systems are involved.

There seems not to be established agreement between stakeholders and there are some insecurity in most research for how a final TSM system should work, at least it is not crystal clear.

Most standardization work present whitepapers showing only partial solutions. Hopefully this work can show a more holistic view.

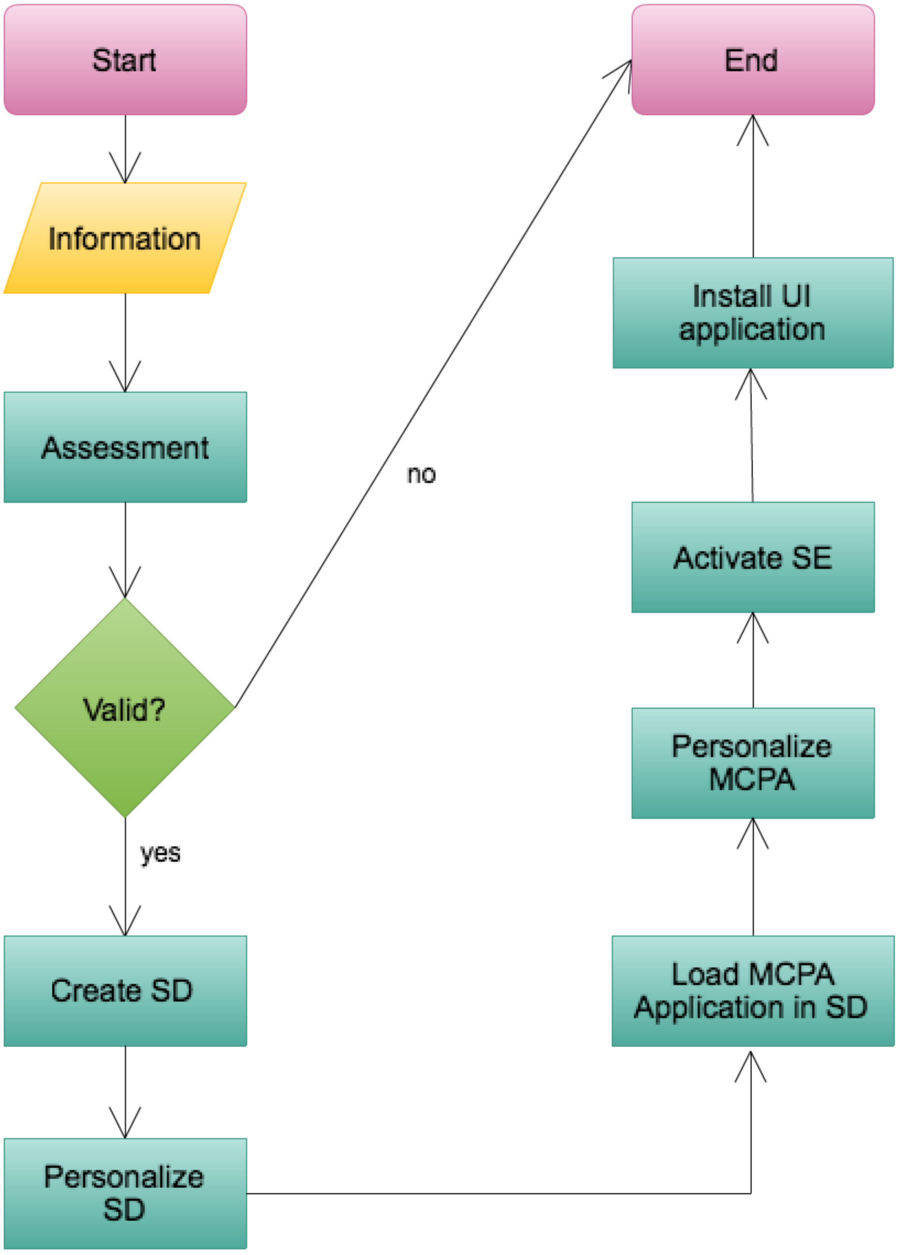


Figure 5.6: MCPA lifecycle management installation process diagram

Chapter 6

Results

Designs and figures as well as specifications modeling a TSM has been created and is presented in the main part.

6.1 Research questions answered

6.1.1 In what ways can a TSM be designed using current proposed standards/protocols, guidelines and work in academia/commercial work(Best practices etc.)?

Logical and abstract designs and specifications of a TSM has been presented in the main part. These designs take a basis in work from academia, commercial works and standards.

