Managing Near Field Communication (NFC) Payment Applications through Cloud Computing

A thesis submitted for the degree of Doctor of Philosophy

By

Pardis Pourghomi

Department of Information Systems and Computing,
Brunel University

June **2014**

ABSTRACT

The Near Field Communication (NFC) technology is a short-range radio communication channel which enables users to exchange data between devices. NFC provides a contactless technology for data transmission between smart phones, Personal Computers (PCs), Personal Digital Assistants (PDAs) and such devices. It enables the mobile phone to act as identification and a credit card for customers. However, the NFC chip can act as a reader as well as a card, and also be used to design symmetric protocols. Having several parties involved in NFC ecosystem and not having a common standard affects the security of this technology where all the parties are claiming to have access to client's information (e.g. bank account details).

The dynamic relationships of the parties in an NFC transaction process make them partners in a way that sometimes they share their access permissions on the applications that are running in the service environment. These parties can only access their part of involvement as they are not fully aware of each other's rights and access permissions. The lack of knowledge between involved parties makes the management and ownership of the NFC ecosystem very puzzling. To solve this issue, a security module that is called Secure Element (SE) is designed to be the base of the security for NFC. However, there are still some security issues with SE personalization, management, ownership and architecture that can be exploitable by attackers and delay the adaption of NFC payment technology.

Reorganizing and describing what is required for the success of this technology have motivated us to extend the current NFC ecosystem models to accelerate the development of this business area. One of the technologies that can be used to ensure secure NFC transactions is cloud computing which offers wide range advantages compared to the use of SE as a single entity in an NFC enabled mobile phone. We believe cloud computing can solve many issues in regards to NFC application management. Therefore, in the first contribution of part of this thesis we propose a new payment model called "NFC Cloud Wallet". This model demonstrates a reliable structure of an NFC ecosystem which satisfies the requirements of an NFC payment during the development process in a systematic, manageable, and effective way.

In the rest of this thesis, we design three transaction authentication protocols which execute over the cloud, GSM network and NFC channel respectively. Each of the proposed protocols is an extension of the initially proposed NFC Cloud Wallet model. However, we design each protocol based on a different payment scenario that improves the existing problems which have delayed the adoption of NFC payment technology. Furthermore, the proposed protocols are carefully designed and evaluated against multiple attack scenarios in order to indicate their utility and value from a security viewpoint.

ACKNOWLEDGEMENT

I would not have been able to complete this thesis without the aid and support of the kind people around me. My sincere thanks would go to my supervisor Dr George Ghinea for all his support, time and guidance. This thesis would not be completed without the in-depth discussions and comments from him.

I owe my sincerest gratitude to my parents for their understanding and endless love at all times. They have given me their continuous support throughout, for which my mere expression of thanks does not suffice.

Last, but by no means least, I would also like to convey thanks to all my fellow colleagues, the academic and support staff in the Department of Information Systems and Computing at Brunel University. I am grateful to all of those with whom I have had the pleasure to work with during the course of my Ph.D.

LIST OF PUBLICATIONS

The following papers have been published (or submitted for publication) as a direct result of the research discussed in this thesis:

Journals

1. Pourghomi, P., Saeed, Q. & Ghinea, G (2013) 'A Proposed NFC Payment Application', International Journal of Advanced Computer Science and Applications (IJACSA), Volume. 4 No. 8, pp. 173-181.

2. Pourghomi, P. and Ghinea, G (2013) 'Cloud-based NFC Mobile Payments', Journal of Internet Technology and Secured Transactions (JITST), Vol. 2, Issues 1/2/3/4, pp. 167-175.

3. Grønli, T. M., Pourghomi, P., Ghinea, G (2014) 'Towards NFC Payments using a Lightweight Architecture for the Web of Things', Computing Journal, Springer 1-15.

4. Pourghomi, P. and Ghinea, G 'Mobile Payments over GSM', submitted to: Journal of Electronic Commerce Research (JECR), Springer.

Conferences

1. Pourghoumi, P. and Ghinea, G (2012) 'Managing NFC Payments Applications through Cloud Computing' in *Proceedings of the 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012), London, UK.* IEEE, 2012, pp. 772–777.

2. Pourghoumi, P. and Ghinea, G (2012) 'Challenges of Managing Secure Elements within the NFC Ecosystem' in *Proceedings of the 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012), London, UK.* IEEE, 2012, pp. 720–725.

3. Pourghomi, P. and Ghinea, G (2013) 'Ecosystem Scenarios for Cloud-based NFC Payments', in *Proceedings of the 5th International Conference on Management of Emergent Digital EcoSystems (MEDES), Luxembourg*. ACM, 2013, pp. 113-118.

4. Pourghomi, P., Saeed, Q. & Ghinea, G (Accepted) 'Trusted Integration of Cloud-based NFC Transaction Players', to appear in *the 9th International Conference on Information Assurance and Security (IAS), Tunis, Tunisia*. IEEE.

5. Saeed, M.Q., Pourghomi, P., Walter, C., & Ghinea, G (Accepted) 'Mobile Payments over NFC and GSM', to appear in *the 8th International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM), Rome, Italy*. IARIA XPS Press.

ABBREVIATIONS

Acc_{ID}	Account ID of the customer
AI	Application Issuer
API	Application Programming Interface
App_{ID}	Approval ID. Generated after credit approval
AuC	Authentication Centre
B2B	Business-to-business
C_{r_app}	Credit Approved Message
C_{r_req}	Credit Request Message
CLF	Contactless Front-end
CRM	Customer Relationship Management
DSR	Design Science Research
EMV	Europay, MasterCard and Visa
ETSI	European Telecommunications Standard Institute
FI	Financial Institution
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GSMA	Global System for Mobile Communications Association
HCI	Host controller Interface
HLR	Home Location Register
IaaS	Infrastructure-as-a-Service
ICOM	Issuer Centric Smart Card Ownership Model
ID	Identification
IdP	Identity Provider
IMSI	Internet Mobile Subscriber Identity

IS	Information System
ISDN	Integrated Services Digital Network
ISO	International Organisation for Standardization
K_i	SIM specific key. Stored at a secure location in SIM and at AuC
K_c	$E_{ki}(R)$ using A8 algorithm
K_{c1}	$H(K_c)$. Used for MAC calculation
K_{c2}	$H(K_{c1})$. Encryption key
K_p	Shared key between MNO and shop POS terminal
K_{pr} (2nd protocol)	Private key of MNO
K_{pr} (3rd protocol)	Private key of MTD
K_{pub} (2nd protocol)	Public key of MNO
K_{pub} (3rd protocol)	Public key of MTD
K_{sig} (2nd protocol)	Signing key of MNO
K_{sig} (3rd protocol)	Signing key of MTD
K_{ver} (2nd protocol)	Verification key of MNO
K_{ver} (3rd protocol)	Verification key of MTD
K_1 (2nd protocol)	Encryption key generated by shop
K_1 (3rd protocol)	Encryption key generated by the SIM
K_2 (2nd protocol)	MAC key generated by shop
K_2 (3rd protocol)	MAC key generated by the SIM
K_3	Encryption key generated by shop (the POS)
K_4	MAC key generated by shop
LAI	Local Area Identifier
MNO	Mobile Network Operator
MO	Mobile Operator
MS	Mobile Station

MSC	Mobile Switching Centre
MSISDN	Mobile Station International ISDN Number
MTD	Mobile Transaction Department
MVNO	Mobile Virtual Network Operator
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
OS	Operating System
OTA	Over-The-Air
PC	Personal Computer
PG	Payment Gateway
PI	Payment Information
PIN	Personal Identification Number
PDA	Personal Digital Assistant
PaaS	Platform-as-a-Service
POS	Point Of Sale. Part of shop.
PKI	Public Key Infrastructure
QR	Quick Response
R	Random Number (128 bits) generated by MNO
R_s	Random number generated by SIM (128 bits)
RF	Radio Frequency
RFID	Radio Frequency Identification
SaaS	Software-as-a-Service
SD	Shopping Details
SE	Secure Element
SEI	Secure Element Issuer
SET	Secure Electronic Transaction

SEV	Secure Element Vendor
SIM	Subscriber Identity Module
SMC	Secure Memory Card
SP	Service Provider
SPA	Secure Payment Application
SSO	Single Sign-On
TC	Transaction Counter
TI	Transaction Information
TM_m	Transaction Message for mobile
TM_s	Transaction Message for shop
TMB	Trusted Mobile Base
TMSI	Temporary Mobile Subscriber Identity
TP	Total Price
TRM	Transaction Request Message
T_{SID}	Temporary Shop ID
TS_a	Approval Time Stamp
TS_s	Shop Time Stamp
TS_t	Transaction Time Stamp
TSM	Trusted Service Manager
TSN	Transaction Number
TSU	User's Time Stamp
TTP	Trusted Third Party
UMTS	Universal Mobile Telecommunications System
UCOM	User Centric Smart Card Ownership Model
UICC	Universal Integrated Circuit Card
VLR	Visitor Location Register

VPN	Virtual Private Network

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1 - Introduction

With NFC/ISO 18092, also specified as NFCIP1 (near field communication and transmission protocol), two inductively joined devices functioning at 13.56 MHz can connect through a Radio Frequency (RF) interface and transmission protocol. This technology can be used as a short-range peer-to-peer communication technique that also allows active devices such as PDAs and mobile phones to perform as a reader or a passive token. In this case, these active devices can access Radio Frequency Identification (RFID) application (Mayes & Markantonakis, 2008).

The two entities defined by this standard are referred to as the target and the initiator, and handle two modes of communication: active and passive. The active communication mode provides a channel in which both target and initiator should generate RF field. The process begins with the modulation of the initiator's carrier which should be performed by the initiator itself. Once the modulation is finished, the initiator switches off the carrier and waits for a response from the target. In order to start the communication, the target then switches on its carrier and transmits a response to the initiator.

The passive communication mode operates when the initiator modulates its own carrier and generates an RF field. In this mode, the target is not required to switch on its carrier; instead it acts as a reader while the initiator emulates a passive token (Mayes & Markantonakis, 2008).

1.1 Payment and Ticketing

The main drivers for the creation of the NFC standard have been payment and ticketing applications since the main business parties involved in this technology e.g. financial institutions and Mobile Network Operators (MNO) were interested to place payment and ticketing applications on NFC phones. Visa International's research shows that 89 percent of

people, who tried NFC transactions, prefer phone-based transactions rather than alternative payment methods (Mayes & Markantonakis, 2008). Accordingly, NFC-enabled devices can be used as electronic wallets; that mean that, with the use of payment, ticketing and other applications, people can use their mobile phone to pay for their day to day requirements. Eventually, this can replace debit, credit, loyalty and other countless cards that people carry every day.

Indeed, during the past decade, the concept of contactless card technology has increasingly been used in transport, ticketing and in retail. The technology helps people save time by just holding their contactless cards on a reader in a close proximity instead of having to insert the paper cards in and taking it out of some train entrance gates for example. With NFC technology, mobile phones can have additional functionality, such as acting as a contactless card to be used as an easy method of payment.

Successful development of NFC technology has recently started in some countries where companies offer several services based on contactless card technology and mobile phones. Primarily, NFC-enabled devices are being used in small payment circumstances such as parking meters and vending machines (Innovation Research and Technology, 2011). For example, people can check how much credit is left on their multi-use smart ticket without having to check the ticket machine every time. Thus, when all the NFC infrastructure, security, transaction handling are in place then NFC enabled devices can be used as a proper credit card with a certain amount of payment limit (e.g. £30). However, gathering the required assets in this technology has raised a few issues that are going to be explored in this thesis.

1.1.2 Smart Card Application Management

The applications of NFC technology such as telecom, transport, ID credentialing and banking have been on trial in 38 countries during the last few years (NFC World, 2013a).The Issuer Centric Smart Card Ownership Model (ICOM) (Akram, Markantonakis & Mayes, 2010a) as a traditional model of managing smart card applications has been used on these trials to manage the service applications. In this model, the card issuer, as a centralised authority, is responsible for issuing and controlling the smart cards. Thus, the card issuer has to authorise

the application provider's request to install their applications on the smart cards. The Trusted Service Manager (TSM) architecture provides an extension to the traditional ICOM model in which was deployed in the NFC service trials (GSM Association, 2007; Guaus et. al., 2008). The main purpose of having a TSM in the NFC service architecture is to manage the platform and to authorise the application installation requests from different application providers. Moreover, the TSM can also be responsible for card issuing.

An approach based on the citizen ownership architecture has also been introduced as an alternative to the smart card ownership model. As the term "ownership" implies, in this approach the customers are in a position to decide whether they would like to install or delete applications on their smart cards. However, this was the only authority that was given to customers, and therefore the platform management remains out of their control. The platform itself is responsible for ensuring its reliability and security, which makes it easier in terms of management for application providers since they have the choice not to rely on the trustworthiness of the customer (Akram, Markantonakis & Mayes, 2010b). This approach is named as User Centric Smart Card Ownership Model (UCOM) (Akram, Markantonakis & Mayes, 2010a), and provides an active, pervasive, accessible and open environment.

The Initial Drivers

A debate was prompted by researchers about different types of controls which should be in place to manage the smart cards. This was because the nature of a smart card is to provide security for stored information, and having multiple untrusted applications raises the concerns of both service providers and users. Pierre Girard (1999) stated three different approaches for managing applications in smart cards.

In the first approach, he suggested using a centralized controlling unit as the main and only party to manage smart card applications. This approach was widely developed before deployment of the multi-application smart cards concept, termed as ICOM. This architecture allows an organisation to obtain the smart card from the smart card manufacturer to issue it to different customers. The negotiation then takes place between the application provider and the smart card issuer to discuss the conditions of application installation on the smart card. If the smart card issuer does not authorise the application issuer, the application cannot be

installed on the smart card. The weakness of this model is that customers do not have a choice to decide which applications to install on their smart cards.

In the second approach, Pierre Girard (1999) proposed an architecture in which a customer can play the role of a card issuer, just as in the first model. In this approach, a customer can obtain the smart card from the smart card issuer and then acquires an application (transport, loyalty, ticketing, etc.) from the application issuer to install on his smart card. Although this approach provided decision flexibility for customers, organizations did not consider this model as a serious approach since they cannot fully trust the customer. Moreover, they cannot assure the performance of the smart card platform since customers might have installed malicious applications on the platform.

Lastly, the third approach proposes a model as an extension to the ICOM model. This model, suggests having a certification authority for managing the multi-application environment. The reason which makes this approach an extension to ICOM is that its architecture allows a centralised authority to issue the smart card. However, the application providers cannot negotiate the conditions of application installation procedures with the card issuer, instead they should agree with the principal certification authority to be able to install the applications and perform under the control of the certification authority.

As M'Chirgui (2005) pointed out, the cooperative competition (coopetition) attitude of organizations towards the product and market improved the rapid spread of the smart card industry. The term coopetition refers to the cooperation of two companies towards establishing a market and then their competition to take a larger share than the other company.

Examples of coopetition in the smart card industry are EMV (EMV 4.2, 2008), GlobalPlatform (GlobalPlatform, 2006), and the Java Card (Java Card Platform Specification, 2009) specification. Nevertheless organisations did not follow the coopetition attitude with regards to deployment of multi-application smart cards due to various issues. Some of the issues which prevented organisations from following the coopetotion attitude towards managing multi-application smart cards are mentioned below (Akram, Markantonakis & Mayes, 2010a):

1) Smart Card Control (Ownership)
2) Marketing Potential
3) Customer Loyalty
4) Customer Relationship Management
5) Potential Revenue Source

In the last few years, having to face the above issues in a multi-application smart card environment delayed the adoption of this initiative. However, since other technologies such as NFC, cloud, etc. have become hot topics in the industry, this concept is gaining momentum again.

Renewed Attention!

This section describes a few of the contributing factors which have revived the multi-application initiative in the smart card industry yet again.

One of the most important factors is the existence of NFC technology, which enables a mobile phone to emulate a contactless smart card (ISO/IEC 18092, 2004).This emulation enables the NFC phone to act as a contactless card payment on the current smart card infrastructure, such as contactless POS terminals (Mayes & Markantonakis, 2008). Consequently, merchants are not required to upgrade their smart card service POS infrastructure. The only difference is from a user perspective, since they now use an NFC-enabled device (phone, tablet, etc.) to perform the transaction. From the merchant's perspective, the POS terminal is communicating with a contactless interface which is in the form of a NFC mobile device. Despite what has just been said, and although NFC is on trial in 38 countries (NFC World, 2013a), the wide practical deployment of NFC technology is still in the pipeline, however.

In addition to the NFC technology and its deployment issues, business dynamics have been significantly reshaped by a totally non-relevant area. The concept of "iPhone effect" was introduced to this business sector; this entails customers installing an application on a mobile device. Although this concept was possible with traditional smart card architectures, iPhone however made it easier for both service providers and customers to manage, navigate, search and install third party applications (Laugesen & Yuan, 2010). Additionally, installing an

application on iPhone did not require any negotiation between the application developer and the mobile operator. Moreover, application developers pay a percentage to Apple after they have charged customers for their service. This has enabled Apple to remain in the sales loop and at last, mobile operators are able to offer data usage to clients and make financial profits from data price plans. With the rapid increase of multitude smart phone usage among younger customers, the smart card leading companies have to remain ambitious for introducing new services and control the platform to reduce their investments (i.e. purchasing of new smart cards).

According to the above discussions, the concept of mobile payment can be considered as one of the challenges that the traditional smart card industry has faced recently. For example, there are existing mobile payment applications such as the PayPal app, Starbucks app, etc. that are available to users for download onto their mobile phones, enabling them to make payments for different services. However, companies are still considering alternative payment methods to achieve security, profit and customer satisfaction.

Having new technologies such as cloud computing already developing in the market, we argue that the multi-application smart card model has become mature enough to be treated in the same way as other trustworthy business models. Nonetheless, the combination of several services in a single smart card remains as a natural next step in this business sector. Thus, the level of its success might still be open for debate. In the next section, we describe the challenges which have delayed the adoption of NFC transaction operation.

1.1.3 Challenges of NFC Transaction Operation

Having high security mechanisms as well as minimizing the chances of fraud in NFC payments have always been a major concern for both service providers and customers. In order to improve the security in NFC transactions, having a security controller stored within the NFC device is an essential requirement that can be designed in the form of a Secure Element (SE) (Mayes & Markantonakis, 2008). The key purpose of designing a SE is to provide an attack resistant microcontroller, similar to the chip that can be stored in a high quality smart card. Moreover, the payment application execution is supposed to be carried out

in a secure area within the SE that also stores confidential transaction assets such as transaction information, keys, and transaction application code (Association.G, 2007).
The challenges of NFC transactions are mainly security issues with SE personalization, management, ownership and architecture that can be exploitable by attackers to delay the adaption of NFC within the society. Managing a mobile multi-application environment similar to NFC is very puzzling as there are many parties involved such as Service Providers (SP) and SE Issuers (SEI). Those parties are somehow partners as they have a dynamic relationship within the whole process and they also have limited control on their applications that are running in the service environment. They do not have full knowledge about each other and can only access their part of involvement, which makes the management and ownership of NFC challenging.

One of the main challenges of the new mobile NFC service environment is that current card issuance models cannot support the dynamic post issuance personalization process (Konidala et al., 2012). This is because service providers:

- Have absolutely no control over the SEs on which their applications are stored, except for deciding whether or not to use them
- Have no control over the applications stored in the same SE
- May not know their client personally, or have the opportunity to contact the SE or the user physically

Therefore, there is a need for a common standard applicable to all ecosystem players in order to improve the interaction complexities they may have. Otherwise, isolated solutions will prevail and the technology will be incapable of serving the projected several hundred million users and thousands of service providers (Mayes & Markantonakis, 2008; Kadambi et al., 2009; Morese & Raval, 2008).

Global Platform's Approach

As an independent and non-profit organization which is concerned with smart card development and management, GlobalPlatform introduces a new way of managing the security of each application within the SIM. They have defined a way which guarantees the security and isolation of each application. For instance, a bank can control/be in charge of its

application while the transport operator controls its own mobile ticketing application. On top of that, the MNO will have full control of its mobile service subscription. GlobalPlatform also defines a new model which can be used to add and remove applications in the Subscriber Identity Module (SIM) at any time. The SIM is divided into different domains and each Service Provider (SP) has been given a security domain. Each SP has full control of its own domain and no other SP can access other domains. This security model is necessary for division of responsibilities, roles and accesses especially an NFC ecosystem which contains multiple SPs. Figure 1 illustrates the GlobalPlatform SIM architecture.

Figure 1: GlobalPlatform SIM Architecture (Gemalto, 2011)

1.2 Research Motivations

The SE as a single entity that acts as a controlling party is unable to carry out remote operations within the NFC ecosystem. The remote operations include installation and loading of new applications in an external party, creation of security domains for an external party, as well as activation and personalization of the applications that are loaded on the SE for an external party.

At present, many restrictions and unknown constrains have created problems for the operations of SPs and SEIs in the mobile NFC world. Those restrictions have presented a new approach for business cooperation in which collaboration is essential between unknown parties, and none of the parties are able to influence the service environment substantially. Therefore, a technical solution and a clear framework are required in order to define constant procedures for ecosystem players. These constant procedures improve the interaction of business partners, at the same time making the negotiation and description of each interaction

unnecessary. It also provides easy management and deployment of applications for unknown business partners.

The NFC ecosystem will not succeed without having a clear framework as well as constant procedures. Technical standards and fundamental interoperability are essential to be achieved for industries working with NFC technology in order to establish a positive cooperation in the service environment. Indeed, lack of interoperability in the complex application level of the service environment (Mayes &Markantonakis, 2008) has resulted in the slow adoption of NFC technology within societies. Moreover, the current service applications do not provide a unique solution for the ecosystem. Therefore the service environment does not meet the right conditions (Guaus et. al., 2008). The current situation is that many independent business players are making decisions based on their own benefits which may not be acceptable to other business players. Our goal is to provide a concept for an NFC ecosystem that is technically feasible, is accepted by all parties involved and thus provides a business case for each player in this ecosystem.

1.3 Research Aim and Objectives

The previous section (1.2) has highlighted that there is a considerable number of issues that have delayed the adaption of NFC transactions due to not having a feasible ecosystem that is accepted by all involved parties. Accordingly, the main aim of this research is thus:

To explore the problems with existing NFC transaction ecosystem models, design three novel transaction authentication protocols based on our proposed transaction architectures, and to carry out detailed security analysis of the proposed protocols.

In fulfilling this aim, the following objectives are considered important to be achieved:

Objective 1: To consider the existing NFC transaction models in order to understand the limitations which have been raised regarding the adoption of this technology.

Objective 2: To develop a payment model based on the results and limitations obtained from consideration of the existing models and to propose an ecosystem architecture and its respective authentication protocol so as to indicate the framework's utility and value.

Objective 3: To design and evaluate a novel secure NFC transaction authentication protocol based on our second developed model that proposes a trusted relationship between a single MNO and the merchant in the transaction architecture.

Objective 4: To design and evaluate a novel secure NFC transaction authentication protocol based on our third developed model which proposes a trusted relationship between multiple MNOs and the merchant in order to provide a complete transaction solution based on the second and third models.

1.4 Thesis Structure

The rest of this thesis is structured as follows:

Chapter 2 presents background information on electronic payments, NFC transactions security and its related specifications, as well as examining the role of cloud computing in NFC transactions. In addition, this chapter emphasizes the level of security and manageability in existing NFC payment models while discussing several approaches to evaluate the flexibility in popular NFC transaction ecosystems. Finally, the research challenges section points out the research gaps that this thesis intends to tackle.