6.1.2 What other mobile payment systems are proposed or are live today? How are they designed? How do they work? Are there something to learn from best-practices?

Google Wallet shows an example of an implementation of a MCPA SP presented in the background section. They have created a system using a backend TSM solution, but in addition they have now also extended their electronical wallet to also include a Cloud wallet.

The State of the Art section also shows that there are some works in progress working on proposing TSM systems solutions.

The State of Art works show few designs for TSM systems. Best practices are found by doing an analysis by comparing the different works.

Trust Nordics(Previously Trust Norway) are advertising a TSM on their webpage [10]. In addition ISIS are trying to gain dominance as a mobile payment provider using NFC technology [2].

6.1.3 What non-functional and functional requirements are required in order to build a TSM service providing properties at least as good as current payment systems? How can non-functional requirements be achieved in the system and service design?

Different functional requirements that is needed as a minimum has been gathered and defined in the main part.

Non-functional requirements are also presented and discussed in the main part.

Chapter 7

Discussion and Evaluation

This thesis has proposed design models and specifications for a TSM system. The designs shows abstract and logical designs based on the requirements gathered. There are multiple functionalities for a TSM to perform. A minimum requirement that is essential for a TSM is to perform MCPA lifecycle management tasks. But requirements could also include value added services, CA management and User specific Application management for the SP.

Some discussion around the designs and discussion around interoperability and system opennes will also be presented in this chapter.

7.1 Discussion

It has been learned in this thesis that a good understanding of a domain is important in order to build some systems and that this will affect the system design. [31] discusses design of technical network architectures from a business aspect point of view, and states that the following must be considered in a technical architecture: "Relations between current state, financial aspects, product forecasts and technical solution.". This can according to [31] be achieved by looking at different models:

Some models to be considered in a technical architecture [31]:

- Finance model: Not studied in this thesis.
- Vendor relations model: Studied in this thesis
- Players in the market: Studied in this thesis.
- Business operation model: Not studied in this thesis.
- Market model: Studied in this thesis.

In literature studied it has not much been discussed TSM solutions that support multiple SE types. Most literature studied, even literature that discusses different SE types, will sketch future systems to only support one variety. The assumption is that one SE would gain dominance and would then be the preferred SE. A TSM that support multiple SE types is however suggested in this thesis.

A scenario where the TSM acts as a CA for the keys/SD to be exchanged could enable an ecosystem with a TSM that is not neutral. Or could make the ecosystem more neutral. In order for the TSM to stay neutral when it is also CA it should have clear policies on for instance what to do in a situation where it would compromise its own values. However if the policy of the TSM is to stay neutral and it acts as CA, the whole ecosystem could gain the advantage of having a CA that is neutral to business needs. This would however require some business agreement with the SE issuer where the SE issuers would likely loose some power. And would most likely require the TSM to pay for this loss of power through fee schemes. An example of the power of the keys/SD is how Google are for instance producing their own phones with Google wallet support and where Google is both SE issuer and SP. This gives Google control over the Keys and if a big competitor where to come in with a service similar to Google wallet 2.0 they would most likely deny it. Another example can be thought out: A MNO would most likely not give away the keys to the UICC for free. But if the TSM was free to install certified applications to the SE through fees to the MNO the TSM would have more freedom and the whole ecosystem would be more open.

There is not much need for POS to invest in new payments devices containing NFC capabilities as of now. Most POS are said to be happy with their current payment systems in literature. In order to propose value to the POS's value added services needs to be developed. Value added services are discussed in literature to be essential in order for the POS to transition to NFC payment solutions. But how a Trusted Service Manager should perform these tasks or not are not much discussed in literature studied except for some cases showed in the Related Works section that demonstrates that it is possible to build such solutions and especially with security in mind. It is possible to imagine however that coupons that can redeem offers, discounts or loyalty cards could also be stored securely in the SE. When the users pay for the wares or services they could then utilize the value added service offer before the actual payment. After the payment the coupons/discount offerings would need to be deleted from the users SE. And the loyalty coupons would need to be updated. So the actual value added services can be identified to be the same operations as in a Card Lifecycle Management and personalization process. To make this work the TSM would need to set up some business agreement with the POS.

There is a trend that some players are now trying to utilize the Cloud to perform payments. These players will be competitors to TSM creators. This is how PayPal has worked for a long time. The idea is to store the user information about their card in the cloud instead of the users device. This model will presumably be easier to manage because it does not need a card management process, but there would possibly be trade offs from what NFC technology could offer. Especially considering security where the NFC MCPA is stored in a SE whereas a Cloud solution would presumably not. Google manages to mix the best of both of the Cloud and NFC world with its Google Wallet 2.0.