Chapter 3 explains the methodology followed to conduct this research. The fundamentals of Design Science Research (DSR) are explained and then justified as an appropriate approach for this research. At the end, different stages of this research are indicated and then discussed in line with the DSR research cycle.

Chapter 4 describes the general idea of our proposed payment model, called NFC Cloud Wallet. This model is a novel cloud-based approach towards managing mobile payment ecosystem using NFC technology. Based on the mentioned model, it then proposes a transaction authentication protocol which provides a secure communication channel to the communication parties. Moreover, it considers the detailed execution of the protocol and justifies the security, validity, and reliability of the protocol by providing a detailed security analysis and expert evaluation of such protocol.

Chapter 5 discusses the NFC transaction ecosystem scenario in which cloud computing plays an important role in the payment architecture and the merchant's POS and MNO do not have a direct communication, as is the case with the first proposed protocol (chapter 4). In this scenario, the merchant's POS and MNO have a trusted relationship and they only communicate through the NFC phone. This chapter also introduces a new insight towards NFC mobile payment frameworks and proposes a secure payment protocol accordingly which executes over the GSM network. In order to justify the security, validity and reliability of the proposed protocol, a detailed security analysis and expert evaluation of the protocol execution is provided and several attack scenarios are discussed.

Chapter 6 proposes a novel cloud-based NFC transaction authentication protocol, which follows the same assumptions as the second protocol, proposed in chapter 5. However, this protocol defines a new concept, which enables the merchant to authenticate with multiple MNOs rather than just one MNO, as is the case with the second proposed protocol in chapter 5. Furthermore, a detailed security analysis and expert evaluation of the protocol is provided to examine its reliability in different real-time attack scenarios.

Chapter 7 provides a summary of the research findings and outlines the research contributions to the knowledge. After all, the limitations of this research are discussed and directions for future research are proposed.

Chapter 2 - Literature Review

2. Overview

In this chapter, the fundamentals of information security will be discussed and an overview of electronic payments will be described. This will be followed by a discussion of the role of cellular phones in electronic payments, which will be taken forward to discuss NFC and payment ecosystems in detail. Accordingly, we will start off by discussing the management issues within the SE architecture, considered to be one the essential components in the NFC payment technology. Having explained the surrounding issues in managing payment applications on the SE, we will add the concept of cloud computing into the discussion and describe its deployment models as well as its security issues. We then consider the importance of cloud computing in NFC payments and describe the ways in which the cloud is able to improve the management issues of the NFC payment ecosystem. Finally, we describe related work proposed by well-known industry stakeholders as well as Chen et al.'s protocol and highlight the existing research challenges, which have delayed the adoption of NFC payments.

2.1 Transaction Security Requirements

In order for a transaction to perform reliably there are a number of requirements that must be met to guarantee the security of information during data transmission in a communication channel. These requirements are confidentiality, integrity, non-repudiation, authentication, authorisation, availability, and privacy. They will now be explained in more detail.

2.1.1 Confidentiality

The concept of information security defines confidentiality as a set of rules which ensures that transmitting information amongst communicating parties are not available to a different

party that aims to gain unauthorised access (O'Neill et al., 2003). These set of rules must meet this requirement when communicating parties need to exchange data in any networked systems and thus ensure that only the expected party is receiving the information. Meaning that security of transmitting information is guaranteed against eavesdroppers, as disclosure of data breaches the confidentiality of the transmitting information (Nakamur, Hada & Neyama, 2002; Geer, 2003). For example, when making online purchases, a customer should provide his credit card details in the merchant's website. The merchant then sends this information to the transaction-processing network. In this case, confidentiality is achieved when data is transmitted in an encrypted format so no unauthorised party or individual can gain access to the transmitting information. One of the approaches that provide confidentiality between communicating parties is the use of a dedicated private line or a Virtual Private Network (VPN) (Rao et al., 2004).

2.1.2 Integrity

Integrity of information is achieved when accuracy and consistency of data is assured during its transmission. This means, transmitting information should not be modified or changed in an unauthorised manner during its transmission (Nakamur, Hada & Neyama, 2002; Geer, 2003). Since preventing unauthorised tampering of information in an un-trusted network (e.g. Internet) is impossible, it is essential to detect the tampering once it occurs. Having the knowledge to detect any data modifications during its transmission fulfils the integrity requirements. Digital signatures are one of the methods used in information security to satisfy the integrity requirements of information (O'Neill et al., 2003).

2.1.3 Non-repudiation

Non-repudiation of the message refers to ensuring the sender and the receiver of the message are the parties who are claiming to have sent and received the message. In this case, neither the sender nor the receiver can deny sending and receiving the message. The integrity and confidentiality of the message will be thrown into question when there is any doubt about the sender or the receiver of the message. Public Key Infrastructure (PKI) and digital signatures are the techniques that are used to ensure that non-repudiation requirements are met (Nakamur, Hada & Neyama, 2002; Geer, 2003).

2.1.4 Authentication

Authentication is the act of identity establishment (Geer, 2003) to provide secure data accesses to those that have suitable proof of identity (Nakamur, Hada & Neyama, 2002). In other words, accessing information is only possible for parties who present suitable proof of identity. For example, when a person goes to a bank to withdrawn money, he introduces himself to the cashier by saying his full name (e.g. David Francis). He is in fact claiming to be David Francis. The cashier should verify his claim by asking for a photo Identification (ID) and checking the information against David's claim. If the provided ID matches David's claim, then the cashier authenticates David that he is who he is claiming to be. There are several methods available for authentication process such as PKI, smart cards, dongles, passwords, biometrics, etc. Having more than one type of authentication (two-factor authentication) provides stronger authentication. Each of the mentioned authentication methods follows the idea of having either a hardware-based or software-based authentication token that is in the possession of an entity and is authenticated.

2.1.5 Authorisation

After the authentication of an entity, its privileges should be determined and the particular resources/services that the entity is permitted and not permitted to access and perform (e.g. view, delete, run, read and write) should be decided. This determination of an authenticated entity's privileges is called authorisation (Yang, 2002; Nakamur, Hada & Neyama, 2002; Geer, 2003). Having passed the authentication process and being authenticated does not necessarily mean that the entity is also authorised. The authorisation process is managed by an administrator that configures the policies and procedures for access controls to determine which resources and services are available for which authenticated users and under what conditions. Role-based access controls and simple file permissions in Windows and other Operating Systems (OS) are very common to use as an authorisation process (O'Neill et al., 2003).

2.1.6 Availability

The term availability in information systems entails that all resources and services that have a role in computing systems should be available when required. This means the computer

systems, the communication channel and other participating resources must be functioning correctly. If not, the resources become useless and companies face financial crisis if the required resources are not available (O'Neill et al., 2003). Some businesses should provide high availability since their resources must remain available 24/7 to provide critical services to customers. This availability should remain active even in the case of hardware failure, system update or power failure.

2.1.7 Privacy

Data privacy can be considered as an additional mechanism to data confidentiality. While data confidentiality prevents eavesdroppers to gain unauthorised access to transmitting data, data privacy is concerned about the privacy rights of the subject of the data. This means that in data transmission, although strong encryption mechanisms are in place, there might be a back door available for intruders while data are being stored in a database. Data privacy assures that data is protected at all times (O'Neill et al., 2003).

This section described the core principles of information security that also plays an essential role in online payments. In the following section we will discuss the concept of electronic payments in order to better understand the key issues of this payment method. This will be followed by a consideration about the role of cellular phones in e-payments that is discussed in section 2.3.

2.2 E-payment

Electronic payment (e-payment) refers to the use of electronic means for making a payment from the payer (customer) to the payee (merchant). With e-payment systems the purpose of real payment scenarios is implemented in a virtual world. Due to the widespread use of Internet, e-payments have become very popular (Tsiakis & Sthephanides, 2005).

The e-payment system consists of at least four participating parties. They are payer, payee, an issuer and an acquirer. The issuer and the acquirer are considered as third parties in whom the issuer processes the payer's transaction (e.g. customer's bank) and the acquirer processes the payee's transactions (e.g. merchant's bank). "Cash-like" and "cheque-like" e-payments systems are two models of e-payment systems which have been identified by Asokan, Janson, Steiner and Waidner (1997). The "Cash-like" model is similar to the real cash payment

scenario where both payer and payee exchange money directly and without the involvement of their banks. However, in the cheque-like model, both payer and payee do need to have an issuer (bank account) either in the same bank or in different banks. Therefore, their banks are involved in order to process their transaction.

In the "cash-like" model, when a person intends to make an online purchase, before making the online payment over the Internet, he withdraws the money from his bank account. Then when he makes the online payment, he uses the money that has been withdrawn previously and sends it to the payee. The payee's acquirer then deposits and settles the money from the issuer (Asokan et al., 1997)

In the "cheque-like" model, the payee needs to have a bank account as well as a debit or a credit card in order to make online payments. A debit card can be described as an electronic readable card which stores the unique payment credentials of the payer and deposits the available money from the payer bank account. A credit card stores the same information, but when a payer decides to make a payment, he has to borrow the money from the issuer (credit company), which provided the credit card and should pay the money back to the same company later. The summary of the credit card e-payment system is as follows (Turban et al., 2004). After completion of the online payment form by the payer (customer), the page is transmitted to the payee (merchant). Then the acquirer receives the payer's credit card information as well as the payee's identification number. In order to approve the payer's credit card information, the acquirer sends the information to the payer's credit card issuer. Consequently, the payer's credit card company responds back to the acquirer's request stating whether or not the credit card information is approved. The card issuer then sends the result of this process all the way back to the payer (customer) to update him/her of his/her card statements. Figure 2 shows the money flow in the credit/debit card e-payment system.

The payer's credit card information can be entered in three different methods (Wright, 2002). Similar to the above mentioned method, the payer's credit card information can be entered into the online form that is provided by the payee. In this case, the payee receives the payer's credit card information and stores it in its database.

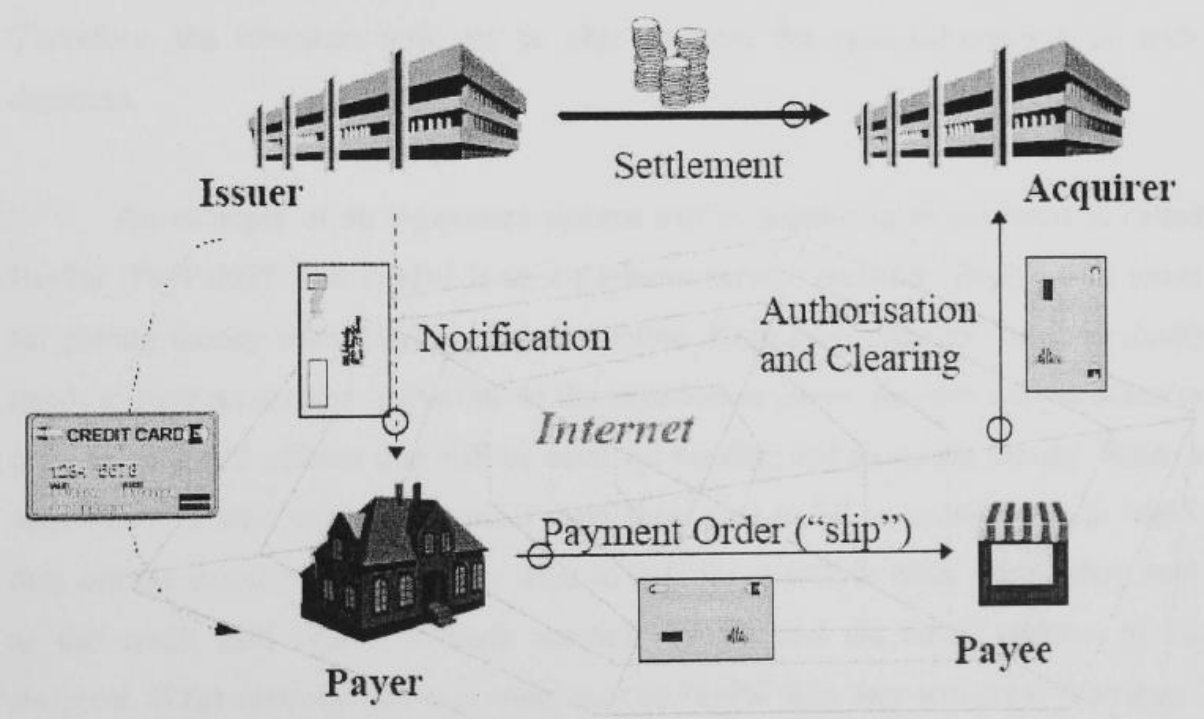

Figure 2: Money Flow in Credit/debit Card-based E-payment Systems
(Asokan et al., 1997)

In this method, hackers may gain unauthorised access to the merchant's database where the customers' credentials are stored, as was the case in 2007, when attackers hacked into the "TK Maxx" database and stole the details of 45.7 million debit and credit cards (BBC News, 2007).

The second method of entering the payment card details is to complete the form that is provided by a payment service provider. The payment service provider's role is to provide e-payment services for payees (merchants) and is not the merchant itself. PayPal is a good example of the e-payment service provider. In this method, the payer's credentials are not available to payees and accordingly are not stored in the merchants' database like in the first method.

Using a Secure Electronic Transaction (SET) is the third method that a payer can follow to enter his card details. This method facilitates the process where the payer's card details are encrypted by its issuer's public key. Then the encrypted card details are sent to the payee (merchant) who in turn sends it to the acquirer. Since the card details are encrypted, the

merchant cannot read the information. Subsequently, the merchant cannot store those details in its database.

PayPal is an example of an e-payment system provider that has become very popular in recent years (PayPal, 2013; Kauffman et al., 2013). Users register with PayPal and provide an email address to be able to use the e-payment system. Either to pay or to receive money, both payers (customers) and payees (merchants) must have an account with PayPal. In order to send money, a payer should complete a form which requires his credit/debit card or his bank account details as well as the amount of the money which needs to be transferred. The payer is also required to provide the email address of the recipient in order to specify where the money is reaching to. The recipient receives the transferred amount as well as the confirmation email if it is a registered user of PayPal. In this case, the recipient should login to his account in order to find the money. However, if the recipient is not registered with PayPal, he will have to register and create an account in order to receive the money. Registered users of PayPal are able to withdraw money either by requesting PayPal to deposit the required amount into their bank accounts or by asking PayPal to send them a cheque. Users are also able to transfer the available money from their accounts to the accounts of other PayPal users (Jones, 2001; Guadamuz, 2003).

The payer's credit/debit card details as well as their bank account information are not available to payees and PayPal is the only party who can view and process the payer's credentials (PayPal, 2013). This method provides privacy protection for payers from distributed payees and encourages them to use such e-payment service.

The major concerns regarding the security of user credentials in e-payment systems are the communication channel which transfers the payment credentials as well as the database that stores the credentials (Hsieh, 2001; Wright, 2002). Indeed, security has always been the major concern of all involved parties in an e-payment system especially to customers. For this reason, some of the customers prefer to be unknown to merchants, which prevent merchants from building a record of their customers' purchases.

2.3 Cellular Phones for E- payments

This section discusses the idea of using cellular phones in e-payments. The discussion is based on identity attributes and describes the related work that has been developed in the mobile identity management industry.

The popularity of the Internet and other high-speed data networks in combination with the attractiveness of smart phones have increased the interest of companies to invest in the concept of mobile wallet (Mjolsnes & Rong, 2001; Boly et al., 1994). CWI Amsterdam was one of the first companies in Europe which carried out two distinct projects to combine digital cash and mobile telephones. The first project investigated mobile device authentication, while the other was based on Chaum's online digital payment protocols (Chaum, 1985). The aim of both projects was to use Global System for Mobile Communication (GSM) (Rannenberg, 2004) to act as an electronic wallet for payers in order to connect to the bank and payee. Subsequently, this idea was extended to another scheme, which was part of the European CAFÉ e-commerce project (Boly et al., 1994). The goal of this extended work was to propose the concept of wallets with observers (Chaum, 1985) in order to enable credentials and off-line digital cash to be used in commercial settings.

Although the results of the European CAFÉ project were never implemented in combination with cellular networks, electronic wallet technology was developed as an outcome of this project. The developed electronic wallet technology had the potential to perform the transactions based on a short-range infrared link that could directly connect to wallets held by individuals as well as connecting to compliant cash registers. However, the transaction could also be performed over the Internet to other SPs. During the off-line transaction, an observer that is trusted by the credential issuer protects the credential issuer's interests. The observer also uses the credentials on behalf of the issuer and controls copying of the credentials. An off-line transaction is carried out when the payer (credential holder) and the payee (credential verifier) are not connected to any supplementary services. In this scenario, the service is trusted by the payer. While the result of European CAFÉ project did not demonstrate the ability of electronic wallets to perform transactions in combination with GSM networks, it was a significant step towards improving the mobile wallet technology.

Valista (Hennsey, 2003) is another company that follows the mobile wallet approach and introduces a new service which supports secure payments, user identity verification and personalization. Their system works based on a provider-centric model in which a hosted server such as Identity Provider (IdP) acts as a central database for storing customers' wallet information and can be accessed from the user's mobile device. Valista wallet service meets the requirements of main security standards such as Visa Mobile 3-D Secure and MasterCard's Secure Payment Application (SPA). The fast acceptance of second generation mobile communication systems made an enormous influence on increasing the essence of mobile identity services which led to the rapid development of mobile commerce (m-commerce) services (Jendricke et al., 2002; Rannenberg, 2004). The two main factors that have a direct effect on the growth of m-commerce services are usability and trust. For this reason, several approaches have been proposed in order to enhance usability in mobile devices (Dix et al., 2000). On the other hand, confidentiality, integrity, user control and minimal disclosure of the sensitive data are the key issues in the perception of trust on mobile devices. GSM-based IdM (Rannenberg, 2004) is one of the approaches that use SIM and the GSM infrastructure as the fundamental platform. This approach has several benefits, however the number of managed identity attributes is very restricted since they are only related to the GSM infrastructure and the SIM hardware.

2.4 NFC & NFC Ecosystem

This section describes the functions of adding contact-less card features to mobile phones in order to produce an intelligent device that enables us to make payments with. The intelligent device is called an NFC mobile phone (Francis et al, 2010). We thus describe the roles of the parties involved in an NFC transaction so that the responsibilities of each party are clarified.

A. NFC Transmission Classification

Based on the ISO/IEC 18092 NFC IP-1 and ISO/IEC 14443 contactless smart card standards, in an NFC transmission, there are three different modes of operation namely read/write, peer-to-peer, and card emulation (NFC Forum, 2013; Desai & Shajan, 2012).

- The read/write mode enables the NFC device to read the NFC forum mandated tag types (i.e. a tag embedded in a smart poster). This mode of operation on the RF interface is supported by the ISO 14443 and FeliCa schemes.

- According to the NFCIP-1 and LLCP standards, the peer-to-peer mode of operation enables two NFC devices to communicate directly for transferring information such as an SMS, contact numbers, etc. The NFCIP-1 that allows the initiator – target model, requires the target and the initiator to be defined before the communication initiates. The connection decision is made by the application that operates in the application layer only once the initial handshake is completed. In this mode, both the mobile device and the tag are in the active mode enabling data to be sent over a half-duplex channel which means when one device is transmitting data, the other waits until the transmission is finished and then starts to transmit data (Desai & Shajan, 2012).

- The card emulation mode provides a similar kind of environment as a traditional smart card for the NFC device. Additionally, this approach eliminates the need for changing the current infrastructure.

B. Ecosystem

As defined by the Smart Card Alliance Mobile and NFC (2012), an NFC payment ecosystem consists of all the involved parties in the transaction process in order to provide the required services. This can be from a mobile device, merchant's POS terminal, and mobile network operator to trusted service manager and acquirer that is responsible for clearing and settling payments.

When different functions of a mobile phone combine with the functions of contact-less cards, the results of this combination will have a greater significance than just the importance of adding two devices together. This significance defines the NFC-enabled mobile phone which can connect with another NFC-enabled device (i.e. PDA, tablets, etc.) in a short range

communication channel (Hang et al., 2010). NFC technology enables users to benefit from new and countless services on a daily basis where they can pay for their food, buy a cinema ticket by scanning their phone on a movie poster and much more. This newly developed intelligent device is proposed as an all-in-one personal device that can be personalized and used in a highly interactive environment (Madlmayr et al., 2008). Figure 3 demonstrates the concept of the NFC mobile phone (NFC Forum, 2008).

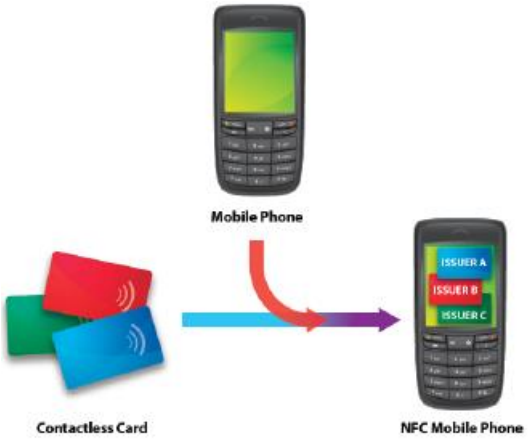

Figure 3: The Concept of NFC Mobile Phone (NFC Forum, 2008)

The success of the NFC mobile ecosystem is based on the relationships between the involved parties, where those relationships have to be clearly defined (Kadambi et al., 2009). The present contactless ecosystem models functionalities can be extended by a well-defined NFC ecosystem which improves the number of functionalities that an involved party can provide. Table 1 describes the key functionalities of NFC ecosystem (NFC Forum, 2008).

Since several components are required in an NFC payment service, different business sectors are also needed to control their part of involvement within the NFC ecosystem. All business parties have realized that, in order to provide NFC payment services to consumers, all parties have to collaborate and it is not possible to provide the service only by a single firm. Although the standardization of NFC has been started from the technical point of view (Schamberger et al., 2013), the adoption of NFC has been slower than expected. Not having a clear structure and slow development of NFC ecosystem among participating industries are the main reasons for the slow take-off of this technology.

Table 1: Key Functionalities of NFC Ecosystem

Key functionalities	Description
Service provisioning	It provides authentication and remote user management due to network availability. Also users can subscribe and personalize their contactless cards
Mobile network provisioning	It offers user authentication and user care for data connectivity as well as ensuring that the network infrastructure is maintained to enable users to receive data connectivity service
Trusted Service Manager (TSM)	Delivers a communication platform between Service Providers (SPs) and NFC mobile phones where SPs provide multi-application management functionalities to NFC enabled mobile phone through this platform

Additionally, a business model that could benefit all participants has not yet been sustained. Figure 4 illustrates the generic model for the NFC payment ecosystem that is proposed by the Mobey forum (2011) in which the SE issuer is the MNO. In some cases such as the Mobey forum's model, one player can have more than one role. This makes the ecosystem more flexible in terms of manageability, control, ownership and personalization of NFC transactions.

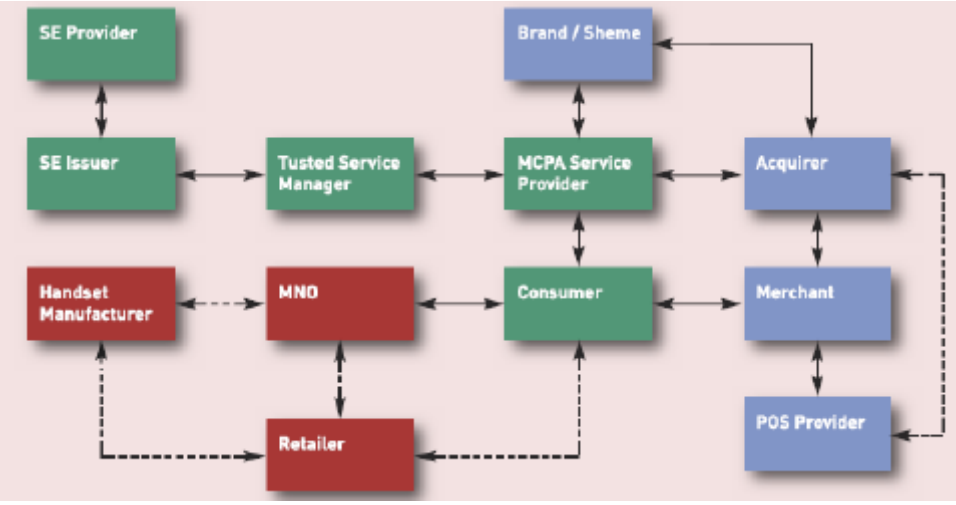

Figure 4: NFC Ecosystem - UICC as SE (Mobey Forum, 2011)

2.4.1 Security in NFC Ecosystem

The cooperation between the involved parties plays an important role when it comes to security in an NFC payment ecosystem. A secure, tamper resistant component, such as SE is required to store confidential payment assets for transaction execution. The responsibilities and access rights of each involved party must be clearly defined in order to ensure secure storage and transmission of sensitive customers' information. Therefore, managing the SE as a crucial component in an NFC payment ecosystem has become the main concern of researchers.

In order for the operating system to handle the above mentioned issues, it should be able to manage and personalize a number of applications that several SPs preferably provide Over-The-Air (OTA). Although some solutions are currently available and researchers are proposing new models for defining the ownership and control of the SE in the NFC payment ecosystem, however this may still result in a business advantage as there is a lack of finalized procedures/standards for all companies to follow. In spite of the location of SE (either in a mobile device or a cloud environment) in the context of NFC transactions, SE provides protection storage for transaction assets such as keys, transaction application code and transaction data. Universal Integrated Circuit Card (UICC) is one of the most reliable components to act as an SE in the NFC architecture. It is removable, provides the same security as a smartcard, can run multiple applications issued by multiple providers, it is compliant with all smart card standards and supports GSM and Universal Mobile Telecommunications System (UMTS) networks. According to Global System for Mobile Communications Association (GSMA) guidelines, UICC is the most appropriate type of SE in NFC mobile transactions (Bender et al., 2011). We will provide a detailed discussion of the SE and its different architectures in section 2.5 of this chapter.

2.4.2 Stakeholders

To understand the business dynamics of the ecosystems discussed in this chapter, this section defines the roles of involved parties in the NFC ecosystem (Stolplan, 2011; Madlmayr et al, 2008; NFC Forum, 2008). The complete scenario cannot be performed without roles; however one single player may assume more than one role in the process.

Consumer: The party who is considered as the end user in an NFC ecosystem. Basically, the consumer is the user of the service who registers his credit card details with the service provider. He is responsible for initiating payment requests and agreements.

Merchant: Is considered as the consumer matching part. The merchant offers products and services to consumers and decides which payment options the consumer can use to make a payment.

Secure Element issuer (SEI): Is the party that issues the SE in NFC ecosystem. It is also controlling the SE in which it decides how the storage of an SE should be used. SE issuer has a crucial role as it is in charge of the SE keys. In our case, the SEI is the MNO, as shall be described later in this thesis.

Secure Element provider: The SE provider is the manufacturer of the SE. It has a direct relationship with SE issuer which is the MNO in our case.

Service Provider (SP): Is the party that issues the payment application and deploys data element to the consumer. SP is also responsible for managing the payment application which is stored on the SE. Examples of SPs include transport operators with ticketing applications, financial institutions, retailers with loyalty applications, etc.

.

Application Issuer (AI): Provides the application which implements and fulfils the business requirements of smart cards SPs. It can guarantee secure interoperability between the card and the card-acceptance device. Sometimes the SP is the application issuer.

Mobile Network Operator (MNO): Is one of the highly active participants in the NFC ecosystem that is responsible for providing the GSM network for data transmission purposes. It also deals with life cycle management of the NFC ecosystem as well as data provisioning Over-The-Air (OTA). In our proposed ecosystem scenarios (chapter 4) the MNO is the SE issuer because the UICC is the SE.

Trusted Service Manager (TSM): The role of the TSM is to integrate several SEs and SPs. Depending on the ecosystem architecture, an SP may decide to increase the services that it

offers by participating in new mode of operation. This conflict is solved by the TSM since it offers a trusted platform that can solve the inefficiency and complexity of multiple agreements.

Acquirer: The role of the acquirer is handling financial payments by clearing and settling transactions through financial institutions.

Over-The-Air (OTA) Provider: Is a secure service which provides data transfer between the SE and the back-offline database. The database can be in the form of a cloud which can be managed by the SP (SP is the cloud owner).

At present, SP and SE issuers are facing many unknown constraints in their current operations. This indicates that none of the involved parties in an NFC ecosystem can influence the service environment individually. Therefore, cooperation is required among unknown parties in order to build a clear partnership to deliver NFC payments. Rather than cooperation, a clear logistical framework is also required to define rules and procedures for the involved parties to follow. This approach avoids the negotiations between parties therefore they do not need to describe every detail of each interaction. This also makes the previous unknown partners understand the application execution procedures and their management. Not having a standardized and transparent ecosystem model with unclear procedures will not succeed and will result in an unsatisfactory business model which is not able to provide valuable services for consumers. Figure 5 demonstrates a business ecosystem model for NFC payments that is proposed by Stolplan (2011). This model suggests using a TSM as a backbone for integrating different SPs and SEIs. However this is the view of Stolpan towards managing the payment ecosystem and it may not be of interest to other involved parties.

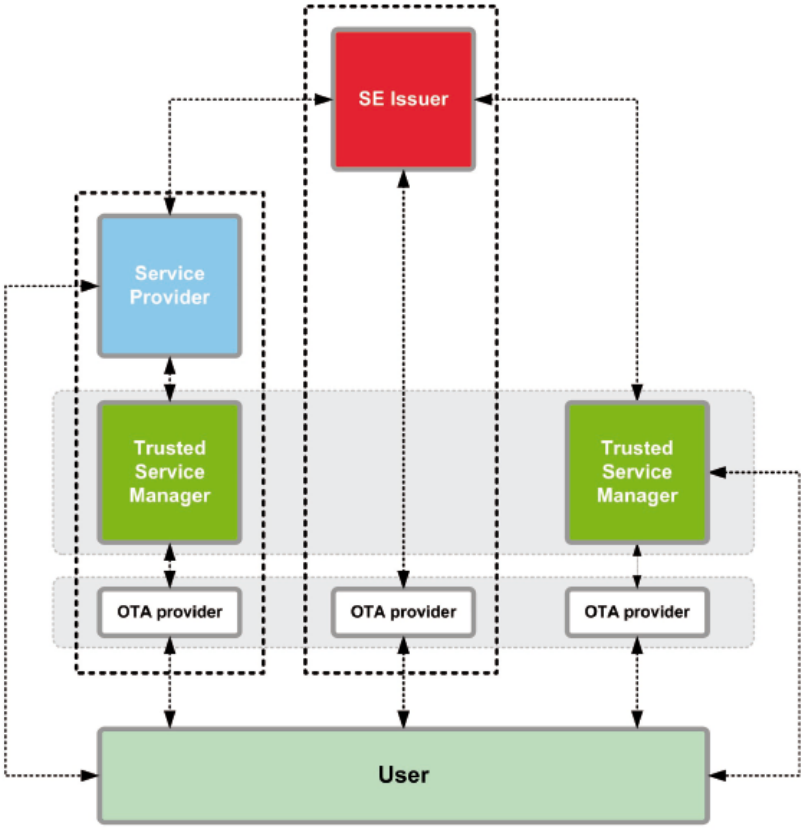

Figure 5: Stakeholders Roles in an NFC Environment

Since the SE plays a crucial role in NFC payments, in the following section we will provide a broad discussion on SE in the payment ecosystem, evaluate different SE architectures within a mobile device, describe the SE lifecycle and consider the SE management issues.

2.5 Secure Element (SE)

Having to ensure secure NFC payments is a necessity which is supposed to be provided by a security controller, normally in the form of an SE (Mayes & Markantonakis, 2008). The SE is intended as an attack resistant microcontroller, rather like the chip found in a good quality smart card. In addition, the SE includes a combination of hardware, software, interfaces and protocols embedded in a mobile handset that enables secure storage (Choudhary & Rissiko, 2006; Francis et al., 2010). Selected by the user during card emulation mode, the SE provides a secure area for the execution of the applications and protection of the payment assets (e.g. payment data, keys, and the payment application code) (Association, 2007; Choudhary & Rissiko, 2006; Francis et al., 2010).

Besides being used for payment applications, the SE can also be involved in the authentication process and can be used for storing applications not related to payments, which nonetheless require security mechanisms. However since the SE is essential in NFC transactions and ownership/control of it may yield commercial or strategic advantage, various solutions have been prompted which will be discussed later on in this chapter. Although different secure element alternatives are currently analysed by the NFC stakeholders, we describe the four main types in this section. First classified by their ability of being removable from the handset or not, they are then categorized by the following criteria: security, reusability and standardization progress.

Baseband processor and embedded hardware alternatives which are non-removable secure element based alternatives are outlined first. This will be followed by removable secure element based alternatives: Secure Memory Card (SMC) and Universal Integrated Circuit Card (UICC) (Alpar et al., 2012).

2.5.1 Baseband Processor

The baseband processor, one of the most important components in a cell phone, handles cell phone connectivity and manages application operation. Providing a high level of security, the SE can be hosted by the secure memory of the baseband. Thus, the handset architecture does not have to be modified. Moreover, such a SE alternative exempts the user from having to insert an additional hardware into his/her cell phone to use security services providing by the secure element. However, as soon as the cell phone is lost, broken or exchanged, the SE must be changed, precluding it from being reusable in another handset (Reveilhac & Pasquet, 2009).

2.5.2 Embedded Hardware

In the embedded hardware case, the SE is a smartcard soldered onto the mobile phone and cannot be removed. Thus, the level of security provided by the SE is as high as the one supported by a smartcard. Nevertheless, this chip, embedded onto the mobile phone during manufacturing stage, must be personalized after the device is delivered to the end user (EMVCo, 2007). This implies the design of a new secured personalization process and indirectly an increase of the cell phone's price for customer. Soldered onto the handset, the

SE chip can't be used in another cell phone. It has to be replaced and personalized every time the user changes his/her handset. Although the SE is compliant with all the smartcard standards (EMV, Java card, etc.), the communication between the NFC controller and this dedicated hardware is not standardized yet, only proprietary protocols can be used up to now. Figure 6 illustrates the SE alternatives.

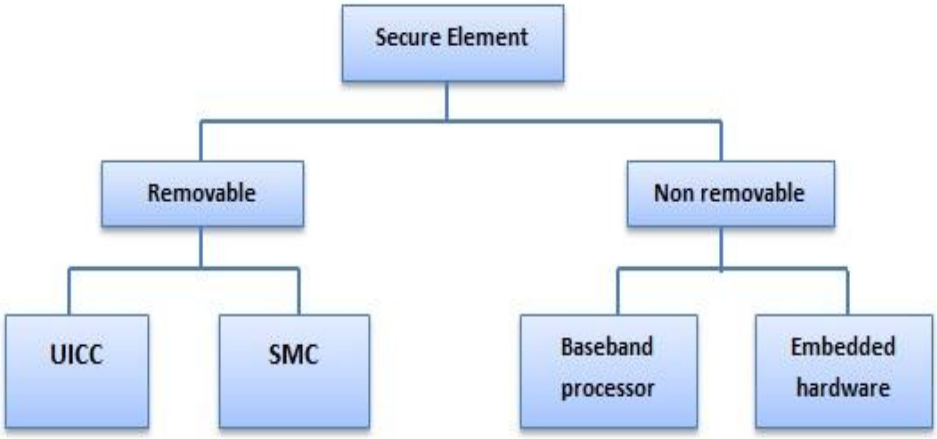

Figure 6: SE Alternatives (Reveilhac & Pasquet, 2009)

2.5.3 Secure Memory Card (SMC)

A removable SMC is made up of memory, embedded smartcard element and smartcard controller. In other words, it is a combination of a memory card (e.g. MMC, SD, etc.) and a smartcard (Choudhary, B. 2006). Thereby, a SMC provides the same high level of security as a smartcard and is compliant with most of the main standard, interfaces and environment for smartcards (e.g. EMV, Global Platform, ISOc 7816, Javacard, etc.).

Removable and having a large capacity memory, the SMC can host a large number of applications in it and does not need to be reissued when the customer buys a new cell phone. The SMC can be inserted in any device supporting NFC technology and is not limited to mobile devices. However, up to now, the communication between the SMC and the NFC controller have not been standardized yet and only a few number of such a chip are currently available (e.g. in September 2008, only one NFC-enabled cell phone supports SMC).

2.5.4 Universal Integrated Circuit Card (UICC)

A Universal Integrated Circuit Card (UICC) is a removable smartcard inserted in a handset. Initially thought to replace the SIM card, the UICC gives access to GSM as well as to UMTS network. As a smartcard, it is compliant with all smartcard standards, is as secure as a smartcard and can host multiple application issued by multiple application providers. Consequently, UICC can host GSM/UMTS applications such as SIM and (U)SIM applications as well as non-telecom applications such as payment applications, loyalty, ticketing, e-passport, etc. (Guaus, J. 2008; Mobey Forum, 2009). Originally designed for mobile networks, the use of UICC as SE, unlike the SMC alternative, is at that time limited to mobile terminal utilization. Since 2007, the standardization of protocols allowing the use of UICC as the secure element is on track. In October 2007, the European Telecommunications Standard Institute (ETSI) approved the Single Wire Protocol (SWP) as a standard defining the physical layer as well as the data link between the UICC and the contactless frontend (CLF) (embedded onto the NFC controller). A few months later, in February 2008, this first standard was completed with the ETSI's approval of the Host Controller Interface (HCI). This interface, one of the most important for NFC, is the software layer that runs on top of the SWP. It defines specific commands to create gates, pipes and registries, allowing CLF and UICC to communicate together. Table 2 evaluates the SE alternatives discussed above (Reveilhac & Pasquet, 2009).

Table 2: SE Alternatives Evaluation

Criteria / SE Alternatives	Security	Reusability	Standardization	Total
Baseband processor	+	-	-	-
Embedded hardware	++	-	+	++
SMC	+	++	+	++++
UICC	++	+	++	+++++

2.6 SE Lifecycle

As noted by Madlmayr, Langer and Scharinger (2008), the lifecycle of an SE contains initialization, activation, application upload and deactivation. The explanations of these steps are described in what follows.

The **Initialization** of an SE can be completed by different SEIs such as credit card companies, Mobile Network Operator (MNO), financial institution or retailers. The SEI can also act as a platform provider. If the SE does not contain any applications when issued, that means there is no platform manager assigned to that SE. A platform manager cannot deal with SE applications without having different certifications (i.e. Visa PayWave certification). These certifications are provided by the SP.

In most cases, the assignment of platform managers is dependent on the installation of the first application. Any party that installs the first application on the SE will be assigned as a first platform manager. However, the SE can also be managed by other AIs. The SE can be issued by pre-installed applications that can be provided by SP, which means the SE is already under the control of SP as its platform manager.

The **Activation** process takes place when the SE is inserted into the phone. The SE then signs in to the NFC controller and it sends a confirmation message to the platform manager in order to inform the platform manager of the successful insertion of the SE in the phone. The platform manager then sends a confirmation message to the mobile phone in order to activate the SE. The platform manager is the only party that has the authority to hold the SE keys for data configuration purposes. The NFC controller's identifier is also stored in the SE to inform SE in case if it was inserted into another phone.

During phase 1 of the **Applications Upload** process, the SP (in this case also the AI) contacts the MNO, the only party who is in charge of the Mobile Station International ISDN Number (MSISDN). The only way to classify the external party for an OTA transaction with the NFC phone is the MSISDN.

In phase 2, the MNO forwards the SP request to the platform manager (s) in charge of the SE. If there is no SE in the phone, the MNO will inform the SP concerning this issue.
In this case the application upload process terminates. However, if the platform manager is positive with the request, it will send an offer directly to the SP to upload its application.
In the next phase, the SP selects one platform manager amongst others (if more than one platform manager exists) to load data to the security domain area which is under the control of the same platform manager.

The application data passes through a secure channel to reach the security domain for application personalization purposes. If the handset is logged in to the network, the SP has no problems in terms of alteration and deletion of data stored in the security domain.
Having security domains ensures the privacy of each security domain in a way that different SPs will only have access to their own space within a specific security domain.

The **Deactivation** procedures are also managed by the platform manager where it can deactivate the SE, OTA in the case of theft or loss. If the SE is installed in a new device, then the activation process should be renewed and the platform manager is the only party that should confirm the activation process to enable the SE to be used for contactless transactions.

The above description is dependent on the multi-host interface implementation that is not standardized yet. Accordingly, a control instance is required in order to control the SEs within the handset. Currently, there is only one control instance for the whole phone and not individual control instances for individual SEs.

The control instance is responsible for establishing a direct communication between the NFC controller and the SIM through the SWP (GSM Association, 2011). It also deals with the communication between the NFC phone and MNO and routes the communication. While SEs only act as a tamper-resistant data containers this communication channel is required to establish data channels and also to send short messages.

2.7 SE Management Issues

Although mobile devices are increasingly becoming a tool for ID recording, however not having standardized procedures for managing an SE has raised several legal questions and uncertainties for companies aiming to use mobile devices for IDs (Coskun et. al.; Madlmayr et al., 2008). Since critical transaction data are stored on the SE, managing and controlling the SE also has several issues with NFC technology. For instance, in the case of identity checks and payment technology options, users' choices cannot be dependent on the handsets they buy. Thus, most probably the MNO will decide which services the customers can use in identity checks and payment services (Madlmayr et al., 2008; Benyo et al, 2007). There are still several legal questions concerning the ownership and control of an SE such as: which

party has the authority to decide what services customers can access? Which party is responsible when customer authentication fails? Having different SE owners in service operation results in potential failure transfer responsibility to other involved parties. The rest of this section provides broad discussion on SE management issues.

2.7.1 Traditional Card Issuance and Management

In the traditional issuance process of contact and contactless cards, the card environment and the services loaded onto them are well specified and known in advance. The whole technical and logistical process is strictly controlled. Usually, it is not possible or even necessary to manage card content throughout the card's lifecycle. After the card is distributed, the SP typically loses any control over it.

In today's multi-application environment, the applications and their SPs are known to each other: card management and all commercial issues are contractually regulated well in advance. The stored applications and SPs involved are usually static, and will not change during the card's life cycle. Technically the cards do allow content download after issuance, but this is rarely done. Examples of contact and contactless services on traditional cards are those provided by public transportation companies, or banks with diverse payment methods.

2.7.2 Card Issuance – Complexity of the Mobile NFC Ecosystem

The service environment which runs the NFC payment operation deals with a number of complex issues which need to be clear before service operation. For instance, several SPs may decide to place their applications on the SE in mobile handsets. The SE is an external condition for all SPs. This means that the technical constraints of the SE cannot be compromised. Having multiple card issuers can also raise issues such as card personalisation and ownership as well as access privileges to user information. The mobility of customers also makes the service environment more complex as customers may wish to use the services in different countries. In this case, the SPs should widen their infrastructure in order to provide global services. However, international companies may prefer to follow standardized procedures for application deployment and payment operation to avoid following new payment procedures in every particular market. Furthermore, customers may decide to add and/or delete the services which they receive from their SPs. Having specific requirements in

each service application does not solve the problem when it comes to application installation and deployment since they all should share the same SE in a mobile device (Benyo et al., 2007).

In the mobile NFC world, there are many constraints unknown to either SPs or SE issuers in their current operations. The NFC ecosystem presents a new way of doing business in which no-one can substantially influence the service environment, and cooperation is necessary between even unknown partners. A transparent logistical model and a technical solution are needed that can ensure uniform procedures for the parties involved. This makes it unnecessary to negotiate and describe the details of each and every interaction, and allow even previously unknown business partners to seamlessly realize the procedures for application deployment and management. Without such an approach the NFC ecosystem will not prevail, resulting in an unsatisfactory business model that is unable to provide user-friendly, valuable services for customers.

2.7.3 Need for Interoperability

Industries working with NFC technology are striving to achieve technical standards and interoperability at the basic, underlying technology level (Widmann et al., 2012; Kanniaine, 2010). At least the same level of interoperability needs to be achieved on the more complex application level too, where it is still missing. The present environment with proprietary service applications, unique logistical solutions do not provide the right conditions. For services and applications there are many independent players involved. Their decisions are primarily driven by considerations that are not NFC specific, therefore they only accept transparent, financially sound solutions.

2.7.4 Service Distribution

There are several players involved in the NFC value chain, however their roles and the form of their cooperation are poorly defined (Widmann et al., 2012). This means distributing any NFC service application requires special, individual agreements between the partners involved. With relationships ill-defined, SPs face new logistical challenges every time their application is loaded onto their users' SEs.

This section evaluated the role of SE from different perspectives; in the next, we will continue by considering the integration of roles within ecosystem players and discuss the SE issuance process.

2.8 Stakeholder Positions along the MFS Value Chain

Mobile Financial Services (MFS) or mobile commerce is referred to as a wireless technology which enables the electronic transmission of data into the customer mobile device irrespective of the location of the actual mobile device (Lee et al., 2012; Tiwari et al., 2007).
The MFS Value chain may consist of a number of technology stakeholders with several responsibilities. For instance, the bank may decide to be the SEI and fully control the SE. In this case, the bank is able to process the transaction data through the SE in which it issues. Moreover, the bank is capable of allowing different AIs to use the SE functionalities while it can decide not to do this. In another scenario, the bank may decide to be the AI. In this case, the bank is only able to manage the particular keys of its own application and is unable to control the root keys of the SE. Additionally, the bank is the business-to-business (B2B) partner of the SEI (Kanniainen, 2010). Furthermore, the bank may decide to employ a TSM to manage its services in a trusted manner; this makes the TSM a partner with the SEI, SEV and AI as it should collaborate with them in order to manage the bank's services. On the other hand, TSM may choose to operate as a SEV and/or a SEI at once (or vice versa, a SEV and/or SEI as TSM). In this case, the TSM will have full access and control over the SE and can create the root keys, manage the SE throughout its lifecycle, and possibly allow different AIs to use the storage space of the SE. Having different roles in a MFS value chain may raise several issues from the consumer point of view. For example, the TSMs, AIs and SEIs should come up with an agreement regarding establishing the rules or customer care as consumers might be unsure which party to call in case if there is an issue with the service operation. This can be an important issue particularly when AIs, TSMs, and SEIs are separate legal parties.

In general, in the MFS value chain, a bank or a financial institution can be the AI, SEI and AI, or SEI, AI and TSM at once. Having common characteristics and possibly overlapping of the responsibilities amongst the stakeholders in the MFS value chain has made ecosystem set-up quite complicated. However, there is a good potential for ecosystem participants to

integrate their motivations and perspectives into a consistent service offerings (Kanniainen, 2010; Lee et al., 2012; Tiwari et al., 2007).