7.2 Discussion around TSM interoperability and openness

There is a sense that most work will loose theirself in defining interoperability and then for instance target multiple MNO's instead of multiple SE types, where a SE type is for instance the UICC. In addition the new kind of SE found in NFC devices inside some modern Mobile phones further expands the SE issuers and adds a new SE type. This new SE and how to adapt the TSM with its addition has barely been discussed in most current work studied. This thesis work suggests a solution that is independent of SE type. A MCPA that supports the SE type should be negotiated for transparently in a request from the end user. In order to do so the MCPA's are created from a Configuration database as suggested in the main part, where the SE type is required to be input in addition to brand type/mcpa type and other personalization information.

There are some issues in who should have the TSM role still. Some MNO's would want to be TSM in order to use the UICC as SE. But to enable interoperability across multiple SE it is important that the TSM stays neutral to the use of SE. The MNO could still be be part of the ecosystem in using the UICC and provisioning the network required to perform OTA operations against a fee.

It has been showed that it is possible to logically design a TSM system that can be flexible to the complex ecosystem's needs on openness: Openness is achieved by letting the user have functionalities to change number, perform MNO swaps, use new handset devices and so on as specified in the requirements. And the system is open for different actors to connect to the TSM.

The TSM designs and specifications in the main part also shows and describes how to achieve interoperability between the different systems that needs to communicate in the ecosystem. For instance by proposing a standard API for all to communicate in addition to a standard message specification.

7.3 Evaluation of Contributions to the existing TSM projects

This work contributes to existing work by proposing standard formal design models described using UML and model figures.

The work also proposed a common service language description in order to create interoperability across multiple vendors. This is presented with an API and a common language to achieve interoperability across systems.

Openness is achieved by adding functionalities that enable the Users to have flexibility.

The thesis combines a lot of State of the Art work and gives an evaluation of this work.

The study done on the State of the Art covers a lot of whitepapers in addition to one standard proposed by GlobalPlatform. The whitepapers show only partly solutions. While the GlobalPlatform standard that gives specifications for the whole ecosystem but with a low focus on the TSM role. Hopefully this thesis gives a good overview and a clear view on requirements of a TSM as well as design model proposals.

Chapter 8

Conclusion

A common terminology used by different standardization bodies has been identified. A taxonomy of the players in the NFC ecosystem has been sorted. This thesis combined multiple works in order to do so to give multiple views. With the taxonomy and terminology identified the different stakeholders can use this report as a reference for a language to communicate.

Most of the focus in this work has been on the MCPA issuance process which is a central part of a TSM solution. A lot of effort has gone to trying to understand and combine the different use cases and requirements. From this effort logical and abstract designs and specifications for a TSM was created.

A service and system design was documented and graphically modeled using logical figures and UML. These system models and designs should be verified and validated by the ecosystem and especially TSM creators.

The idea of using multiple different SE types is barely discussed in literature, [24] for instance states that the final design of a TSM will vary depending on the SE choice. This thesis has however proposed that this is to be a necessity in future TSM systems.

8.1 Future work

More work could be done in creating abstract designs. However a more specific implementation design could be investigated into in order to gain more knowledge about a final solution.

The focus in this report has been on MCPA payments and some investigation into value added services. This work could be extended to look at how the designs could be extended in order to also support ticketing and other authorization based service.

A future work could also look into risk and fraud management for a TSM performing MCPA payments.

The design models for a TSM proposed should be evaluated and verified and possibly go through some iterations of changes before moving to an implementation phase.

This thesis has only discussed the TSM side of design and architecture. And it has also been mentioned that the POS would have to change infrastructure to NFC enabled terminals. However a system for an SE issuer controlling the SE keys/a CA also needs to be developed. And the MCPA SP's would also need a system if they are to be the access point for card issuance process. A deeper study on how these systems should work could be studied in a future work.

Discreet Simulation could in a future work including implementation design be done in order to test and validate the system designs in terms of non-functional requirements.

An actual implementation could also be a work in it self. An implementation could also verify and will possibly change the design based on what is learned during the implementation process.

Some work looking into the finance and business operation models and how they affect the architecture could be done in a future work.