2.8.1 SE Keys as Crucial Pivot

The employments and conditions of NFC contactless payments for managing all SEs are normally based on the GlobalPlatform smart card standards. For instance, the standardization of UICC, eSE or Secure uSD Card, and Trusted Mobile Base (TMB) is still in progress. Since the international employment of NFC payments models, processes, protocols and infrastructure can be shared amongst technology stakeholders, investors have constantly got involved in order to provide different solutions for service offerings. Figure 7 demonstrates an outline of a common NFC payment application issuance model (Kanniainen, 2010).

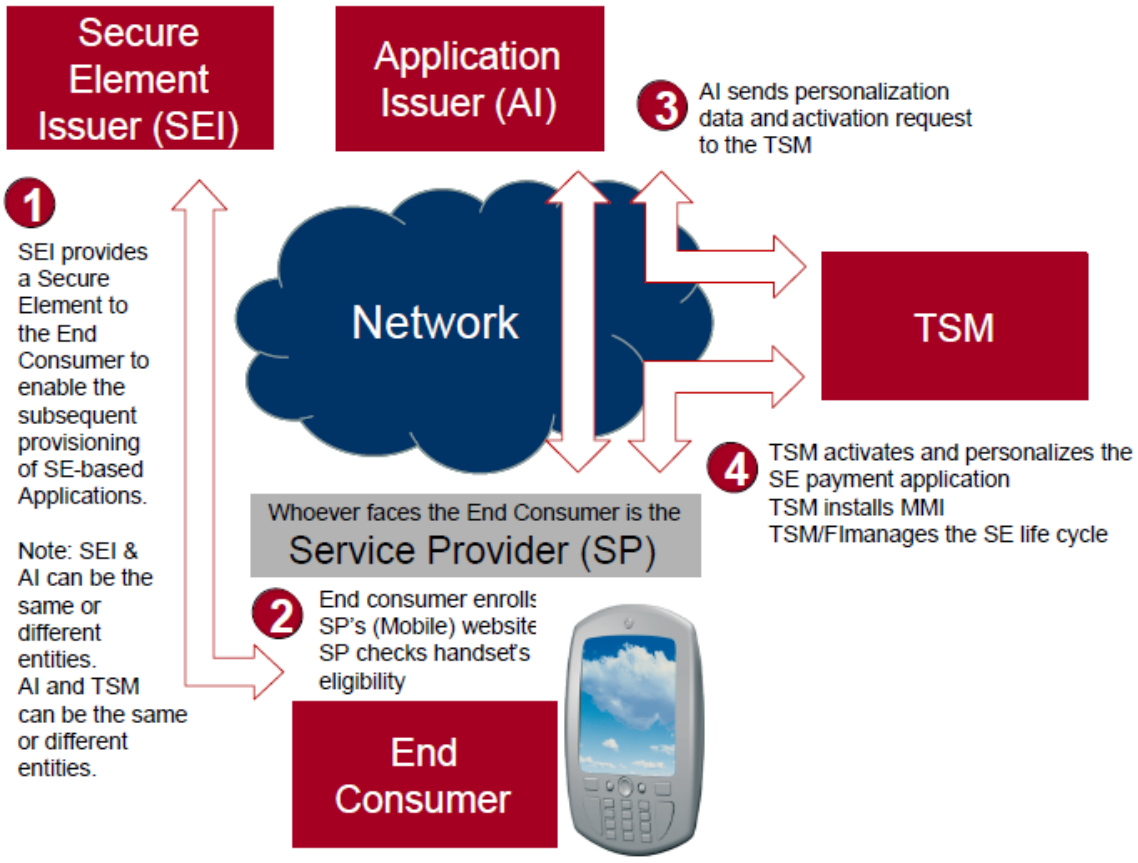

Figure 7: Key Provisioning Process to Secure Elements

(Kanniainen, 2010)

2.8.2 SE Issuance Process, Ownership and Personalization

The existing processes for card issuance in NFC payments are completely different from the former method. In the former method, the card is personalized during its production process; in this case, the card manufacturer matches the verified name and the existing address before their production is ordered. However, in the existing method the card is left blank during the production process and is personalized when a customer buys it from the MNO.

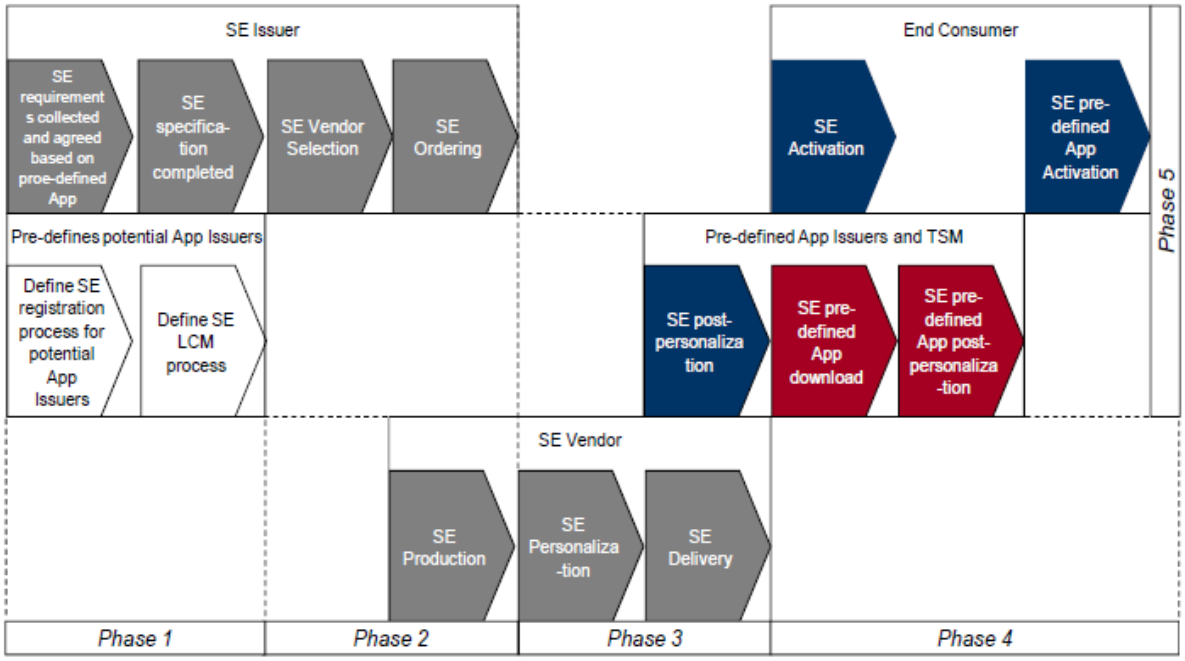

Figure 8: Conceptual Combination of Payment and SE Issuance Processes

(Kanniainen, 2010)

It is essential to identify and define the processes in which the respective stakeholders employ in order to verify the identity of clients for securing their ownership and relationship with every single customer. Also, it is necessary to continue the mobile payment business even if any process requires a change or an improvement. In other words, any process change should not have a negative impact on this on-going business. As a conceptual draft, the SE issuance process could take the form shown in Figure 8.

2.9 Proposed Models

The following models are the major proposed solutions to the existing issues of managing NFC payment ecosystems discussed up to now in this thesis.

2.9.1 The StoLPaN-NFC Mobile Services Standards Consortium

The StoLPan experts proposed a new logistical and technical model that fulfils the following criteria (Ahson & Ilyas, 2012; Benyo et al., 2007; Stolplan, 2011):

- Open relationship between SPs, SE issuers and users
- Technical transparency for SPs
- Service homogeneity for users

Basic Requirement:

The first basic requirement for this goal is to provide technical compatibility between the services and the hosting environments.

There will be numerous players involved in the dynamic post issuance and remote personalization process. It cannot be expected that all parties know each other or have established commercial relationships. The multi-application mobile environment establishes the requirement that the technical model supporting the dynamic post issuance procedure for NFC services should be capable of detecting any and all environment specifics, and should eventually hide any technical incompatibility from the players involved.

Summary of the Model:

One single logistical process can be created – covering, loading, personalization and life cycle management of applications – that is technologically agnostic and supports all SE types, even multiple ones, in communication devices. The process also ensures that both the user and the SP need not rely on third party services, unless they prefer to outsource certain activities.

In this environment the user can enjoy the services of multiple SPs, and can decide which SP and services to use. The process describes a homogenous system which supports SE issuers such as Mobile Operators (MO) in promoting their services to SPs, facilitating growth and improving business conditions. This homogenous system also improves business conditions for SPs by achieving technical compatibility with platforms of various SE issuers. The result is free access to the customer base of multiple SE issuers, and improved economics of developing NFC services.

2.9.2 GlobalPlatform SE Management Approaches

The approaches proposed by GlobalPlatform Mobile Task-Force concentrates around two major architectures: without aggregation versus with aggregation (Stolplan, 2011; Ahson & Ilyas, 2012).

Architecture without aggregation: In this model, as only one SE can be used to process the transaction, the customer should select the correct SE. For example, Customer Relationship Management (CRM) or customer support services can be managed directly by the SEI instead of being managed by SPs. Therefore for all applications which are being downloaded into the SE, the SEI is the responsible entity for controlling and managing them.

Architecture with aggregation: In this architecture, SPs can directly manage their respective CRM and customer support service and they can arrange their own application through all types of SEs. In this model, all SEs can perform a contactless transaction in any point of time. That means all present SEs can be active within a single mobile phone. Therefore, a collection of all the services will appear on user's mobile phone where the end-user does not know where those services are hosted from.

2.9.3 The Collaborative Model, f.ex. French Payez Mobile Project

This model recommends using the UICC or SIM as a SE to enable large number of SPs to co-operate as well as provide their services. In this model, the SE should be shared between multiple parties that are involved in the whole process. A multi-service provider ecosystem and customer convenience are the main goals of this kind of environment (Benyo, 2007). This model provides several benefits with regard to consistent service provisioning. It is user

friendly, enables easy access for SPs to mass markets and has the potential to introduce clear business rules (Mobey Forum, 2008; Benyo, 2007).

.

Another big advantage of this model is having the SE within the SIM that brings more flexibility into the ecosystem. For example, a bank does not need to directly invest in SEs where the common hardware space is shared between multiple parties. It should also be mentioned that the SIMs should be replaced by UICCs to be served as SE for NFC services. GSMA is strongly supporting this model as it has a very good market potential from the operator's point of view, as the handset will have faster performance with the MNO than without. This model also provides potential for joint business efforts aimed at the end-user (Mobey Forum, 2008; Benyo et al., 2007; Benyo, 2007).

Banks and MNOs should agree on their role in the payments value chain because the business model needs to be defined between them. MNOs should leverage their infrastructure to enable the bank to deliver the actual payment services. However, there is still no conclusion for industry-level business model agreement.

The biggest challenge of this model might be the need for strong dependencies between banks and operator business processes. For a successful process, a necessary number of business partners i.e. MNOs, FIs and merchants should make a positive decision based on their own business cases. If a bank be is a SP then it has to have a commercial agreement with every single MNO to be able to deliver the service to customers, which can then be a direct delivery or through TSMs (Mobey Forum, 2009).

2.9.4 The "Joint Venture" Model, f.ex. Barclays and Orange

This model introduces a new joint venture between the FI and the MNO. The solution may work on a basis of exclusivity or it may be open for competition to join later. SIM/UICC cards that are shared by the FI and the MNO are used to offer services to their customers. Business partners will have equal cooperation and the theoretical model might be co-ownership of the UICC (Mobey Forum, 2008; Mobey Forum, 2009).

This model allows business partners to agree on their rights and management tasks to run the system with cooperation. Familiar business partners in a specific market can implement this model easily because they will have fewer problems with regards to ownership issues.
The clear disadvantage of this model is that it is a "Wall garden" approach, which does not allow either the bank or the MNO to offer the same services to their clients. The other obvious challenge is interoperability if the market begins with multiple wall gardens as well as different implementations (Bouwman et al., 2008).

2.9.5 The SP-driven Model, f.ex. Rabobank in the Netherlands

There are several SE alternatives and several implementation options in this model (Waris et al., 2006; Mobey Forum, 2009). The SE does not need to be shared by different parties as the SP serves as the SEI. In some cases the SP can be the TSM or it may use an external TSM. The following alternatives are available, all slightly different from the model's perspective:

Banks issuing mini secure digital cards to their customers: In this option, the bank owns everything and it also can serve as the TSM. Therefore, there is no need for other SPs and all of them are excluded from the same SE. Many handsets are in the market that support secure digital cards but there is a need only for one secure digital card which should not be swapped by customers to use different applications. They should accept and only use the applications that their bank is offering to them. From the bank's point of view, there is no need for B2B agreements but it would be advisable for the bank to open up some space in the secure digital card for other SPs. This model does not have interoperability issues as the owner of the SE is one entity (bank) - of course if the bank does not open up its SE - but there is a potential for having another SE in the handset in the form of UICC issued by the operator.

Using a non-removable SE integrated into the phone hardware: In this case, the SE is stored in a handset as a separate hardware or it should be stored as a part of embedded chip. This model definitively requires a TSM to manage the keys for the handset-based SE.

SIM / UlCC: This model suggests a Mobile Virtual Network Operator (MVNO) to be owned/launched by the bank itself. So the bank should distribute the UICC card to its customers, which include payment and ID applications. The obvious disadvantage of this

model is that the bank should invest on the entire business area which bankers are rarely familiar with. However, in today's market there are MVNOs available that are offering their services for a reasonable price, so purchasing their services will be a decent option.

Banks issuing "Stickers" that can be attached to mobile phones: This option can be temporarily used until the other business models are mature enough to be implemented and used within societies. In this model, there is no connection between the sticker and the handset's components but apparently this can be developed through Bluetooth. There are no challenges such as interoperability, management, ownership, personalization, etc. in this model and that is a worthy excuse for bankers to invest in this model to issue stickers to their clients.

Having discussed the above models, it is important to mention that the industry has not come to the conclusion to widely implement these NFC payment ecosystems since the benefits of all players have not been met by their standards. For this reason there is still a lack of a standard procedure for stakeholders to follow while delivering the NFC payment service.

In the following sections of this chapter, we will describe the concept of cloud computing and continue by considering the advantages which it brings to the existing issues in NFC payment ecosystem models. In addition, a detailed discussion about the ways in which cloud computing changes the use of SE in NFC transactions will be provided in chapter 4.

2.10 Cloud Computing

The idea of using cloud computing within an NFC ecosystem introduces a new layer towards managing stakeholders that are involved in the whole NFC ecosystem. First, we briefly describe the main characteristics of cloud before we discuss our idea.

The primary concept of cloud computing is to use other IT technologies in order to provide a single service. The majority of IT technologies that are being used in cloud computing are already being used independently in other computing services. However, in a cloud, some of the capabilities of those technologies are selected in order to run the service environment.

The National Institute of Standards and Technology (NIST) defines cloud as below (Brian et al., 2008; Mell & Grance, 2009):

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"

To further clarify the NIST definition, cloud computing improves the network accessibility of ready to use resources by providing fast and easy network access. Thus, it enables the cloud provider to combine the available computing resources into a single host in order to serve all users. Furthermore, rapid provisioning facilitates the rapid matching of required resources at a specific time in which those resources are needed to operate. In addition, it provides constant computing power in case of increased needs, whereas rapid release of assigned resources helps keep the resources active at all times as they might be required for other operations in a different place (Mell & Grance, 2009; Brian et al., 2008).

2.10.1 Cloud Key Characteristics

The cloud characteristics can be described in what follows (Subashini & Kavitha 2011).

Broad Network Access: There is no need to access the cloud environment only with personal computers. Users can also use their smartphones, tablets, PDAs to access the cloud service environment. This feature of cloud computing allows broad network access from several devices as well as standardized interfaces.

On-demand Self-service: Depending on the cloud provider, users can either purchase or use a particular space of the cloud service free of charge. This means customers can purchase and use the service without having to deal with the cloud provider's personnel. From the provider's point of view, this feature of cloud computing reduces the budget required for employing personnel to deal with service offerings.

Resource Sharing: Cloud resources can be grouped using virtualization techniques. The resource grouping facilitates the possibility of several customers using a single resource. In other words, users can simultaneously use a shared cloud resource according to the service they require. Resource assignment and releasing procedures are carried out dynamically instead of physically assigning and releasing resources to multiple customers. Moreover, the physical location of resources is not known to customers apart from when customers need to limit their resource to meet legal requirements.

Rapid Elasticity: According to customers' demand requirements, cloud computing can match the required resources to provide flexible services. Dynamic use of the cloud service by customers has made service provisioning time and cost effective for cloud providers since it has raised the adoption of cloud services according to customers' demands. Thus, this dynamic automated system improves the power usage in the system as it prevents the operation of unused resources.

Measured Service: Cloud computing measures the operations of its resources in order to ensure effective computing is in place. Cloud technology can be configured in such a way as to report information like the number of resources being used at a certain point, the user of a specific resource, resource efficiency (e.g. data transfer) and so on. In addition, customers can use a service called "pay-per-use" which enables them to pay for the particular and each service which they receive. For instance, customers can pay for the number of hours that they use the system or they can pay for the volumes of data transfer.

2.10.2 Cloud Service Models

Cloud models can be categorized as follows (Buya et al., 2009; Mell & Grance, 2009):

Software-as-a-Service (SaaS): In this model, the application's services are delivered from the cloud provider to the customer. The cloud provider is responsible for managing the infrastructure, operating systems, and applications. Therefore the customer has certain control over the resources as well as particular application configuration settings. Moreover, customers are not aware of the services which run on top of the cloud infrastructure.

Platform-as-a-Service (PaaS): This model enables the cloud provider to deliver its platforms and operations to the customer. The customer's application needs to be developed and run on the cloud provider's infrastructure. Since customers do not have full control over the provider's infrastructure, they cannot access infrastructure components such as network, servers, operating systems and platforms. However, they have full control on their own running applications as well as certain application configuration settings.

Infrastructure-as-a-Service (IaaS): This model enables the cloud provider to deliver infrastructure resources such as processing power, raw data, and network capacity to the customer. In addition, this model enables customers to install their own applications and operating systems on the cloud provider's infrastructure. This feature of IaaS provides more flexibility for customers compared to previous models. Yet, customers can only control their own operating systems and applications and they still cannot manage the cloud provider's underlying infrastructure.

2.10.3 Cloud Deployment Models

As Mell & Grance (2009) state, the deployment of cloud models can take place by considering the owner of the cloud infrastructure, the responsible team who manages the cloud infrastructure, the infrastructure's location, and the people who can access the cloud services. Different cloud deployment models are described in what follows (Leaveitt, 2009; Mell & Grance, 2009):

Public clouds: Represents the cloud environment which can be used by everybody since it provides large scale services to general public. However, the cloud provider has the full control over the cloud environment and it manages the activities which are carried out within the service. Thus, both the software and hardware infrastructure are located on the provider's premises. The main issue regarding public cloud deployment model is the users who do not have a contractual agreement as an organizational employee or a third party contractor. In this case, the user is considered as untrusted.

Private clouds: These denote the cloud environment in which a single organization is responsible for operating the service. An organization may have a contractual agreement with

a third party which provides the cloud or it can be a cloud provider itself. In the first case, since there is a contractual agreement between the organization and the third party, the third party is considered as trusted. Thus, the organization will have full control over the cloud which is also being managed by the trusted third party.

Community clouds: Represents a community that is part of an organization. This model has almost the same characteristics as private clouds-in which the internal community is considered as trusted.

Hybrid clouds: This model includes the three above mentioned clouds models in one. Moreover, it represents the characteristics of public, private and community cloud deployment models and therefore it deals with both trusted and untrusted users. The trusted users are allowed to manage and control the cloud infrastructure whereas the untrusted users do not have such permission. The users of private and community clouds can monitor and manage the flow of data through the connected gateways in each division within the hybrid cloud. However, public cloud users do not have the permission to monitor and manage data flow as well as their resources. The location of hybrid clouds can be in an organisation or in a trusted third party site.

Still, there are some schemes which cloud providers offer that do not fall into the described deployment models. As an example, Amazon offers a model in which public cloud users are able to connect to private cloud services and resources. In this case, Amazon defines specific controls and access rights in order to manage the connectivity of public cloud users to private cloud resources. However, those exclusive Amazon defined procedures do not fall into the general cloud deployment models (Bugiotti et al, 2012).

2.10.4 Cloud Security Issues

According to Zissis & Lekkas (2012) it is not possible to define the entire cloud operations and services by using a single label. This is because the cloud's management, ownership, location, and access right permissions must be explicitly described. The model in which a cloud service is deployed may specify different terms in order to name a phase. For example

the words *internal* and *external* clouds are sometimes used to refer to *private* and *public* clouds.

The locations in which a cloud provider places the required security perimeters for running the system, normally specifies the services that they offer to customers. A firewall is one of those security mechanisms, which is used to partition networks in the cloud environment. While it is necessary to specify whether the cloud service is public or private (external or internal), describing the location of security perimeters may not be essential any longer since those perimeters (e.g. network firewall) were used to define the location of an asset to be protected. However, this type of separation is considered as an out of date model since cloud providers have expanded their offerings towards globalizing their services, hence the number of clients and contractors have increased (Kandukuri et al., 2009).

In cloud computing, the trust among users and providers has decreased since the service provisioning has been expanded into international scale which involves huge volume of data transfer. This has forced cloud providers to define strict access rights procedures in order to increase the system security as well as to raise the trust among both users and the service provider.

2.11 The Role of Cloud Computing within NFC Ecosystem

Having several parties involved in the NFC ecosystem with a lack of standards to define their roles and accesses to NFC components and applications, means that companies are increasingly considering using the cloud environment as a single entity to make things easier (Alliance, 2011). Moreover, cloud-based payment solution can help the adaption of NFC as they only require downloadable applications for both retailers and customers. However, it might bring more openness towards the security of customer's credentials (e.g. bank account details), but in terms of flexibility and manageability, it makes the whole process much clearer and easier to handle (Losup et al., 2011).

Cloud computing introduces a new method of storing payment credentials which improves the manageability of the NFC ecosystem. Rather than having all the sensitive information in the NFC handset, the cloud can store this information and transmit it when required. When a

client scans his NFC phone on the merchant's POS terminal, encrypted payment credentials are taken out from a virtual SE that is stored in the cloud and transfers to the SE that is stored in the NFC handset. The purpose of having a SE in an NFC handset is to provide temporary storage in order to store authentication assets. Once payment credentials reached the NFC phone, they are again pulled out to get transmitted to the merchant's terminal in order to perform the transaction. In this scenario, the communication between merchant's terminal and NFC phone is established through an NFC link. The cloud solution enables the client to manage transaction data by using a cloud-based payment application that is subscribed by both client and merchant. The payment application is accessible via a mobile phone using either email or a mobile browser and the transaction report can be in the form of a Short Message Service (SMS), email or just a sound. Examples of this approach include PayPal and PayCloud Mobile Wallet (PayPal, 2013; Alliance, 2011). Although in this approach, most of the focus has been towards vendor gift cards, the cloud-based approach is also feasible in open payment systems.

Development of this approach can be easy for vendors as they are not required to install new POS terminals. Thus, this approach gives the opportunity to vendors to better differentiate and customize applications. Another advantage that this solution offers to vendors is that, in the case of operating a different payment type, the solution might be lower costs for the vendor. Moreover, clients are already familiar with this type of payment methods (i.e. PayPal).

As cloud-based NFC payments might be treated as card-not-present in some cases, it is more likely that the transaction fees will be higher than the normal card payments. Furthermore, in order to execute a transaction, a connection is required to the cloud. Executing a transaction may not be possible if this connectivity is somehow interrupted. In addition, some security issues may arise from using email and SMS that can be the sign of a transaction notification. As the current payment infrastructure is not leveraged, there might be a possibility that a vendor should install a non-standard application in order to process a payment. Replacement of current POS terminals with NFC terminals may be required, as the POS has to be capable of communicating with an NFC enabled phone. The transaction execution performance depends on the network connection speed, data capacity and the way that wallet's data are

accessed. Last but not least, both client and vendor have to sign up with the cloud service provider to use its services (Kounelis et al, 2012; Alliance, 2011; Ko et al., 2011).

2.11.1 Fujitsu Cloud-based Data Transfer Service Project

One of the companies which established the use of NFC through cloud computing is Fujitsu. It developed a platform technology that automatically downloads runs and erases applications in a required time and place. The main focus is on data transfer and not payment systems. However, this platform can be used as an initial start for developing cloud-based payment platforms.

The Fujitsu system has the following three characteristics:

1. The system is the combination of a cloud-based communication platform and an application runtime environment.
2. Application and data transmission are automatically performed from the cloud.
3. Applications are launched and run on a device (PC, laptop or smart-phone) and are deleted when they are not required anymore.

With the use of NFC technology, devices are connected so applications and data can be transferred between them. Then the applications can be downloaded and fitted to size for which ever device that they are asked to be downloaded to for easy observation. For example, a user attends a conference. Once entered in the conference venue, the relevant presentation apps and materials will automatically download to the user's device from the cloud and once the conference finishes, that information will automatically be erased from the device. This technology also uses Global Positioning System (GPS) to find the user location for downloading necessary data and apps from the cloud. This approach improves the user operational efficiency by reducing the time for setting up apps and transfer data.

2.11.2 Cloud-based NFC Payments in Austria

A1, a mobile network operator in Austria, announced in 2011 that McDonald's and Merkur supermarket have signed a contract with A1 to test the development of PayBox NFC mobile payment service (NFC World, 2012a). A1 is a subsidiary of the Telekom Austria group

which holds the full Austrian banking license. The PayBox service does not require a Personal Identification Number (PIN) and allows a payment of up to €25. The service does not use MasterCard PayPass or Visa PayWave and does not support Europay, MasterCard and Visa (EMV) chip and pin technology. As an alternative, Paybox processes the payments in a cloud environment and suppliers use a small PayBox NFC unit rather than contactless point of sale terminals for handling mobile payments. To be able to use this service, clients should have an account with PayBox and designate that account to handle the mobile payment services' financial issues. Consequently, every time a client uses the PayBox services a certain amount of money will be deducted from his account. The following steps describe the process of PayBox cloud-based NFC mobile payments (NFC World, 2012a):

1. The client's mobile phone number and account number are joined together in the back office and the clients download the payment application to their mobile phone.
2. There is no need for other identifying data such as clients' bank account details and mobile phone numbers to be downloaded with the application.
3. PayBox deducts payments a few days later than the actual payment day from the designated bank account.
4. The daily purchase limit is €50 and all the transmitted data is encrypted. Thus, the debit from the bank account can be for multiple transactions.
5. Clients receive a confirmation text message for each payment they make, which takes half a second to process.

2.11.3 NFC Cloud Payment Security

This section highlights the vulnerabilities of NFC cloud payments and addresses possible exploits from Cyber-attacks.

A. Wireless Threats

There are a number of possible attacks over a public wireless network such as NFC. One of the most well-known attacks is typically called Man-In-The-Middle where the attacker (Eve) establishes connections with both genuine sender (Alice) and recipient (Bob). Nonetheless,

neither Alice nor Bob are aware of the existence of Eve who controls the entire conversation while making Alive and Bob believe that they are communicating directly.

Impersonating a wireless legitimate access point, i.e. a public Wi-Fi hot spot such as an airport first class lounge, through a configured computer enables the attacker to access client connections and take advantage of the sensitive data being transmitted to/from the access point (Biba, E, 2005; TheShmooGroup, 2008). Along with routing the traffic to a legitimate access point, a computer can also monitor the communication channel simultaneously. Additionally, authentic domains of particular Websites such as banks can be mapped to the IP address of a malicious Website in order to take advantage of clients' credentials. This is due to the provision of gateway services and DNS settings by the computer to the connecting clients. Similarly, setting up a fake base station to pose as a legitimate user, can also be a possibility (Meyer & Wetze, 2004).

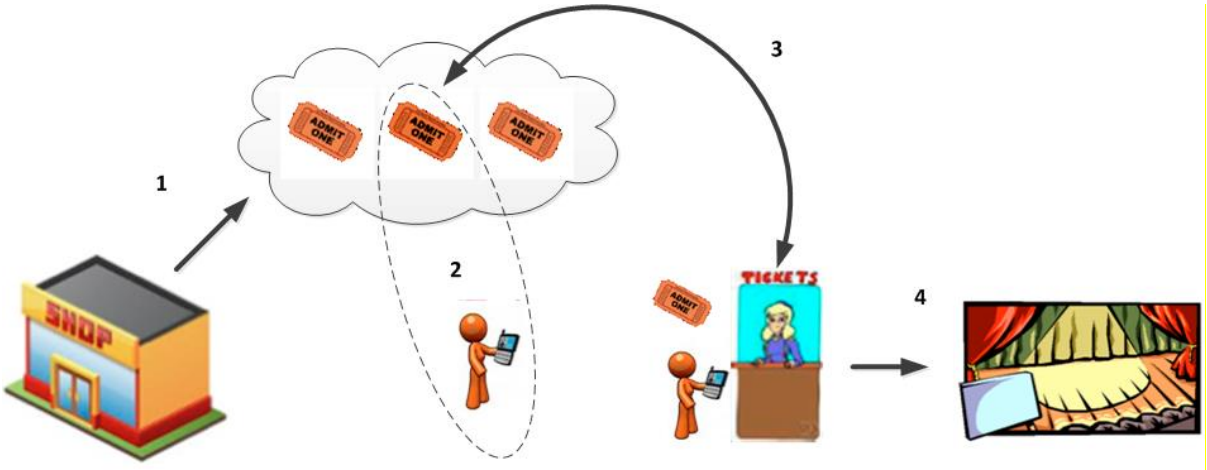

Figure 9: The Lifecycle of a Mobile Ticket (Kounelis et al., 2012)

1. The cloud service is requested to issue the tickets. 2. The ticket is purchased through the user's mobile device. 3. Ticket verification. 4. Admittance to the venue.

When users are filled with radio interfaces, their mobile devices demand for connectivity potentials. The radio interfaces can include Bluetooth, NFC, Wi-Fi, 2G/GSM, 3G/UMTS, 4G and GPRS technologies. For instance, a mobile device may use a 3G connection to access the Internet and exchange data; it may then handover to the available Wi-Fi connection. A number of mobile network operators such as Orange UK allow automatic hand over from 3G to Wi-Fi through a built-in Orange Wi-Fi application. From the security viewpoint, the

automatic method of connection hand over exposes a new vulnerability at the point of the actual hand over from 3G to Wi-Fi. Typically, this can be the case when 3G connections have a better quality of service outside a building than a Wi-Fi connection. So as the user goes into the building the hand over takes place where the Wi-Fi takes over as carrying the data packets.

In order to ensure that an adequate level of security is in place within the mobile cloud, the modern cryptographic properties must be utilised in the cloud (data storage), mobile devices and POS terminals. This approach minimizes the generalized security risks as the cloud providers can only see encrypted data while in transmission. However, it seems that the cloud providers are not yet ready to take the new challenge by implementing such system. This can be caused by the lack high-level authority to enforce regulations for cloud service providers to implement encryption on the client side rather than collecting unencrypted data from them.

B. Citizen's Threats

The user may find itself under a number of security threats throughout the purchasing process; the security threats are described in what follows.

1) Attacks while Purchasing and Using the Ticket

The attacker may steal the user's ticket during the purchasing process. This can be done through different types of attacks:

- The connection between the cloud and the mobile device can be eavesdropped and consequently the attacker may get a copy of the ticket that can be used before the legitimate user uses it.

- The displayed information on the mobile device itself can be eavesdropped or recorded while in use in public mobile locations.

- The attacker may intercept the connection between the mobile device and the cloud (Man-In-The-Middle). In this case, the attacker will have the capability of tricking the user that the transaction is unsuccessful while using the ticket for his own benefit.

2) Attacks during the Verification of the Ticket

When the mobile device is shown at the venue inspector system, it is an indication that the ticket and the mobile device are verified by the venue system. Nonetheless, there are yet a number of possible threats that should be addressed. The verification system may become unavailable as a result of a denial of service attack. Using a cloud server for implementing the verification mechanisms can be an effective and secure solution as it provides scalability and avoids losing the system because of high demand in a short period of time.

In the case of radio jamming attack and the failure of the verification system, there would be no way for ticket verification and therefore clients would not be permitted to enter the venue. Consequently, having a human inspector becomes a need as this would be the only alternative to verify the validity of the tickets shown by clients. However, this approach would have its own consequences that may lead to many false positive and false negative results.

In order to prevent the jamming attacks, it would be ideal to have mobile device radio hardware for scanning the environment to identify new radio frequency growing threats; such threat may include 'fake' GSM base station. The protocol scan that occurs in the background would notify the mobile device in the case of a malicious action such as jamming or denial of service attacks.

3) Potential Countermeasures

Several countermeasures can be in place to reduce and/or eliminate the described above threats. Moreover, secure communication must be in place to ensure the confidentiality of the exchanged messages in the communication channel. Additionally, in order to avoid false impersonation, mutual authentication should take place amongst all involved parties in the whole process; this would also guarantee data integrity.

2.12 Related Work

In this section we describe the most popular and recent cloud-based mobile payments which have been developed by well-known companies.

A. Google Wallet

One of the major companies which operates the concept of mobile wallet is Google. They named this service as "Google Wallet" (Google, 2013; Ronald et al., 2013). The communication between the mobile phone and the POS is carried out through NFC technology that transmits the payment details to merchant's POS. Customer credentials are not stored in the mobile phone; rather, they are stored online. Google Wallet takes the form of an application stored on the customer's mobile phone. The customer will have an account with Google Wallet which includes the relevant registered credit/debit cards. Accordingly, the Google Wallet device has a chip /SE which stores encrypted payment card information. Linked credit or debit card credentials are not stored on the SE; rather, the virtual prepaid credit/debit card which is created during the setup is stored on the SE. The transaction then operates through the virtual prepaid credit/debit card that transfers funds from the Google Wallet into the merchant's POS when the customer taps his phone on the POS.

B. MasterPass

"MasterPass" (Mastercard, 2013; Bodhani, 2013) is a service which has been developed by MasterCard as an extended version of PayPass Wallet Services (NFC World, 2013) and provides a digital wallet service for secure and convenient online shopping. In MasterPass, delivery information and transaction data are stored in a central and secure location. The latest MasterPass provides the following services (NFC World, 2013):

- *MasterPass checkout services:* This service enables the vendor’s payment acceptance in a consistent way irrespective of the client’s location. This means vendors have the ability to accept a payment without having to know where the client is. For instance, when the client is in store, he can use this service since it supports NFC, Quick Response (QR) codes, tags, and mobile devices to pay for products at a vendor’s POS. Thus, in online shopping scenarios, the client can use this service to pay for a product

without having to enter the card and delivery details every time he intends to make a purchase.

- *MasterPass-connected wallets:* Vendors, financial institutions, and partners are able to provide their own wallets using this service. The client's card information, address books, etc. can be saved in a secure cloud provided by a party they trust. Thus, clients can use other credit and debit cards in addition to their MasterCard's cards.

- *MasterPass value added services:* The purpose of this service is to improve the client's shopping experience before, during and after checkout. Value added services include account balances, offers, loyalty programs, and real-time alerts.

C. Bell ID Solution

In June 2013 (NFC World, 2013b; SecureIDNews, 2013), Bell ID proposed a new platform which enables card issuers to store certificates, keys and NFC credentials in a cloud environment instead of in mobile devices' SE. This approach equips application issuers with sufficient level of control to manage their credentials without being in need to share the access rights with a third party. During the transaction process, the clients' credentials are pulled out from the cloud (remote secure element) which then generates commands for the payment and sends it to the merchant's POS terminal through the mobile device. Their approach also allows pre-authorisation of payments that improves the flexibility of payments for customers in the sense that they can make payments even when the cloud server is offline or the connection between the device and the cloud is not properly established. Furthermore, Bell ID 'SE in the cloud' approach also enables the instant fraud detection, meaning that the payment application is blocked when necessary.

Having published the general benefits and use of their service, we argue that this approach was initially proposed by us in December 2012 (Pourghoumi, P. and Ghinea, G (2012) 'Managing NFC Payments Applications through Cloud Computing' in *Proceedings of the 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012), London, UK.* IEEE, 2012, pp. 772–777).

D. Chen et al.'s Protocol

This section briefly describes the NFC payment system based on GSM that has been proposed by Chen, Hancke, Mayes, Lien and Chiu (2010). The assumptions and requirements for their approach for mobile payments system are first described followed by a summary of their payment protocol.

Their proposed protocol meets the number of requirements. Firstly, all the involved parties are considered to be under the control of the same Mobile Operator (MO). Secondly, user's phone contains a SE that is embedded in the SIM (UICC). Thirdly, user's phone and merchant's POS device are both NFC-enabled. Furthermore, their approach assumes that the user fully trusts the MO and follows the present GSM security mechanisms (Brookson, c., 1994; Eberspaecher et al., 2008). Moreover, the communication between the Payment Gateway (PG) and the merchant's POS is assumed secure since it passes over a secure network. The PG is also considered as the sub-system of MO that should act as a Visitor Location Register (VLR). This is because in step 7 the PG should receive the confidential triplets from VLR. Therefore, the main role of the PG in their approach is based on the actions related to the payment and user authentication. Their proposed protocol that runs over the GSM network as well as the payment data flows are detailed in the above figure.

Their proposed protocol includes five entities: HLR/Billing Centre, VLR, Payment Gateway, Merchant NFC POS and Customer NFC phone/SIM. Moreover, their proposed protocol consists four phases:

1. Initial Setup: There are some fundamentals to encounter before starting the key stages of the payment process (see the "initial state" in Figure 10).

Their proposed protocol includes five entities: HLR/Billing Centre, VLR, Payment Gateway, Merchant NFC POS and Customer NFC phone/SIM. Moreover, their proposed protocol consists four phases:

2. Price Visual Checking: The first 4 steps contain the initial goods scanning, the price displaying and the visual confirmation at both the merchant's POS and the customer's phone.

3. Triple Authentication: When the customer views the Payment Information (PI) on his/her NFC phone and agrees to proceed with the transaction (step 4), the triple authentication begins its execution. The payment processes are enclosed in this section whereby the backend system, merchant's POS and the customer's phone authenticate the other two payment participants for protecting the following transaction processes.

4. Transaction Execution: Takes place after the successful authentication. In this step, the system performs further transaction checking and deduction, using the transaction information.

A: Analysis

The security analysis of the protocol that has also been carried out by Chen et al. (2010) shows that the protocol is secure in the following scenarios:

1. Customer is dishonest or has altered the phone, and is aiming to break the protocol rules for personal e.g. customer account impersonation and/or credit modification.

2. The merchant is dishonest and has access to an altered device, and s/he is trying to modify the PI in order to deceive the backend system or customer to take financial advantage.

However, we argue that due to the presence of several entities, and considering the number of interactions passed through different stages of this protocol, flexibility remains as a concern with respect to both service providers and customers. Moreover, a further layer of security could have been added by introducing PIN authentication by the user. Additionally, mutual authentication of the SIM and the MNO should be in place for improved security by adding freshness by the mobile device in order to resist replay attack. There is also no use of digital signatures with the transaction messages for data integrity and non-repudiation purposes.

In summary, their proposed protocol includes an easy method for integrating the technological benefits of NFC to the existing GSM networks as well as deployed POS systems.

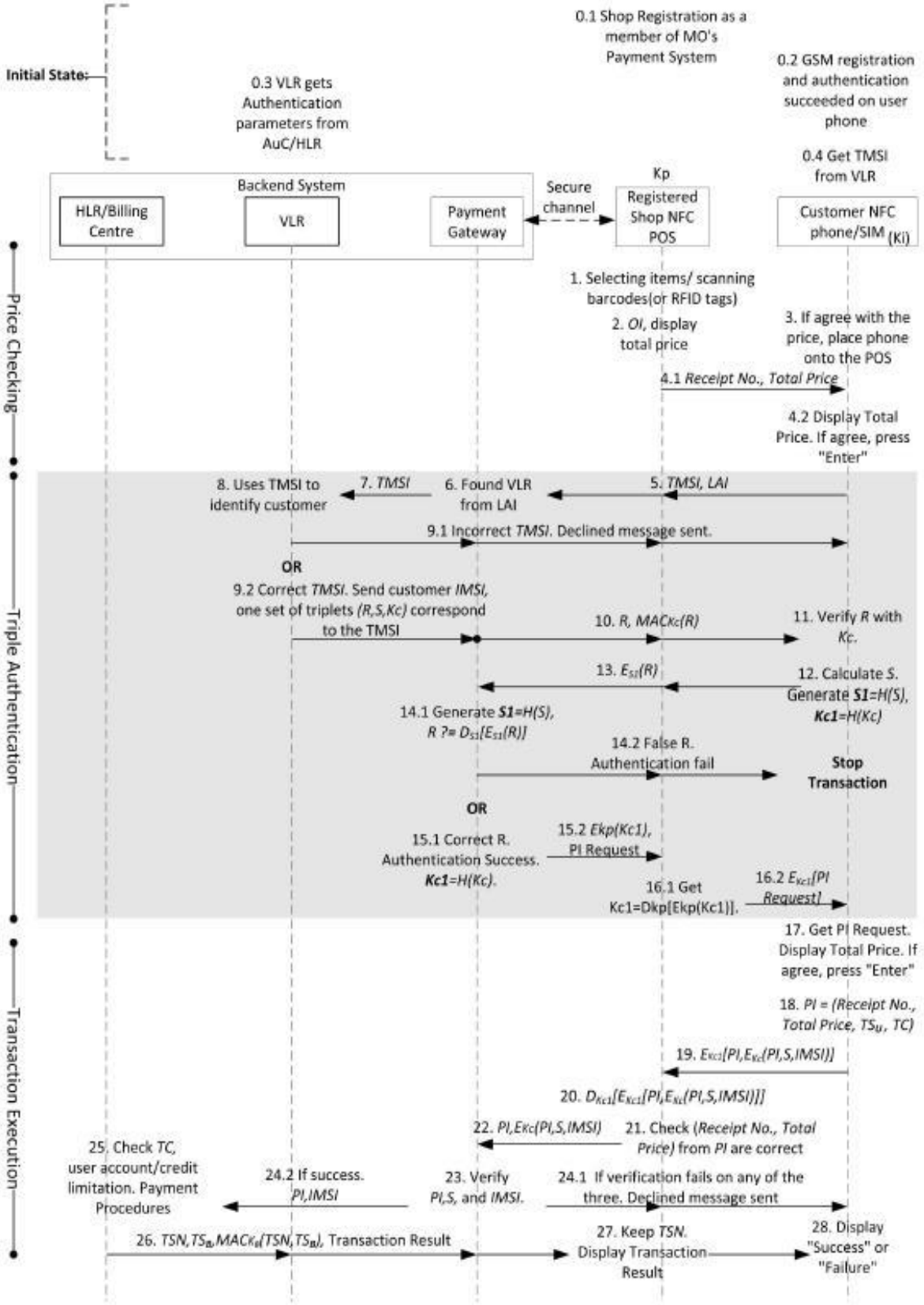

Figure 10: GSM Authentication and Encryption (Chen et al., 2010)

2.13 Summary and Discussion

This chapter provided background information in the area of electronic and mobile payments. Several approaches towards managing SE services were discussed, which in turn highlighted the complexity of the NFC payment ecosystem as well as dissatisfaction of involved parties with the current proposed models.

The literature indicates that the flexibility, manageability, personalization, ownership and control of the payment ecosystem depend largely on the relationships and agreements which ecosystem's players establish. This has resulted in increased private contracts/agreements for service provisioning between players since they all have not come to community standardized procedures in order to clearly define the responsibilities and control permissions of each party.

On the other hand, industry-leading companies such as Google and MasterCard have introduced their own method of mobile payment using the cloud environment as the centre where all customer credentials are stored. Although this approach provides flexibility, we believe that at the same time it is largely dependent on the speed of the Internet network and it yet does not improve the existing Internet security risks. This is the cause which forced the service providers to offer their cloud-based payment services only for monetary transactions.

The issue of selecting the most secure and flexible approach towards managing the payment ecosystem is still the main concern of industry stakeholders. Consequently, our focus in this thesis is to propose real-time and secure NFC payment ecosystem models that provide security and flexibility to both customers and service providers. Therefore we will start off by proposing cloud-based NFC payment scenarios, which improve the complexities of existing ecosystem models. This will be followed by designing secure transaction protocols to show the reliability and validity of our proposed models. A security analysis of designed protocols is then provided to discuss the confidentiality, integrity and availability of sensitive data (i.e. payment details) across different communication channels between the involved parties.

Having described the challenges of NFC payment application management within the SE environment as well as putting forward the idea of using cloud computing for managing NFC payment ecosystem, motivate us to introduce new ecosystem payment protocols in a way that

satisfies both clients and service providers. The next chapter describes the methodology we used to conduct this research. In addition, it discusses the way in which the research aim and objectives are linked with the selected research methodology.

Chapter 3 - Research Design and Approach

3. Overview

In the first chapter of this thesis, the aim and objectives of this research were introduced. This chapter explains the methodology which is used in order to accomplish the aim and objectives of this research. Recognizing the relation between our work and the methodology used is the main goal of this chapter and will be discussed once we introduce the research design and approach. Design Science Research (DSR) is selected as our methodology in this thesis that is discussed from different viewpoints in detail in order to justify its adoption with our research.

3.1 Research

Kuhn (1996) describes research as an activity which helps to understand a phenomenon. A phenomenon consists of entities' behaviours which interests the researcher. A phenomenon or at least some part of it might be created in IS rather than arising naturally. The meaning of understanding is to have the knowledge to predict some aspects of a phenomenon's behaviour. To this end, the set of activities considered by the research community as "appropriate" to provide understanding is called research methods. Furthermore, Gregg, Kulkarni, and Vinzé (2001) define research as an approach which promotes understanding and knowledge enhancement. However, research is also described as a process which systematically tries to resolve a problem, find an answer to a question, or a better understanding of a phenomenon (Hevner and Chatterjee, 2010). Although research might take several forms, knowledge enhancement is the main objective of a research. Research methodology is an important part of a research since it describes the process of a research-related work. It also ensures the validity and rigour of the conducted research. Methodology is defined as "*a body of method, rules, and postulates employed by a discipline"* (Webster Dictionary, 2013). There are many available methods in different fields trying to enhance the current knowledge and this is because there are various areas of research in each field.

3.1.1 Research Perspectives

A set of basic beliefs for guiding the activities of a researcher during the research process is called a "*paradigm*" (Guba & Lincoln, 1994; Mingers, 2001). A research can be separated into three different paradigms in Information Systems (IS) and computing (Chua, 1986; Klein & Myers, 1999; Orlikowski & Baroudi, 1991; Vaishnavi & Kuechler, 2009). These paradigms are:

- *The Design Science Research (DSR) approach:* Construction and evaluation of artefacts are carried out in order to describe and improve system aspects.
- *Positivist Research:* Assumptions and hypotheses of a research investigation are supported by collected data.
- *Interpretive Research:* Does not include assumptions and hypotheses prior to an investigation. Instead, data collection is used to extract knowledge.