A study that interviews, surveys and gathers more data from actual companies and industrial actors for specific markeds(e.g. Norwegian market) could be done. The study could for instance focus on where they are now and what they need to do in order to be part of the ecosystem.

Some more work investigating what data should be exchanged between the different actors should be done.

Finally some works(e.g. Google Wallet) are going towards Cloud based payment solutions meaning that parts of the payment will happen or be stored in the Cloud. Cloud payments could be studied in a future work

8.2 Concluding Remarks

It could be risky to try to create a TSM right now. There are some established variants, but none with a big marked dominance. In order to be successful the TSM should definitely implement support for various scenarios that support system openness and the ecosystem stakeholders should all cooperate on establishing interoperability for instance by taking this report as a basis.

Glossary

FeliCa - Felicity Card A contactless card technology from Sony. Popularly used in Japan and other Asian countries.

Interoperability The ability of two or more systems or components to exchange information

Mobile Commerce Mobile commerce concerns to any business transaction conducted electronically between at least two parties (where one of these use a wireless device) over mobile networks [21].

Mobile wallet A handset application designed to enable a consumer to view and use digital versions of what would typically be found in a physical wallet [27].

NFC Near Field Communication – A short range (typically 4cm) communication technology which is compatible with ISO/IEC 14443 and FeliCa contactless technologies. [27]

NFC tag An NFC device in a fixed location that stores information that can be read by another NFC device [27].

NFC terminal An NFC-compatible device in a fixed location capable of two-way interaction with another NFC device [27]

Open system An open system is a system that is open to all actors or stakeholders that are directly or materially affected by the system to access required functions or data

OTA Managing SE securely and remotely over the air(OTA)

Player Players in the market may be seen as i) partners ii) competitors or iii) market regulators [31].

Secure Domain A dedicated space within the secure element reserved for data related to a specific set of mobile NFC services [27].

Service Manager terminal A Common Infrastructure service whose responsibility is to manage other Common Infrastructure services and Application Components for the life of a session [36].

Trusted service manager Business contractor/connecter service between multiple actors(for instance a business and a consumer) wanting to perform a NFC management process

UICC A Universal Integrated Circuit Card commonly known as a SIM card [27].

Bibliography

[1] Atb nyhet. http://www.nrk.no/nyheter/distrikt/nrk_trondelag/1.8364535, last checked: 9. mars 2013.

[2] Isis webpage. http://www.paywithisis.com/, last checked 10. mars 2013.

[3] Open system architecture. http://www.businessdictionary.com/definition/open-system-architecture.html, last checked 10. mars 2013.

[4] Singapores national nfc service goes live. http://www.nfcworld.com/2012/08/27/317386/singapores-national-nfc-service-goes-live/, last checked 10. mars 2013.

[5] The keys to truly interoperable communications. Published online by NFC Forum, 2007.

[6] Ieee standard glossary. http://www.ieee.org/education_careers/education/standards/standards_glossary.html, March 2010.

[7] Stolpan webpage. www.stolpan.com, last checked: 9. mars 2013, November 2012.

[8] Trustnorway article. http://www.digi.no/903134/norsk-selskap-vil-ta-nfc-markedet, last checked 10. mars 2013, December 2012.

[9] Transfert webpage. http://www.orangemoneyonline.com/, last checked 10. mars 2013, January 2013.

[10] Trustnordics webpage. http://www.trustnordics.com/, last checked 10. mars 2013, January 2013.

[11] Smart Card Alliance. Proximity mobile payments: Leveraging nfc and the contactless financial payments infrastructure. https://www.nacha.org/userfiles/File/The_Internet_Council/Resources/Proximity_Mobile_Payments_200709.pdf, September 2007.

[12] Michael Kristian Gjernes Avila. Smarte betalingsløsninger - hvordan minimere transaksjonskostnadene for betaling av elektronisk tjenester, December 2011.

[13] IEEE Standards Board. Ieee standard glossary of software engineering terminology, September 1990.

[14] Aleksandar Radulović Borko Lepojević, Dejan Simić. Architecture of tsm solutions in systems based on nfc technology. TECHNOLOGY AND INNOVATION MANAGEMENT, 2012.

[15] J. Bravo, R. Hervás, G. Chavira, S.W. Nava, and V. Villarreal. From implicit to touching interaction: Rfid and nfc approaches. In *Human System Interactions, 2008 Conference on*, pages 743–748. IEEE, 2008.

[16] Vedat Coskun Busra Ozdenizci, Kerem Ok. Nfc loyal for enhancing loyalty services through nfc loyal for enhancing loyalty services through near field communication. `http://link.springer.com/content/pdf/10.1007%2Fs11277-012-0556-z`, April 2012.

[17] Vedat COŞKUN Kerem OK Büşra ÖZDENİZCİ, Mehmet AYDIN. Nfc research framework: A literature review. Published in 14th IBIMA Conference, 23-24 June 2010.

[18] Peter De Jong Carl Hewitt. Open systems. `http://dspace.mit.edu/bitstream/handle/1721.1/6370/AIM-691.pdf?sequence=2`, December 1982.

[19] Eric Conderaerts. System openness. `http://www.vubis-smart.com/html/ennewsletter_ed200901_109.htm`, January 2009.

[20] Chris Cox. Trusted service manager: The key to accelerating mobile commerce. `http://www.firstdata.com/downloads/thought-leadership/fd_mobiletsm_whitepaper.pdf`, 2009.

[21] Mildrey Carbonell Jesus Tellez Diego Suarez, Joaquin Torres. A new domain-based payment model for emerging mobile commerce scenarios. 18th International Workshop on Database and Expert Systems Applications, 2007.

[22] S. Dominikus and M. Aigner. mcoupons: An application for near field communication (nfc). In *Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on*, volume 2, pages 421–428. IEEE, 2007.

[23] EPC/GSMA. Epc – gsma trusted service manager service management requirements and specifications. Online: http://www.europeanpaymentscouncil.eu/documents/EPC220-08January 2010.

[24] Mobey forum. Business models for nfc payments, October 2011.

[25] NFC forum. Essentials for successful nfc mobile ecosystem. Published online, October 2008.

[26] Josef Scharinger Gerald Madlmayr, Josef Langer. Managing an nfc ecosystem. 7th International Conference on Mobile Business, 2008.

[27] GSMA. White paper : Mobile nfc in transport. Online 23. October 2012, September 2012.

[28] Peter Henderson. On open systems and openness. `http://pmh-systems.co.uk/OpenSystems/OpenSystems.pdf`, October 2007.

[29] GlobalPlatform Inc. Globalplatform's proposition for nfc mobile: Secure element management and messaging. Published online: `http://www.paymentscardsandmobile.com/research/reports/GlobalPlatform_NFC_Mobile_White_Paper.pdf`, April 2009.

[30] GlobalPlatform Inc. Globalplatform system messaging specification for management of mobile-nfc services. Published online at: http://www.globalplatform.org/, February 2011.

[31] Terje Jensen. Business aspects impacting technical architecture. Teletronikk No. 2, 2009.

[32] Terje Jensen. Technical apects to consider in architecture. Teletronikk No. 2, 2009.

[33] K.S. Kadambi, J. Li, and A.H. Karp. Near-field communication-based secure mobile payment service. In *Proceedings of the 11th international Conference on Electronic Commerce*, pages 142–151. ACM, 2009.

[34] Ryan Kim. Google wallet aspires to hold all your cards and tickets. `http://gigaom.com/2012/08/28/google-wallet-aspires-to-hold-all-your-cards-and-tickets/`, last checked: 9. mars 2013, August 2012.

[35] J. Neefs, F. Schrooyen, J. Doggen, and K. Renckens. Paper ticketing vs. electronic ticketing based on off-line system'tapango'. In *Near Field Communication (NFC), 2010 Second International Workshop on*, pages 3–8. IEEE, 2010.

[36] Mike Ormerod. Defining the openedge® reference architecture - common infrastructure: Service manager. Published online: http://communities.progress.com/pcom/docs/DOC-11118, May 2006.

[37] F. Resatsch, S. Karpischek, U. Sandner, and S. Hamacher. Mobile sales assistant: Nfc for retailers. In *Proceedings of the 9th international conference on Human computer interaction with mobile devices and services*, pages 313–316. ACM, 2007.

[38] J.J. Sánchez-Silos, F.J. Velasco-Arjona, I.L. Ruiz, and MA Gomez-Nieto. An nfc-based solution for discount and loyalty mobile coupons. In *Near Field Communication (NFC), 2012 4th International Workshop on*, pages 45–50. IEEE, 2012.

[39] P. Schoo and M. Paolucci. Do you talk to each poster? security and privacy for interactions with web service by means of contact free tag readings. In *Near Field Com-*

munication, 2009. NFC'09. First International Workshop on, pages 81–86. IEEE, 2009.