To view the research paradigms in the world of research, four philosophical theories are used (Guba & Lincoln, 1994; Mingers, 2001; Vaishnavi & Kuechler, 2009):

- *The theory of existence (Ontology):* Explains the reality of a subject or entity by considering the fundamentality and reality of that subject. It requires distinguishing between the reality and unreality of the subject.
- *The theory of knowledge (Epistemology):* Studies the nature of a valid or true theoretical knowledge. It asks questions such as what knowledge is and how it can be obtained. To what extent can a given subject be known?
- *The theory of reasoning and inference (Methodology):* Examines the relevance of a theory and practice. This investigation helps to identify a desirable approach in order to generate the best knowledge in a satisfactory manner.
- *The theory of value and value judgement (Axiology or Ethics):* Describes to what degree a given subject has a value. Or is the subject considered as right at all?

A summary of the above four paradigms' viewpoints are described in table 3.

Referring to table 3, the perspective that will be adopted in this thesis is that of design, since we first considered the reality and fundamentality (Ontology) of our research subject that is the emerging area of mobile payments, which is becoming a reality in our lives. We then

explored the existing knowledge in this area, which have also been proposed/developed to examine the validity (Epistemology) of this new method of payment.

Table 3: Philosophical Assumptions of Research Approaches (Vaishnavi & Kuechler, 2009)

Research Perspectives			
Basic Belief	**Positivist**	**Interpretive**	**Design**
Ontology	A single reality. Knowable, probabilistic	Multiple realities, socially constructed	Multiple, contextually situated alternative world-states. Socio-technologically enabled
Epistemology	Objective; dispassionate. detached, observer of truth	Subjective; knowledge and values emerge from the researcher-participant interaction	Knowledge through making: objectively constrained construction within a context. Iterative circumscription reveals meaning
Methodology	Observation; quantitative, statistical	Participation; qualitative. Hermeneutical, dialectical	Developmental: measure artefactual impacts on the composite system
Axiology	Truth: universal and beautiful; prediction	Understanding: situation and description	Control; creation; progress; understanding

Moreover, we measured the relevancy of the theory and practice (Methodology) to identify the desirable approach in order to design and develop our mobile payment model. Having designed our models and their respective protocols, we subsequently carried out a detail security analysis in order to describe to what degree our proposed protocols have a value (Axiology).

3.2 Design

Hevner and Chatterjee (2010) generally describe design as group of instructions for making *things*. However, it is not the *thing* itself. The way we design computer system models before and during the building process gives us the insight of the overall system and the initial plan. However, since the initial plan is not complete, having an overview of the building process'

plan does not provide the actual details of components and relevant running system. The designed model is important for developers because it can be used as a communication tool between technical and non-technical domain developers. It also helps them to understand how the system is built by providing the abstractions of the system's model.

Hevner and Chatterjee (2010) also point out that there is a significant difference between building a large physical system and building a large-scale software system. For example, the processes involved in constructing a building are not involved in IS design. In order to construct a building, a detailed planning is required before the construction process begins. Otherwise, the issues that are not figured out in the initial steps of the construction process will potentially cause large delays and create severe financial consequences. The way in which planning differs in the IS design process is that it does not require as much time and cost as constructing a building does. This means that depending on the size of the project, we can assemble software systems in minutes and discard unwanted results. When looking at the processes of the software design, we realize that this step requires major cost. To avoid large up-front costs, Evans (2003) recommends performing small planning before the actual implementation and breaking down the design process into a series of smaller discrete design steps.

This approach is called a hands-on approach and is one in which developers can learn more about the issues as they go along. Moreover, the goal of software-based system development may change several times during its design and development process. This makes software-based system development very challenging. Indeed, sometimes the final goal of the process is itself unpredictable. Also, during the development process, certain new features that were not part of the project may be added as developers gain more experience in the problem domain. Moreover, there might be a need to alter a system's runtime constraints, and new platforms and hardware may be introduced to the development process in order to enhance the adoptability of design. In this context, Hevner and Chatterjee (2010) discuss that in the system design stage, the main objective is to make precise decisions when selecting different options which places restrictions to utility and resources. Moreover, Gregg, Kulkarni, and Vinzé (2001) suggest that the research aim should be achieved based on the obtained knowledge and experiences during the system development process.

To summarise, developing software artefacts to resolve human difficulties are the main issue that is dealt with in IS design. Artefacts are considered to have a number of mechanisms such as *constructs, models* - abstractions, *methods* - algorithms and practices, and *instantiations* - implemented and prototype systems (Hevner & Chatterjee, 2010). Design research is not the only method that deals with building artefacts, artefacts are also being designed and developed as a part of professional design. Although design and development of artefacts are involved in both design research and professional research, however there is a difference between these two approaches. Henver and Chatterjee (2010) state that in design research, an identification of a contribution to knowledge and strong results are provided whereas professional design provides an application of the existing knowledge to improve business issues. Yet the gained knowledge can be very useful even if the research does not provide satisfactory results.

3.3 Overview of Design Science Research

Vaishnavi and Kuechler (2009) describe Design Science Research (DSR) as set of analytical techniques and perspectives used to carry out research in the area of IS and computing. They discuss that the performance analysis and the utility of designed artefacts are involved in the DSR process in order to recognize, describe, and improve the performance of IS aspects.

The principle of design science research is certainly a *problem solving* paradigm (Hevner et al., 2004) that addresses the so-called *wicked problems* by producing novel artefacts (March & Storey, 2008; Pries-Heje & Baskerville, 2008). In fact, the purpose of design-science research is to provide novel, innovative, and purposeful scientific artefacts that are designed, developed, and evaluated effectively. In design science research, the word "purposeful" specifies that these artefacts should deliver individuals and societies with useful services since they are supposed to improve current practices, or to propose better solutions (Kuechler & Vaishnavi, 2008) and thus address unsolved problems (Hevner et al., 2004). Moreover, providing additional improvements to real-world phenomenon is what artefacts aim to achieve (March & Storey, 2008; Iivari, 2007; Purao, 2002). As a result, organisations may prefer to use these artefacts in their businesses in order to change the ways in which they provide services.

As described in the previous section of this chapter, design is the invention, plan, and development of a certain thing. The design activity itself can be divided into two categories: "natural science" and "science of artificial". The knowledge that describes the interaction between objects or phenomena refers to natural science, while science of artificial refers to knowledge which is about designed artificial objects phenomena that are supposed to meet particular goals.

Furthermore, a general overview of DSR process has been proposed by Hevner and Chatterjee (2010) which define three design cycles. The adoption of the research environment with research activity is done in the *relevance cycle*. *Rigour cycle* connects the knowledge base and the process of design research. The *Design cycle* provides the iterations while developing artefacts, as well as the evaluation. Figure 11 illustrates the cycle of design science research.

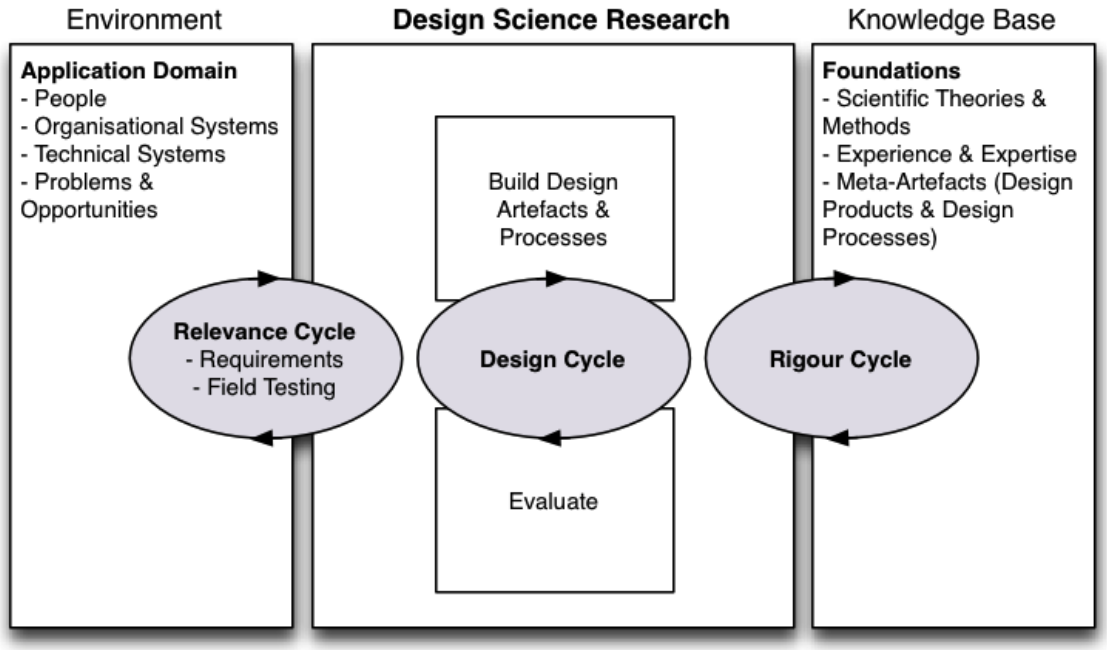

Figure 11: The Cycle of Design Science Research

(Hevner & Chatterjee, 2010)

Five general steps have been proposed by Hevner and Chatterjee (2010) in accordance to these cycles. Each of these five steps follows the same general idea for the DSR process and will now be presented:

1. *Construct a Conceptual Framework* refers to problem identification and solving motivation of the problem. The requirements for artefact's development are defined as the problem. Hevner and Chatterjee (2010) explain that the objectives of this step are to increase the motivation of the researcher, interest of the audience to follow the solution as well as to accept the results. They also discuss that this step improves the communication that is carried out between researchers for understanding the problem.

2. The purpose of the *Develop System Architecture* is to develop a unique architecture design, for extensibility and modularity. In addition, the functionalities of system components and their relationships should also be defined in this stage.

3. Analyse and Design the System phase deals with designing database/knowledge base plan and procedures to perform system functions. Moreover, different solutions can be developed in this phase; nonetheless only one solution is normally selected.

4. In the *Build the (Prototype) System* stage, the researcher should study the concepts, frameworks and design through the system building process. The researcher should also gain an insight on the subject of the problem as well as the complexity of the system.

5. In *Observe and Evaluate the System* step, the researcher should observe the use of the system by case studies and field studies, evaluate the system through laboratory or field experiments, develop new models based on the observation and experimentation of the system's usage, and consolidate learned experiences.

3.4 Design Science Research Methodology

The DSR methodology is considered as an interactive model since each stage can be revisited at any time during the process. The interactivity of this model makes it especially appropriate for software development as design requirements can be modified continuously and outcomes of each stage (Figure 12) may need a revisit to a previous stage in order to be changed and improved (Vaishnavi and Kuechler, 2009).

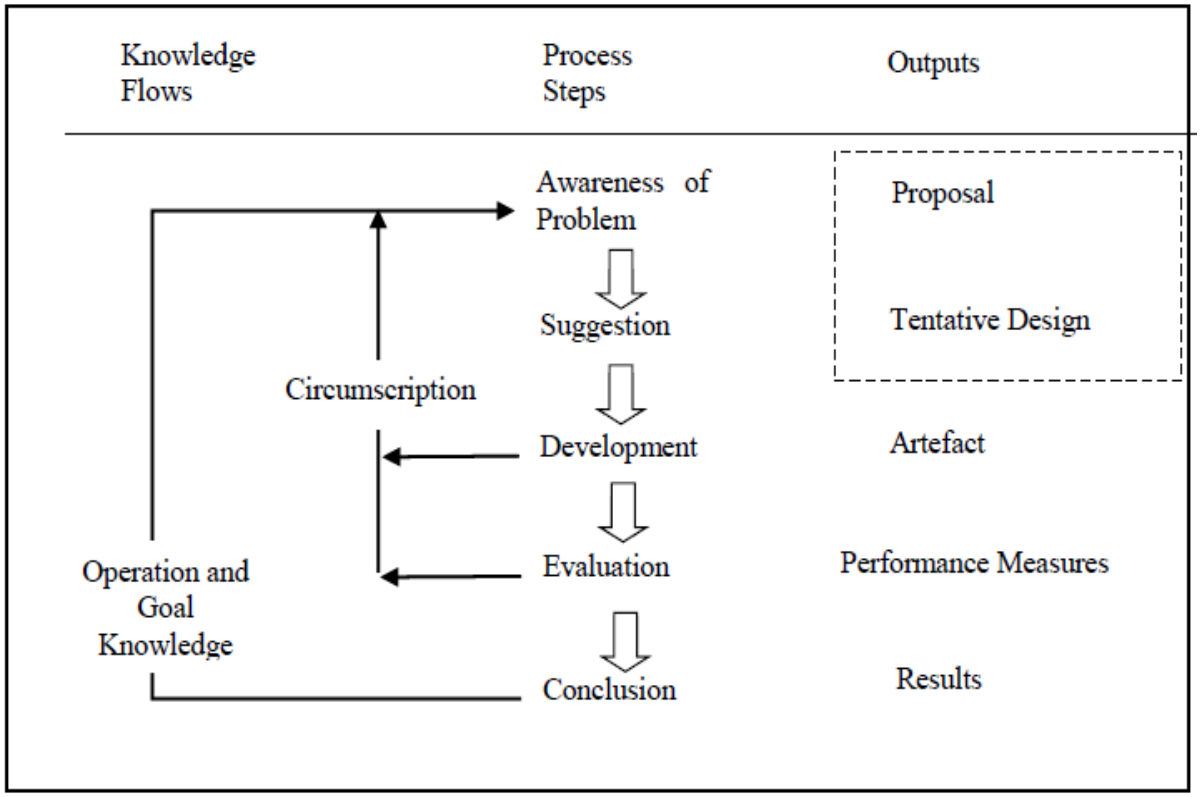

Figure 12: The General Methodology of DSR

(Vaishnavi & Kuechler, 2009)

The processes of DSR cycle stages are demonstrated in the above figure where "knowing is making". A detailed description of each stage is explained in what follows (Vaishnavi & Kuechler, 2009):

Awareness of Problem: Multiple sources have direct influence on this stage. Either there should be new industrial developments or developments in a reference discipline. Further research in the same field can also provide a prospect for the researcher to develop new findings in order to demonstrate them as a formal or informal proposal.

Suggestion: Basically the suggestion phase is a creative point in the process in which different functionalities are designed based on a new configuration of novel or existing elements. The outcome of this stage is a tentative design which has a close connection with the proposal and comes immediately after the proposal.

Development: In this stage, the tentative design is implemented and the outcome is an artefact. Different implementation techniques are required based on the type of the artefact

which a researcher expects to develop. The originality is not in the building of the artefact since it is mainly in the design.

Evaluation: The evaluation of the artefact takes place after the artefact is constructed. The evaluation should be based on the specific criteria that are normally implicit and regularly made clear in the proposal (Awareness of Problem phase).

Conclusion: The final efforts of a research are presented in this stage. The research findings are considered as *good enough* when they are satisfactory. The results are also considered as satisfactory even when there are deviations in the artefact's behaviour from the hypothetical predictions. In this stage, the findings of the research are combined and written up. The knowledge that has been learned and applied or behaviour that can be frequently invoked during the research process are regularly considered as firm facts. However, the gained knowledge is considered as *loose ends* if it is not applied to the research and the uncharacteristic behaviour that should be explained more may serve as the subject of further research.

3.4.1 The Outputs of Design Science Research

Based on DSR results, Vaishnavi and Kuechler (2009) proposed the above five outputs that describe the levels and types of the knowledge, explained in Table 4 (Hevner et al. 2004; March & Smith, 1995).

Table 4: The Outputs of Design Science Research

Output	Description
Constructs	The conceptual vocabulary of a domain.
Models	A set of propositions or statements expressing relationships between constructs.
Methods	A set of steps used to perform a task (how-to-knowledge).
Instantiations	The operationalization of constructs, models and methods.
Better theories	Artefact construction as analogous to experimental natural science.

3.4.2 Why Design Science Research?

The aim of our research is to explore the problems with existing NFC transaction ecosystem models, design three novel transaction authentication protocols based on our proposed transaction architectures, and to carry out detailed security analysis of the proposed protocols. The overall aim of DSR model meets the requirements of this thesis' aim. Hevner, March, Park, and Ram (2004) explain that if the research in information systems and computing aims to transform an existing organisational or social related situation into a more desirable one by using novel artefacts, then it is considered as a DSR model. Since this thesis aims to explore novel and secure cloud-based NFC transaction authentication protocols, we argue that our research is highly consistent with DSR model. In the next section, we continue by describing our research steps according to the DSR process model proposed by Vaishnavi and Kuechler (2009).

3.5 Developing Designed Cloud-based NFC Payment Scenarios Based on DSR

After describing the DSR model, we now aim to design scenarios for cloud-based NFC transaction approaches that are most appropriate for mobile payments. Therefore, three potential approaches are explored throughout the DSR cycle, namely direct communication between the MNO and the merchant, merchant's authentication with single MNO and merchant's authentication with multiple MNOs.

The following sub-sections describe the way in which our proposed models are organised in accordance to the design science process. The aim and objectives of this research are associated to the previously discussed five stages proposed by Vaishnavi and Kuechler (2009). Each step represents a description of the way in which the payments models are designed and evaluated. However, the descriptions are brief since the space is limited in this chapter and thus a detailed description of each model is provided in the latter chapters. In the following three chapters (4,5 and 6) we will look more closely at each model, its respective protocol and discuss their importance to the process step. The below table illustrates a summary of the four iterations and their correspondence to each objective in this thesis.

Table 5: DSR Iterations and Research Objectives

DSR Iterations	Research Objectives
Iteration One: Library Research	Objective 1: To consider the existing NFC transaction models in order to understand the limitations which have been raised regarding the adoption of this technology.
Iteration Two: Initial Design Requirements (Ecosystem/Model design)	Objective 2: To develop a payment model based on the results and limitations obtained from consideration of the existing models and to propose ecosystem architectures so as to indicate the new frameworks.
Iteration Three: Protocol Design	Objective 3: To design and evaluate novel secure NFC transaction authentication protocols based on our proposed transaction architectures.
Iteration Four: Security Analysis and Validation	Objective 4: To carry out detail security analysis based on the proposed protocols in order to justify their utility and value.

3.5.1DSR Iteration One: Library Research (Targets Objective 1)

In order to following this iteration, a complete study of the literature was undertaken to understand the current deployed NFC transaction ecosystems as well as the existing SE management models. Indeed, this iteration was very challenging given the fact that there was not much academic relevant literature available regarding current deployed transaction models.

A. NFC Framework for the Literature Review

As shown in Figure 13 (Aydin, 2013 & Ozdenizci et al., 2010a), NFC theory and development, NFC infrastructure, NFC applications and services as well as NFC ecosystem are the four main categories which are distinguished in the NFC literature (Aydin, 2013;

Ozdenizci et al., 2010a). As this framework indicates, the primary level of the given framework is NFC theory and development. The papers that are written based on this area discuss the NFC development and applications, targeting behavioural issues which aim to provide theory justification instead of designing/developing artefacts. In below figure, in italics, we have pointed out where the work covered in this thesis lies.

According to this framework, *NFC infrastructure* and NFC applications and services are categorized as intermediate levels. There are three main factors which consider the NFC infrastructure. These factors are *network and communication issues*, *hardware issues considering antennae, readers, tags and NFC chip*; and *security and privacy* issues that deal mainly with designing and developing artefacts rather than focusing on behavioural issues. Since we are designing secure transaction authentication protocols based on our cloud-based NFC ecosystem scenarios, according to this framework our research falls into the NFC infrastructure category. NFC applications and service layer deals with application implementation, prototype development as well as artefact design evaluation which can be testing, field studies, experimental, etc. Normally, NFC operation modes have direct influence during NFC application investigation. The operation modes include read/write, card emulation and peer-to-peer modes.

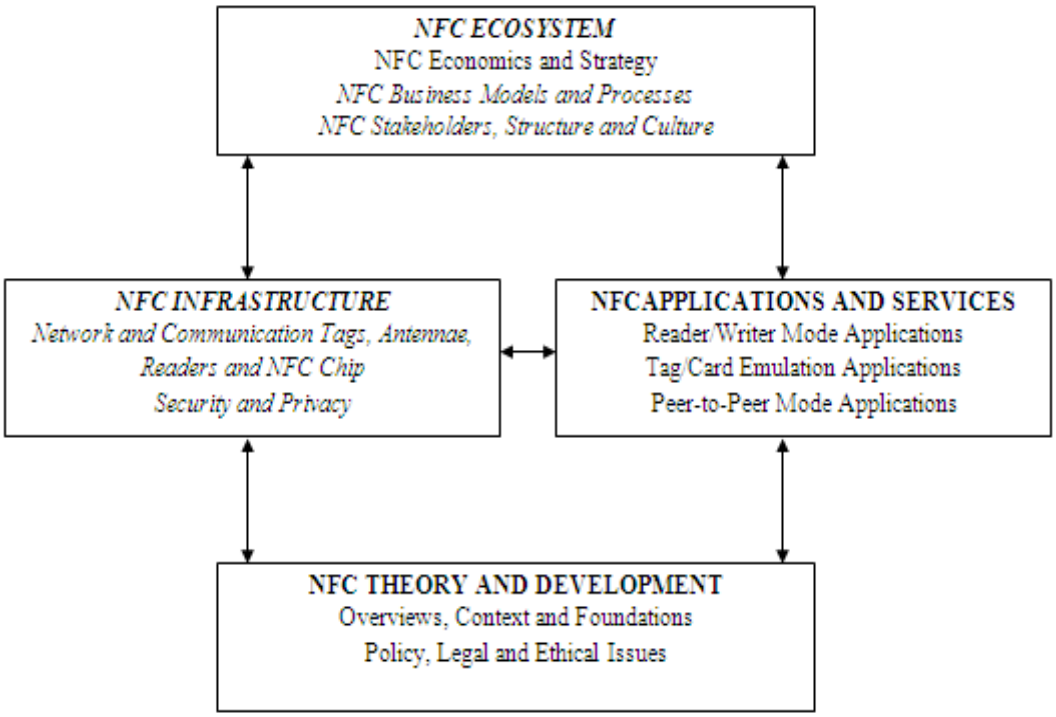

Figure 13: NFC Framework Classification

As the highest level of the NFC research framework, the *NFC ecosystem* stands above all other levels in the framework. This area has also its own issues in which can be further investigated. There are three main categories which examine the NFC ecosystem. These categories are NFC economics and strategy, *NFC business models and processes* and *NFC stakeholders*. The first two categories are more involved in business requirements, analysis and managerial side of the technology while the third category focuses on structure and culture which deals with social aspects of the NFC technology. These aspects can be named as characteristics, roles, and stakeholder capabilities which include technology adoption, user acceptance, manageability and control, reliability and usability. Additionally, stakeholders can be the MNO, service providers, etc. depending on the ecosystem architecture. We argue that our research also falls into this category since it defines new roles and access permissions for our designed ecosystem players. Our proposed protocols are based on novel ecosystem architectures which improve manageability and control of the transaction ecosystem to provide secure and flexible service.

We selected the identified criteria based on NFC transaction ecosystems and SE management models which needed to be considered: (1) *architecture*, (2) *security*, (3) *flexibility*, (4) *access rights, and* (5) *ownership.* After establishing these criteria, we utilised them to study different NFC transaction ecosystems along with SE management concerns. Retrospectively, we found out that although the existing models are implemented and are operating securely in a few countries, ideas such as cloud computing can be taken into consideration in order to improve the existing complexities in NFC ecosystems.