[40] StoLPaN. Dynamic management of multi-application secure elements, 2008.

[41] S. Tamrakar, J.E. Ekberg, and N. Asokan. Identity verification schemes for public transport ticketing with nfc phones. In *Proceedings of the sixth ACM workshop on Scalable trusted computing*, pages 37–48. ACM, 2011.

[42] G. Van Damme, K. Wouters, H. Karahan, and B. Preneel. Offline nfc payments with electronic vouchers. In *Proceedings of the 1st ACM workshop on Networking, systems, and applications for mobile handhelds*, pages 25–30. ACM, 2009.

[43] Kerem Ok Vedat Coskun, Busra Ozdenizci. A survey on near field communication (nfc) technology. Published online on 1. Desember 2012, December 2012.

[44] J. Ylinen, M. Koskela, L. Iso-Anttila, and P. Loula. Near field communication network services. In *Digital Society, 2009. ICDS'09. Third International Conference on*, pages 89–93. IEEE, 2009.

Appendix A

NFC forum use cases

In [25] some relevant use cases are detailed and will be directly referenced here.

A.1 Retail: Restaurant

1. Assumption

It is assumed that restaurants in Eric's office building accept payments at Point-of-Sale terminals equipped with NFC reader/writers, and that contactless cards are widely used there. Eric has enabled one or more of his credit/debit card applications in his NFC Mobile Phone.

2. NFC Common Service Flow

Eric pays for his lunch at the restaurant by touching his contactless card or his NFC Mobile Phone to the Point-of-Sale terminal.

3. NFC Mobile Phone Service Flow

The NFC Mobile Phone brings services in addition to those enabled by a contactless card.

• Using his NFC Mobile Phone, Eric chooses which credit/debit card application to pay with, depending on whether his lunch is a business or personal expense.

• He can link to a mobile banking site to check the balance of a credit/debit card prior to making a payment or view his usage/purchase history.

• He can receive messages indicating that the balance of a credit/debit card is low or indicating that a payment to a credit card is due.

• Depending on the transaction amount, Eric may be prompted by the NFC Mobile Phone to authorize the payment. For example, authorizations might range from simple and quick confirmations in the case of lower amounts all the way to special authentication mechanisms such as biometrics for large amounts.

4. Alternative Service Flow

At some point in the future, it may be possible for Eric, as an informal merchant in his spare time, to use his NFC Mobile Phone as a Point-of-Sale terminal to accept contactless payments from his customers' NFC Mobile Phones or contactless cards.

A.2 Retail: Shopping Center

1. Assumption

It is assumed that the growing popularity of NFC Mobile Phones will provide an incentive to retailers to enhance the functionality of their current Point-of-Sale terminals equipped with NFC readers/writers so that they can read coupons from NFC Mobile Phones. It is also assumed that retailers and consumer goods manufacturers will offer a variety of mechanisms to obtain coupons, such as a "push" or "pull" to NFC Mobile Phones, or reading them from conveniently placed smart posters. With this ubiquity of NFC coupons and opportunities to redeem coupons, it is assumed that Eric has downloaded and personalized the required applications on his NFC Mobile Phone.

2. NFC Common Service Flow

Entering a shopping center, Eric makes a purchase in a shop and pays by touching his contactless card or NFC Mobile Phone to a payment terminal.

3. NFC Mobile Phone Service Flow

The NFC Mobile Phone brings more new services to the retail environment.

• Upon entering the shopping center, Eric touches his NFC Mobile Phone to a conveniently located kiosk and

– Receives shopping center loyalty points for returning to the center

– Receives information linking the current coupons on his NFC Mobile Phone to stores within the center offering those consumer goods and possibly additional discounts

– Receives special offers customized to his profile directly to his NFC Mobile Phone

• Walking through the center, Eric notices a smart poster offering him a discount on a product that he has been considering purchasing. Eric touches his NFC Mobile Phone to the poster to retrieve the coupon.Essentials for Successful NFC Mobile Ecosystems 7

• Eric chooses some products to buy in a store, and during the checkout process he touches his NFC Mobile Phone to the Point-of-Sale terminal to:

– Automatically redeem coupons matched to the items he is purchasing

– Make the purchase

– Receive new special offers for future purchases customized to his profile

• Eric can check the history of purchases and remaining loyalty points on his NFC Mobile Phone whenever he wants.

• Users can share information and coupons, where permitted by the coupon issuer, by touching their NFC Mobile Phones together.