In order for us to investigate the gap in this research and design novel payment models, we studied the present NFC and mobile payment related works. As a result, in some cases we found that the existing issues concerning the deployment of this technology is the result of the previous proposed models. For instance, as, when we were considering Chen's mobile transaction authentication protocol (Chen et al., 2010), we noticed number of security flaws that have the potential to be fulfilled through integrating with our new cloud-based NFC transaction scenario. Therefore, we wanted to expand by conducting a new protocol design that focused on these issues. Table 6 provides a brief overview of the library research iteration. This evaluation enabled us to start the iteration two of our DSR research.

Table 6: DSR Iteration One (Library Research)

Problem	Studying different approaches for managing NFC payment ecosystems.
Suggestion	To identify and define: 1. Clear access permissions to the involved ecosystem players. 2. A novel NFC payment architectures which improve the existing issues such as security and controlling clients' credentials.
Outputs	***Model:*** Using a unique cloud-based architecture for NFC payment ecosystem. ***Construct:*** Security criteria (e.g. authentication, authorisation), manageability and flexibility. ***Method:*** Consideration of initial NFC payment ecosystem models.
Evaluation	The evaluation of the existing NFC payment ecosystems is required.
Conclusion	To design new NFC payment architectures in order to fulfil the existing issues.

3.5.2 DSR Iteration Two: Initial Design Requirements (Ecosystem/Model design)

This iteration targets the second objective of this research. In order for us to design and propose novel NFC payment ecosystem scenarios, we had to study existing business payment models to design our payment ecosystem architectures as a complementary model based on the main ecosystem players such as MNO, financial institution and the NFC phone holder (customer) to reduce the number of involved participants and consequently decrease the payment's complex issues in transaction operation. This method of considering communication interactions between ecosystem players resulted in designing novel NFC payment models.

Having reached this point of the research, we understood that authentication mechanisms also play a crucial role among the interactions that takes place between involved entities in payment ecosystem architectures. Therefore, we designed our payment ecosystem scenarios so that they fulfil possible security implications which might have arisen if we would not have considered transaction authentication protocols. As a result, we started analysing several

cloud-based NFC transaction architectures and scenarios. In this stage, we noticed that there is an important principle such as configuration requirements that needs to be considered. In fact, while analysing a number of design requirements based on the variety of ecosystem architectures, we realised that different security requirements typically need to have different architectures to be in place. Examples of these architecture and configuration requirements involve different authentication protocols that are based on the interactions relevant to their payment ecosystem models. Table 7 illustrates the second iteration.

Table 7: DSR Iteration Two (Initial Design Requirements)

Problem	Selecting secure and flexible payment scenarios for cloud-based NFC payments.
Suggestion	Analyse different possible scenario architectures in order to design ours.
Outputs	***Model:*** Improved selection scenarios (based on cloud technology). ***Construct:*** Security, authentication and flexibility criteria. ***Method:*** Analysing existing cloud-based payment architectures (e.g. Google wallet and MasterPass).
Evaluation	The configuration limitations and preferences of the design should be considered.
Conclusion	To finalize the design requirements of our protocols.

3.5.3 DSR Iteration Three: Protocol Design

This iteration targets the third objective of this research. As mentioned in the previous subsection, each ecosystem architecture involves configuring a number of fundamentals on their desired authentication protocol. These major configuration requirements reflect on the initial selected criteria of the ecosystem architecture. The process of designing secure transaction authentication protocols was based on the initial designed transaction scenarios which are discussed in chapter 4 and 5 of this thesis. For designing ecosystem scenarios as well as transaction authentication protocols, the configuration requirements are (1) *architecture*, (2) *security*, (3) *flexibility*, (4) *access rights, and* (5) *ownership.* We derived these configuration requirements based on the existing issues on NFC payment models which are the results of our comprehensive coverage of literature in this area.

After reaching this stage in which we recognised the protocol design requirements in the conducted design science research, we started to design our transaction authentication protocols. Table 8 illustrates the third iteration.

Table 8: DSR Iteration Three (Protocol Design)

Problem	Selecting payment ecosystem configurations for designing transaction authentication protocols.
Suggestion	Matching the initially designed ecosystem architectures to the required configurations for designing the protocols.
Outputs	***Model:*** propose novel transaction authentication protocols based on initially designed ecosystem architectures. ***Construct:*** security, authentication and flexibility criteria. ***Method:*** analysing the initially proposed ecosystem architectures against the configuration requirements for the protocols.
Evaluation	The transaction protocols are designed and fitted into our ecosystem scenarios.
Conclusion	The security analysis of such ecosystem scenarios with their respective protocols is required.

3.5.4 DSR Iteration Four: Security Analysis and Validation (Targets Objective 4)

Once successfully conducted the first three iteration of design science research, we moved to the stage in which we believed that the developed ecosystem scenarios and their respective protocols can be analysed from the security point of view to verify their utility and value. At that point, a security analysis of each proposed scenario with its respective protocol was carried out against multiple attack scenarios. The attack scenarios are designed based two aspects. Firstly, the possibilities of involved entities (e.g. customer, merchant and service provider) being dishonest and therefore not executing appropriately is discussed. In other

words, we sketched multiple scenarios where a buyer or a seller is dishonest and then analysed their success probability. This includes: (1) POS terminal impersonation as a customer, (2) POS terminal impersonation as MNO, (3) dishonest customer, (4) dishonest shop, (5) user interaction, and (6) disclosure of relevant information (more details in sections 4.6; 5.5; 6.2). Secondly, a broad analysis is provided considering the security of the exchanged messages in different stages based on the science of cryptography that ensures secure encryption (i.e. using MAC keys), transaction security, Non-repudiation of transaction messages (i.e. using digital signatures), new set of keys for every transaction (i.e. to avoid replay attacks).

The results of the security analysis indicate that the three novel transaction authentication protocols which were designed based on the initially proposed cloud-based NFC payment architectures can be used to facilitate new methods of managing the NFC transaction operation. Our proposed scenarios and their respective protocols provide three different approaches to tackle the problem of managing cloud-based NFC transaction ecosystems. These approaches are (1) *direct communication between the MNO and the merchant*, (2) *merchant's authentication with single MNO*, and (3) *merchant's authentication with multiple MNOs*. Since there are three entities (MNO, merchant and client) involved in every transaction, we designed and analysed three protocols which fulfil all three possible interaction scenarios. Each of these scenarios is described in more detail in chapter 4, 5 and 6 respectively. Furthermore, the security analyses of the proposed protocols are provided accordingly. Table 8 illustrates the fourth iteration.

Having analysed the proposed protocols from the security (cryptography) viewpoint, in order for us to ensure the protocols are further analysed to a sufficient extent, supplementary evaluation was carried out by conducting interviews with two different experts as part of this research. One of the experts was a senior security consultant in a telecom company and the other was a professor of information security specializing in smart cards.

Table 9: DSR Iteration Four (Security Analysis and Validation)

Problem	Ensuring the security and validity of proposed architectures and their respective protocols.
Suggestion	Analysing the proposed transaction authentication protocols from the security point of view.
Outputs	***Model:*** Develop security analysis against multiple attack scenarios. ***Construct:*** Security, validity, reliability of the proposed cloud-based NFC transaction authentication protocols/architectures. ***Method:*** Cryptographic analysis of the proposed protocols as well as conducting effective expert interviews
Evaluation	The protocols are secure against all attack scenarios.
Conclusion	The results are satisfactory.

Our strategy for handling this complexity is to carry out verification by interactive theorem proving; thereby shifting the complexity to the human who guides the theorem prover (Matsuo et al., 2010). The interview process consisted of the following three questions:

1. What are the strengths of the protocol?
2. What are the weaknesses of the protocol?
3. What would be the implications of the protocol implementation?

3.6 Summary

This chapter described our approach towards conducting this research. It started off by introducing research, design and related research perspectives. The research presented in this thesis is about building artefacts (cloud-based NFC transaction authentication protocols) and providing complementary security evaluations in order to define range of NFC payment models. Our goal is to help technology stakeholders to select the most reliable payment model and accelerate the adoption of NFC mobile payments. Therefore, we are dealing with an artificial science (information systems and computing) rather than a natural science. For

this reason, we selected the design science research methodology for this research. Furthermore, we described our selected methodology and provided its background information. DSR was linked to our protocols design, with the five steps process identified by Vaishnavi and Kuechler, (2009). This research aims to produce artefacts in the form of payment protocols in order to help mobile payment stakeholders to select the best-suited payment method. In the context of information systems and computing, the aim of DSR is to develop an artefact in order to improve/change the existing organisational and industrial situation (Hevner et al., 2004). Therefore, the aim of this research is highly consistent with the aim of DSR methodology.

In the following chapters we will continue by presenting the proposed models and their respective protocols continued by their security analyses that are conducted as part of this research.

Chapter 4 - First NFC Transaction Authentication Protocol: Direct Communication between the MNO and Merchant

4. Overview

This chapter targets objective 2 of our research. It describes our approach towards cloud-based NFC transactions and introduces our proposed model that is called "NFC Cloud Wallet". We introduce a new model for data storage in the SE in which the main SE is considered to be part of the cloud where all the customers' confidential information are stored; and another type of secure tamper-resistant chip is considered to be stored in the NFC phone to provide temporary storage and handle authentication mechanisms. Moreover, a novel secure NFC transaction protocol is designed based on the proposed model and its execution process is described in detail. Lastly, a security analysis of the proposed protocol is carried out in order to justify the reliability and validity of our protocol in the security domain.

4.1 The Concept of Mobile Wallet

Recently, mobile wallet and mobile payment concepts have increased the attention of researchers and it seems that users have found it easy and convenient to pay with their mobile phones (Fisher & Guha, 2013). Up to now, people seem to accept that the future is in mobile devices but the problem has just begun for industrial stakeholders. There are several unanswered questions regarding the method(s) which a mobile payment process should follow in order to be deployed in a satisfactory manner. One of the main concerns of stakeholders is bringing the idea of cloud computing into the concept of NFC payments. Is there a need for cloud? Would NFC do the job on its own? It seems that they are not quite sure about the right solution as well as the right-to-go market strategy for mobile payments

(Lehdonvirta et al., 2009). Thus, there is not much agreement in the minds of mobile wallet stakeholders. PayPal, Telefonica/O2, and Best Buy have announced wallets that are using cloud technology and are accordingly classified as cloud wallets (Yarbrough & Taylor, 2012). Additionally, Google, ISIS and Visa have developed solutions that use NFC as the main technology and are also called wallets (Google Wallet, 2013; Schamberger et al., 2013; Visa, 2013).

The question that remains unanswered is which technology will finally get accepted by consumers and merchants? Answering this question requires some time, as what consumers prefer may not benefit the merchants and vice-versa. Therefore, at present, many advertisements and trials are in place in an attempt to make up the minds of both stakeholders and consumers as to what solution will ultimately be adopted. To start discussing possible solutions, it is best to consider both NFC and cloud payments first.

4.1.1 NFC Wallet

For NFC wallet payments, a special chip is required to be stored in the phone. There is also a need for a mobile application (app) to enable the consumer to login to the app in order to use it and make a payment. When logging to the app, the consumer should enter a password to confirm his identity. Once logged in to the app, the consumer can use the app and scan his phone on a nearby POS terminal to send the payment request to the merchant. From the consumer and merchant point of view, this is the same procedure as EMV PIN payments. The main benefit that this method of payment has for consumers is the convenience that it brings in busy environments such as train stations. For example, consumers can quickly scan their phones on the merchant POS terminal and top up their travel cards.

In many cases, the focus of NFC wallets are to improve the loyalty experience of consumers by allowing them to integrate different applications into one single app and have the auto redeem at the merchant terminal. This provides a much easier method for consumers compared to traditional cutting out coupons.

4.1.2 Cloud Wallet

Similar to the NFC wallet, a mobile application is required for cloud wallet. By registering the required information (e.g. credit card details) to service providers, consumers can use their phones for one click check outs in e-commerce. The registered information of the consumer is saved in an offline database, but the SP enables the consumer to use his information from the offline database when he aims to make a payment. Consumers pay money into their cloud accounts (prepaid account) from their bank and when they use their phones to make a payment, the required funds are withdrawn from their cloud wallet. Cloud wallet is an improvement to the existing Telefonica and PayPal services since, from the merchant's point of view, in a POS retail situation, consumers can simply enter a password on their app when making a payment and that password confirms the consumer's identity in addition to completing the transaction process. Although the NFC wallet is more practical than the cloud wallet solution, the latter solution sounds more interesting to merchants as they are not required to make an investment in order to update their POS terminals for making them compatible with NFC devices.

4.2 Data Stored in Cloud

There are two main components in an NFC enabled handset: the SE and NFC controller. As mentioned earlier in section 2.5 of this thesis, the SE is responsible for providing secure storage for sensitive data while the NFC controller enables short-range data transmission. Although the number of NFC handsets is increasing in the market, NFC payments are not widely adopted yet. The main reason for this is the existing issues with managing and controlling access to the SE (Kranz et al., 2013). At present, operation of NFC payments requires the participation of both card issuers and SE owners that should be established through a defined relationship. In the concept of cloud-based NFC payments, the ecosystem architecture is designed in a different way in which the main SE is stored in the cloud (virtual SE) and the NFC controller stays in the handset in order to provide a limited and temporary space for authentication assets to deal with authentication processes between the NFC phone and the POS terminal. This approach is beneficial in terms of controlling the SE (card issuer access the SE easily). In this case, client credentials are stored in the virtual SE rather than being stored locally in the NFC handset. When a client scans his/her NFC phone on the POS terminal to make a payment, transaction credentials are transmitted from the virtual SE to the

NFC handset and from there to the POS terminal. The NFC controller is responsible for handling the authentication between the NFC phone and the POS terminal. The newer version of Google Wallet which was launched in August 2012 (Google, 2013) is based on this approach; however, it is not widely implemented yet. Google has provided a central cloud environment where clients' payment credentials are kept. Thus, clients are able to link different credit cards with their mobile wallet service. For example Google Wallet customers can add their Visa, MasterCard, American Express and Discover cards to their mobile wallet service. This increases the flexibility compared to the previously discussed model where data is stored in the SE that is installed in the NFC handset. The Google Wallet solution also defines a proxy card in the handset to enable the transaction at the POS terminal; nonetheless customer payment credentials are still stored in the virtual SE located in the cloud. Storing client credentials in the cloud has some advantages and disadvantages which are discussed below.

From a portability point of view, a wallet service can be available on any device which the user is authenticated to. Moreover, data transmission method from the NFC phone to the POS terminal can be through a variety of methods such as an NFC link. Having customer credentials in the cloud thus makes it easier for cardholders and financial institutions to get their card into the wallet. As the SE does not exist in the phone architecture anymore, there is no third party in control of the SE, those by improving the security, flexibility and manageability of the service. One of the main challenges of this solution is data security, which has always been the main concern of people and technology providers. In this approach, the mobile phone has a key role in data communication as it becomes a conduit for data passing from the cloud to reach the POS terminal. Not having a proper security design on the phone may result in data leakage. On the other hand, an internet connection (WiFi or 3G/4G) is required in order to deliver data from the cloud to the phone to be used at the POS terminal. Connection speed thus definitely has a major impact on the overall service, as slow connectivity or unavailability of Internet connection prevents the service operation. Therefore, properly designed solutions must be in place to ensure transaction data are available at the POS terminal. (e.g. transaction data can be stored on the phone in advance of the payment).

4.2.1 The Concept of NFC Cloud Wallet

Although the use of the SE as a main secure component in an NFC mobile phone was a good start for development of this technology, however once it got to the real stage of its global implementation, the ecosystem players faced many problems (Curran et al., 2012). We believe bringing the cloud infrastructure into the NFC business helps to overcome many of the current problems. Additionally, a cloud-based approach offers several advantages over the use of SE as a single secure component in terms of managing sensitive data for an NFC transaction. Moreover, according to the speed of the present generation mobile data services (Agar, 2013; Pailles et al., 2010), it seems an NFC cloud-based approach needs another 2 to 3 years to become commercially feasible.

The NFC cloud-based approach introduces a new method of storing, managing and accessing sensitive transaction data by storing customers' payment data in the cloud (referred to as a virtual SE) rather than the mobile phone. When a transaction is carried out, the required data is pulled out from a remote virtual SE which is stored within the cloud environment and pushed into the mobile phone's SE in an encrypted format. The mobile phone's SE provides temporary storage and authentication assets for the transaction to take place. After reaching the SE in an NFC phone, data are again pulled out from the handset and reach the vendor's terminal. In addition, the communication between the cloud provider and the vendor's terminal is established through an NFC link. The cloud-based transaction method provides the "card present" payment, since the NFC phone's SE only deals with the authentication between the handset and the POS terminal. This solution enables the NFC phone to be linked to multiple virtual SEs (stored in the cloud) that allows any user to access its own SE in order to modify the information (e.g. to add/delete applications).

In the NFC cloud-based approach, the phone's SE can only be responsible for user/device authentication and not for storing data. This solution increases the cost efficiency compared to the current costs that SE makes for a company. In addition, the NFC controller chips will be smaller and cheaper as they would not have to support all functionalities. Furthermore, the concept of the SE can be completely avoided by replacing it with the concept of a trusted zone that can be created within the processor of a mobile phone. Moreover, the storage capacity of the SE should be large enough in order to store user applications with unknown sizes. Since the user may wish to add more applications to his NFC phone, this issue brings a

limitation for existing solutions as each SE supports a certain storage capacity. The other issue with the SE is that, companies have to meet the requirements of organisations such as EMVco (EMVCo, 2007) to provide high level security in order to store the card's data. This approach makes the SE expensive for the companies, while the cloud-based approach reduces this cost.

Since users' critical information is stored in the cloud, they do not need to be concerned about their mobile wallets any longer. In order for the users to change their mobile wallet information, they can easily use the virtual SE (stored in the cloud) to access the information they require online via a web browser. This approach improves SP services as they are no longer required to develop different applications for different types of mobile phones. Additionally, it reduces the risk of a third party to get unauthorized access while the phone is being shipped to a new user or for repairing purposes. This is because there is no SE which contains the user's confidential information in the NFC phone as that information is now stored in a cloud environment and not in the handset itself. Moreover, the NFC cloud-based approach makes the business simpler for companies in terms of the integration of SE card provisioning. It would be much easier for businesses to implement NFC services without having to perform card provisioning for every single SE. An NFC phone user will be able to access an unlimited number of applications as they are stored within a cloud secure server and not in a physical SE. In terms of flexibility, all users would be able to access all their applications from all their devices (e.g. phones, tablets or laptops) since the applications are stored in a cloud environment that provides a secure storage space. Moreover, fraud detection would be instant as the system fully runs in an online mode.

The acceptance of the NFC cloud-based transaction method is dependent on having the ability to implement strong authentication mechanisms as well as on conducting transactions quickly enough in order to increase the performance. Reassuringly, the processing times are far quicker in this approach because the main SE is stored in a cloud where there is more computing power available, in contrast with a stored SE on a mobile device. However, more time is required for data requests to reach the cloud server and return back to the POS terminal.

To summarise, the NFC cloud-based solution offers potentially infinite computing services and extensive capabilities in terms of storage, networking of shared devices and computing. The solution provides broad capabilities to enable the use of different platforms bringing the user into ubiquitous computing. The different virtual and physical needs of clients makes the cloud-based NFC a flexible technology. Therefore the technology should be capable of providing the infrastructure necessary in order to enable the consumers to manage their resources in the most effective way.

4.3 NFC Cloud Wallet Model

This model proposes the idea of using cloud computing to manage NFC payment applications. This result in a flexible and secure management process, concurrently easing the application personalization and ownership for both customers and service providers to this end, the proposed NFC cloud wallet architecture provides easy management of multiple users and delivers personalized contents to each user. It supports intelligent profiling functions by managing customized information relevant to each user in certain environments, which updates the service offers and user profiles dynamically. Depending on the MNO’s network reception, deployment of this service takes around one minute and deployments can be scaled to any number of users.

The idea of this approach is that every time the customer makes a purchase, the payment application which contains the customer's credentials is downloaded into the phone’s SE from the cloud and, after the transaction, it is deleted from the device and the cloud will update itself to keep a correct record of the customer's account balance. Figure 14 illustrates the steps that should be undertaken to complete the transaction process. The execution of the model is described in what follows:

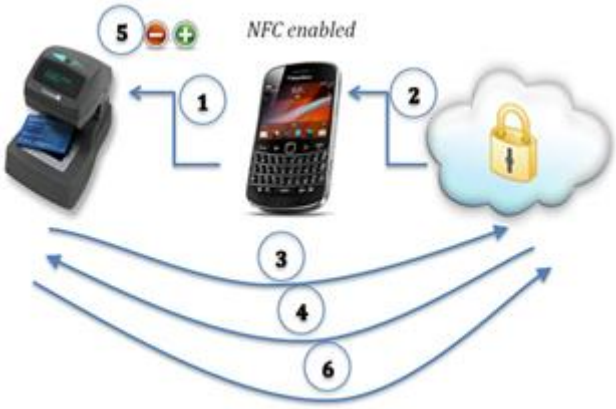

Figure 14: NFC Cloud Wallet

1. The customer scans his/her NFC phone on the merchant's POS terminal to make a payment.
2. The payment application is downloaded from the virtual SE into the customer's phone SE.
3. The merchant's POS terminal communicates with the cloud provider to check whether the customer has enough credit or not.
4. The cloud provider transfers the requested information to the merchant's POS terminal.
5. Based on the information transferred to the merchant, the merchant informs the cloud to either authorize the transaction or reject the customer request.
6. If the customer has sufficient amount of money in his account to make the purchase, the merchant sends the payment information to the cloud and the finance department (a sub-system of the cloud) updates the customer's balance - if the customer's request is authorized, the amount of purchase will be withdrawn from his account otherwise the customer's account will remain with the same balance.

As an addition to this model, we suggest that when the NFC enabled phone sends a request to its cloud provider to get permission to make a payment (step 1), the cloud provider sends a SMS requesting a PIN number to identify the user of the phone - this is how the cloud provider ensures the legitimacy of the phone user. For verification purposes, the customer sends the PIN back to the cloud provider as an SMS.

To extend this model, There are two possible ways to follow this approach: Firstly, the financial institution can be the cloud owner from which the payment application can be downloaded from/into the customer's mobile device; the MNO can be linked to the financial

institution (that is the cloud owner in this case) or it can stand as a separate party. Secondly, the financial institution could have a contract with a third party company such as PayPal that has its own cloud infrastructure (whilst the MNO can be linked with them, it also can stand as a separate party) or the financial institution uses another company's cloud service such as IBM, Microsoft, etc. (the MNO can be linked with either financial institution, cloud provider or it can stand as a separate party).

This approach provides a comprehensive leadership of the cloud provider towards managing and controlling the customer's information and allows the phone's SE to deal with authentication mechanisms rather than storing and managing the required transaction information. Additionally, in the cloud-based payment architecture the processes of assigning different service profiles to multi-clients are performed in a flexible routine while it provides fast and easy delivery of personalized profiles to every client. The personalized profiles can also be dynamically updated or customized for particular clients' requests through managing the content of each client's profile in the cloud in addition to its associated NFC tag. The mobile network coverage of the carrier certainly has an impact on the download speed of applications as well as the whole process. In the case of excellent mobile network coverage, the download time/process will be less than when the network coverage is poor.

4.3.1 Ecosystem Scenarios

In this section, we propose two ecosystem scenarios and discuss the assumptions we made in order to design our protocol. The proposed ecosystem scenarios are listed below.

1. Direct Link between the POS and the MNO
2. Unlinked POS and MNO (Vendor trusts MNO)

In this chapter, a secure transaction authentication protocol is designed based on the first ecosystem scenario in which the merchant and the MNO have a direct communication channel. Subsequently, a security analysis of the proposed protocol is provided in order to justify the reliability and validity of the protocol from the security perspective. The second scenario however will be looked at in the next chapter.

4.3.2 Direct Link between the MNO and Merchant

We propose an extension to NFC Cloud Wallet model. Since there are multiple options applicable to this model, we design our ecosystem model based on the following assumptions:

- The SE is part of the SIM;
- The cloud is part of the MNO;
- The MNO manages the SE/SIM (SE in the form of UICC);
- Banks, etc. are part of the MNO;

Figure 15 demonstrates the ecosystem scenario in which the merchant and the MNO have direct communication.

Figure 15: Direct communication between POS and MNO

These assumptions are appropriate regarding NFC execution process and its ecosystem architecture. For instance, in the SIM/UICC architecture proposed in SP-driven model launched by Robabank in Netherlands (see section 2.9.5), they suggest that the MNO to be owned by the bank itself in order to improve the complexities of the ownership and access right permissions in the payment ecosystem architecture. However, this could be done vice-versa. i.e. the MNO could be the owner of the bank. Our fourth assumption in the first ecosystem scenario is also based on this model in which we assume the bank is part of the MNO or the bank is securely linked with the MNO. Thus, in chapter 5 and 6 we use this assumption in order to design two more transaction authentication protocols based on the

second ecosystem scenario mentioned in section 4.3.1. As discussed in chapter 2 previously, the SE is in the form of a UICC therefore, the SE is part of the SIM and the MNO manages the SIM accordingly (assumptions 1 and 3). In assumption 2, the MNO manages the cloud infrastructure and it is the only party that has full access and permission to manage confidential data stored in the cloud. For example, Verzion – a mobile network carrier based in the US – has recently (Verizon, 2013; Schneiderman, 2011) entered the cloud market and offers a broad range of cloud services to its customers. Moreover, AT&T – another US based mobile network carrier – is also providing cloud storage for its customers (AT&T, 2013; Marston et al., 2011). In our scenario, since the MNO is the owner of the cloud, it fully manages the SIM in terms of monitoring the GSM network and controlling the cloud's data. From the financial institution's point of view, it only deals with the MNO, as it is the only party that has full control over the SIM and the cloud.

Since GSM is still a widely used network as a mobile standard and our cellular calls are mostly based on GSM, we use the existing features of this technology in our model. The following section describes the GSM authentication process.

4.4 GSM Authentication

When a mobile device signs into a network, the MNO first authenticates the device (specifically the SIM). The authentication stage verifies the identity and validity of the SIM and ensures that the subscriber has authorized access to the network. The Authentication Centre (AuC) of the MNO is responsible for authenticating each SIM that attempts to connect to the GSM core network through Mobile Switching Centre (*MSC*). The AuC stores two encryption algorithms A3 and A8 (Kiselev & Tokareva, 2012), as well as a list of all subscribers identity along with corresponding secret key K_i. This key is also stored in the SIM. The AuC first generates a random number known as *R*. This *R* is used to generate two responses, signed response S and key K_c as shown in figure 16, where $S = E_{Ki}\ (R)$ using the A3 algorithm and $K_c = E_{Ki}\ (R)$ using the A8 algorithm (ETSI, 1996).

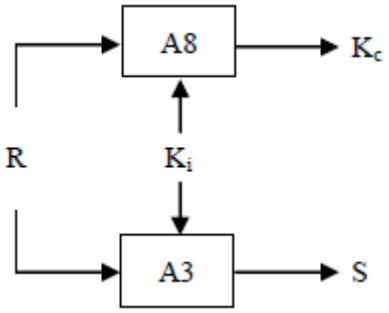

Figure 16: Generation of K_c and S from R

The triplet (R, S, K_c) is known as the Authentication triplet generated by the AuC. The AuC sends this triplet to the MSC. On receiving a triplet from the AuC,the MSC sends R (the first part of the triplet) to the mobile device. The SIM of the mobile device computes the response S from R, as K_i is already stored in the SIM. The mobile device transmits S to the MSC. If this S matches the S in the triplet (which it should in case of a valid SIM), then the mobile is authenticated. K_c is used for communication encryption between the mobile station and the MNO. Having described the GSM authentication, in the following section we propose our protocol, which has been inspired from Chen et al. protocol (Section 2.12 - C).

4.5 The Proposed Protocol

Our proposal is based on the cloud architecture where the cloud is being managed by the MNO. The cloud and the banking sector are the subsystems of the MNO in our proposal, in addition to the existing subsystems of an MNO. We assume that the communication is secure between various subsystems of the MNO. The shop POS terminal, registered with one or more MNOs, shares an MNO specific secret key K_p with the corresponding MNO. This key is issued once a shop is registered with the MNO. The bank details of the merchant are also registered with the MNO for monetary transactions. The communication between the merchant's POS terminal and the mobile device is wireless using NFC peer-to-peer mode technology (section 2.4.1-B). The mobile device has a valid SIM. We used the existing feature of GSM network for mutual authentication. A recent study by Chen, Hancke, Mayes, Lien and Chiu (2010) proposed a mechanism for GSM authentication in an NFC environment. We tailored their model according to our requirement in our proposed architecture. The detailed execution of our protocol is described in Figure 17.

The proposed protocol executes in three different phases: Authentication, Keys generation and Transaction. The protocol initiates when the customer places his cell phone for the payment after agreeing to the total price displayed on the shop POS terminal. The details of these phases are described in what follows:

4.5.1 Phase 1: Authentication

Step 1: As soon as the user places his mobile device, the NFC link between the mobile device and the shop POS terminal is established. The shop POS terminal sends an ID Request message to the mobile device.

Steps 2-3: The mobile device sends *TMSI*, *LAI* as its ID. On receipt of the information from the mobile device, the shop POS terminal determines the user's mobile network. The network code is available in LAI in the form of Mobile Country Code (*MCC*) and Mobile Network Code (*MNC*). An *MNC* is used in combination with *MCC* (also known as a *'MCC/MNC tuple'*) to uniquely identify a mobile phone operator/carrier (Technical Specification Group Core Network, 1999).

Steps 4-5: The shop POS terminal sends *TMSI*, *LAI*, and Shop ID to respective MNO for customer authentication and shop identification.

Step 5.1: In case of incorrect *TMSI*, a declined message is sent.

Step 6: In case of correct identification, the MNO generates one set of authentication triplet (R, S, K_c) and sends R to mobile device through shop POS terminal (as described in section 4.4).

Steps 7-8: SIM computes K_c from R as explained in Section 4.4. The SIM generates a random number R_s and concatenates with R, encrypts with key K_c and sends it to the MNO through shop POS terminal.

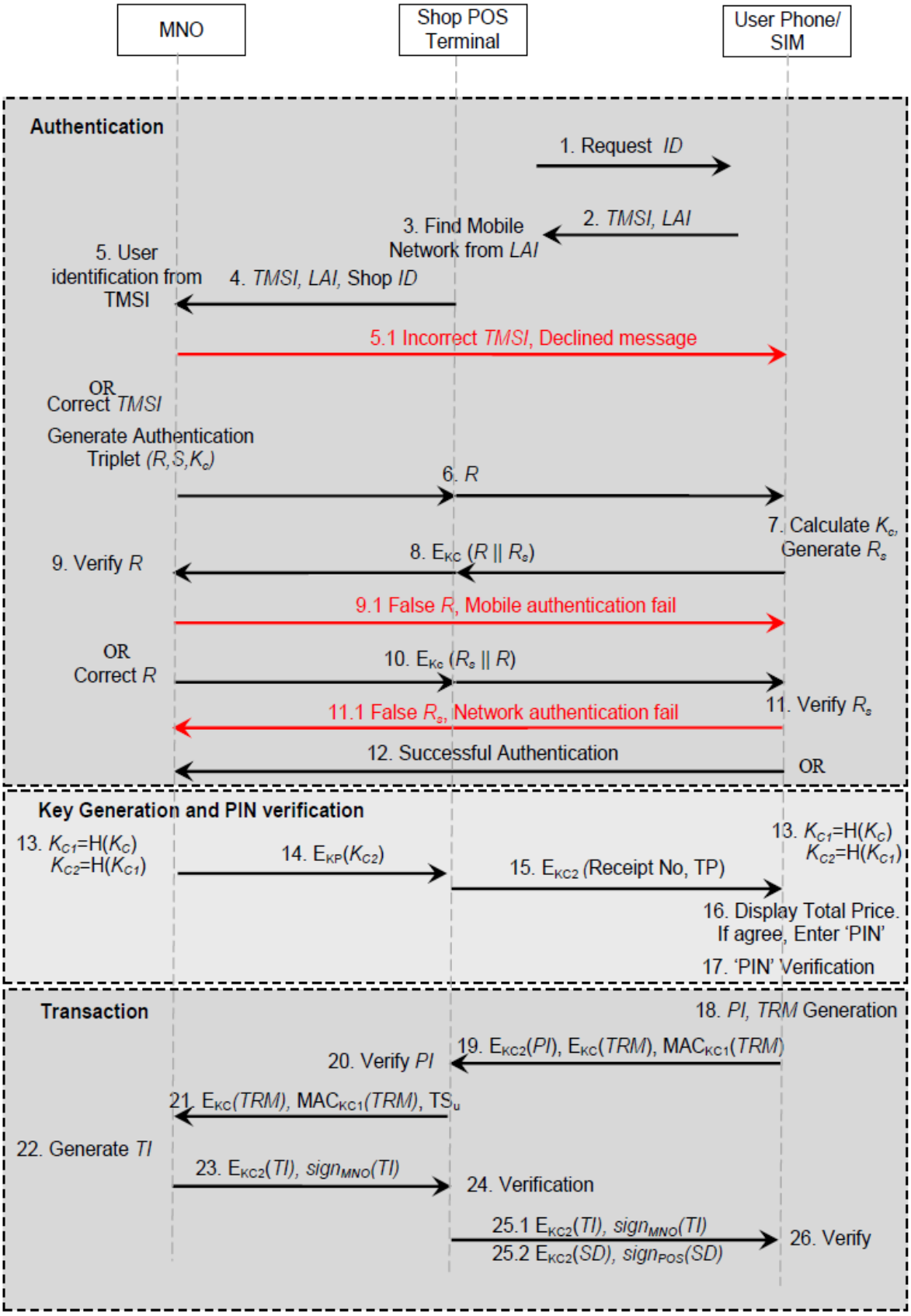

Figure 17: The Proposed Protocol

Steps 9-10: The MNO checks the validity of the SIM (or mobile device). It receives E_{kc} ($R||R_s$) from the mobile device and decrypts the message by K_c, the key it already has in authentication triplet. The MNO compares the R in the authentication triplet with the *R* in the response. In case they do not match, a 'Stop' message is sent to the mobile device and the protocol execution is stopped. If both R are same, then the mobile is authenticated for a valid SIM. In this case, the MNO swaps *R* and R_s, encrypts with K_c and sends it to mobile device.

Steps 11-12: This step authenticates the MNO to the mobile device. The mobile device receives the response E_{kc} $(R_s||R)$ and decrypts it with the key K_c already computed in Step 7. The mobile device compares both *R* and R_s. If both are same, then the MNO is authenticated and a 'successful authentication' message is sent to the MNO.

4.5.2 Phase 2: Keys Generation and PIN Verification

Steps 13-14: K_p is a shared secret between the MNO and the shop POS terminal. K_c is the shared secret between the MNO and the customer's mobile device (computed in step 7). There is no shared secret between the POS terminal and the mobile device till this stage. The MNO and mobile device compute a one-way hash function of K_c to generate K_{c1}, the key that will be used for MAC calculation. The MNO then computes K_{c2} from K_{c1} using a one-way hash function and sends it to shop POS terminal by encrypting it with K_p. The mobile device also computes K_{c2} as it already has K_{c1}. K_{c2} is the encryption key between MNO, shop POS terminal and the customer's mobile device.

Steps 15-17: The shop POS terminal sends the Total Price (*TP*) and the Receipt Number encrypted with K_{c2}. The user's mobile device decrypts the information and displays it to the user. If he agrees, he enters the PIN. The PIN is an additional layer of security and adds trust between the user and the shopkeeper. A PIN binds a user with his mobile device, so the shopkeeper is to believe that the user is the legitimate owner of the mobile device. Moreover, the user feels more secure as no one else can use his mobile device for transaction without his consent. PIN is stored in a secure location in the SIM. The SIM compares both PINs and if both are same, the user is authenticated as the legitimate user of the mobile device. Otherwise, the protocol is stopped.

4.5.3 Phase 3: Transaction

Step 18: The customer's cell phone generates two messages, *PI* and *TRM*, such that;

$$PI = (Receipt\ No, Total\ Price, Time\ Stamp\ (TS_U))$$
$$TRM = (PI, R_s, Transaction\ Counter)$$

Step 19: TS_U represents the exact time and date the transaction has been committed by the user. *TC* is a counter that is incremented after each transaction and is used to prevent replay attack. *PI* is encrypted with K_{c2} so that it can be verified by the shop POS terminal. The user encrypts the *TRM* with K_c so that it cannot be modified by the shop terminal. The user computes MAC with K_{c1} over the *TRM* using Encrypt-then-MAC approach for integrity protection.

Steps 20-21: The POS terminal can decrypt only the *PI* encrypted with by K_{c2} to check its correctness. The POS terminal does not need to verify the MAC (and it cannot do so), as it already knows the main contents of *PI*. The Shop POS terminal also verifies the TS_U to be in a defined time window. If *PI* is correct, the POS terminal relays the encrypted *TRM* with corresponding MAC along with the TS_U to the MNO.

Step 22: On receipt of the message, the MNO checks the integrity of the message by verifying the MAC with K_{c1}. If the MAC is invalid, the transaction execution is stopped. In case of a valid MAC, the MNO decrypts the message. The MNO compares the R_s in the *TRM* with the R_s received earlier in the authentication phase. A correct match confirms that the user is the same who was earlier authenticated. It also verifies the *TC* and TS_U. In case of successful verification, the MNO communicates with the concerned subsections for monetary transaction. The concerned subsections of the MNO check the credit limit of the user, and, if satisfied, execute the transaction. Once the transaction is executed, the MNO generates a Transaction Information (*TI*) message as:

$$TI = (Transaction\ Serial\ Number, Amount, TS_{Tr})$$

Steps 23-25: The MNO encrypts *TI* with K_{c2}, digitally signs the message and sends it to the shop POS terminal. The POS terminal verifies the signature. A valid signature indicates a

correct *TI*. The POS also verifies the *TI* for the amount mentioned in the *TI*. In case of successful verification, the POS terminal appends the message it received from the MNO with the Shopping Details (*SD*) and corresponding digital signature.

Step 26: The user verifies both signatures. It verifies the contents of *TI* and *SD*.

4.6 Protocol Analysis

In this section, we analyse our proposed model from multiple security aspects. This analysis encompasses the authentication and security of the messages among customer, shop POS terminal and the MNO. The analysis also includes multiple attack scenarios, such as a customer is dishonest and has intentions to pay less, or the shopkeeper is dishonest and has plans to receive more money.

4.6.1 Mutual Authentication

A mutual authentication between a customer and MNO occurs whenever the customer agrees to pay some amount. Since this authentication is performed through a shop's POS terminal, we analyse our protocol from the perspective that the POS terminal has some malicious intentions. In this case, there can be the following two scenarios:

POS Terminal Impersonation as a Customer

We assume that the shop POS terminal is dishonest and keeps a record of all messages against a legitimate customer (referred to as 'target customer'). The aim of the shopkeeper is to transfer money from the target customer without his/her consent. The shop POS terminal impersonates a target customer to the MNO by replaying message 4. In case the *TMSI* and *LAI* are valid at that time (the chances are higher if the message is replayed just after the legitimate transaction of the target customer), the MNO will send a random number *R* to the terminal. *R* is a 128 bit random number generated by the MNO so the chances for its repetition are almost negligible. The shopkeeper cannot compute a valid response in step 8 for a different *R*, as the shop lacks K_i to compute K_c. Therefore, a shop cannot successfully impersonate as a customer by replaying old messages.

POS Terminal Impersonation as MNO

In this scenario, we assume that the shop is dishonest and communicates with a target customer without establishing a communication link with the MNO. Again, we assume that the shop keeps a record of legitimate messages of the target customer. The shop sends message 1 (Request ID) to the target customer and gets its response in message 2. Since the shop does not communicate with MNO in this scenario, it does not send message 4 to the MNO. However, the shop replays the recorded R in message 6 to the target customer. The target customer believes that he has been correctly identified by the MNO and the R is actually generated the MNO. So the user computes a response and sends it in message 8 to the shop. Message 8 contains R_s encrypted with the K_c. The R_s is a random number generated by the SIM and is different in each transaction. So, message 8 will be different than the one already recorded with the shop. Since message 8 is different, the shop can neither replay message 10, as it will be different for this transaction, nor can it compute a valid message 10. This scenario is, again, not successful.

4.6.2 Encryption and MAC Keys

Separate keys are used for encryption and MAC calculation making the protocol more secure. Encrypt-then-MAC is an approach where the ciphertext is generated by encrypting the plaintext and then appending a MAC of the encrypted plaintext. This approach is cryptographically more secure than other approaches (Bellare & Namprempre 2000). Apart from the cryptographic advantage, the MAC can be verified without performing decryption. So, if the MAC is invalid for a message, the message is discarded without decryption. This results in computational efficiency.

4.6.3 User Interaction

The user interaction with the system is reduced to a single interaction making it a user-friendly protocol. Moreover, the user feels more secure as the transaction is protected by PIN verification. There are chances that a user withdraws his mobile device from NFC terminal as a psychological move to enter PIN. This will break the NFC link, but, as the PIN is stored in the SIM, it does not require a NFC link for verification. Once the user PIN has been verified by the SIM, the user places his mobile device back on the NFC terminal and the protocol

resumes from the same point. There are chances that a dishonest user could withdraw his/her mobile device in order to enter the PIN, and then places it back on another mobile device for transaction. To counter this threat, R_s is transmitted by the mobile device in Transaction Request Message (message 19). R_s is generated by the SIM and is encrypted with K_c (message 7, 8), so it cannot be eavesdropped in the authentication phase. This ensures that the mobile device does not change.

4.6.4 Disclosure of Relevant Information

The protocol is designed considering disclosure of information on a need to know basis. For example, *TC* is a counter that increments after each successful transaction. The record of the *TC* is kept by both, the user and the MNO. Shop POS terminal does not need to know the *TC*. In our proposed protocol, the *TC* is not exposed to POS terminal as it is a part of the *TRM*. Similarly, the MNO does not need to know the shopping details of the customer. Therefore, only the total amount is transmitted to the MNO for transaction.

4.6.5 Transaction Security

The transaction phase of the protocol requires maximum security. The *TRM* message is initiated by the customer rather than the shop terminal in order to satisfy the customer. The integrity of the *TRM* message is protected by the MAC so any alteration in this message is not possible. Message 19 is designed in such a way that the first half of the message containing encrypted *PI* is for the shop's POS terminal, which can decrypt and check the authenticity of the payment information. The remaining half of the message, containing encrypted *TRM* and corresponding MAC can neither be decrypted nor altered by the shop's POS terminal. The POS terminal relays the remaining half to the MNO along with the Time Stamp. Hence, the transaction information generated by the customer is relayed to the MNO without any alteration. In this phase, there can be a scenario where a dishonest customer has an intention of paying less than the actual amount. Accordingly, the customer designs a malicious *TRM* message (*TRM´*) consisting of *PI´* (an illegitimate payment information, *PI´* < *PI*). The dishonest customer then forms message 19 as:

$$PI = \text{Receipt Number, Total Price, Time Stamp } TS_U$$

$$TRM' = PI', R_s, \text{Transaction Counter (TC)}$$

It may be noted that the *PI* is legitimate whereas the *TRM´* consists of amended *PI (PI´)*. The dishonest customer forms message 19 as:

$$Message\ 19 = E_{kc2}(PI),\ E_{Kc}(TRM´),\ MAC_{Kc1}(TRM´)$$

The first half of the message, consisting of encrypted *PI*, is legitimate and the shop can verify it. However, the malicious part cannot be decrypted by the shop, so the shop cannot determine that the remaining part contains amended price information. The shop forms message 21 as *PI* is verified. The MNO executes the transaction with an amended price and forms message 23 and digitally signs it. Message 23 contains the information about the amount deducted from the customer. Once this message is received by the shop terminal, the shop detects that the deducted amount is not the same as required. Hence, a dishonest customer with the intention to pay a lesser amount does not succeed in our proposed design.

4.6.6 New Set of Keys for every Transaction

The keys are generated from a random number *R* (generated by the MNO), which acts as a seed for all keys. As *R* is fresh for every transaction, therefore the keys are also new in each transaction.

4.6.7 Non-repudiation of Transaction Messages

The transaction result messages (message 23, message 25) are digitally signed. In case of any dispute about the payment, the MNO is to honour message 23 as it contains the MNO's digital signature. The shopping detail is also digitally signed by the shop POS terminal so the shop has to honour the prices mentioned in this message. Therefore the customer is completely secured in transaction.

4.6.8 Securing Long Term Secret

K_p is the long term secret between the MNO and shop POS terminal. In our protocol, K_p is used with the least exposure (only once). The security policy of the MNO can define the update of this key after a defined interval.

The above proposed transaction protocol provides secure communication channels to the communicating parties. The proposed protocol is based on the NFC Cloud Wallet model for secure cloud-based NFC transaction authentication. The operations performed by the vendor's reader, an NFC enabled phone and the cloud provider (the MNO) are provided, with such operations being possible thanks to the current state of technology, as most of these measures are already implemented to support other mechanisms.

4.7 Expert Review Evaluation

As a motivating and challenging problem, cryptographic protocols should be designed in a way to support even worst-case assumptions. These assumptions may still provide the opportunity for adversaries to eavesdropped and/or modify the transmitting messages inside the communication channel. Moreover, the cryptographic techniques may not themselves provide complete security since a number of attacks can be conducted to break such properties. Man-In-The-Middle attack is one of such attacks that enables the attacker to take control over the message execution sessions with impersonation techniques. Furthermore, replay (playback) attacks are also possible where the attacker records the previous messages and retransmit them. Another type of an attack is called reflection attack where the adversary sends back the initiated message to the originator; and type flaw attack where the intruder substitutes different messages into a protocol – for example an attacker can alter the name with a key.

Normally, these attacks are simply overlooked, as it is problematic for humans, even by a detailed review of simple protocols, to control all the complex ways that different protocol sessions could be interleaved together, with possible interferences coming from an adversary. What is needed are methods to speed up the development and analysis of cryptographic protocols. Moreover, if these methods are to be used to certify protocols, then they must be mathematically precise, so that exact statements are possible about the scope and significance of the analysis results. This role can be filled by analysing the technical properties of the protocol against multiple attack scenarios in order to assure that the protocol satisfies the given objectives.

4.7.1 Scenario Evaluation

The scenario is designed based on the following four assumptions:

1) The SE is part of the SIM;
2) The cloud is part of the MNO;
3) The MNO manages the SE/SIM (SE in the form of UICC);
4) Banks, etc. are part of the MNO;

As one of the challenging issues of deploying NFC transactions in a global scale is yet the collaboration of involved entities, proposing a cloud-based approach can be beneficial in a number of ways. This approach reduces the number of involved entities such as trusted service manager which mainly acts as a trusted third party for service providers, network operators, SIM manufacturers and financial institutions. In the proposed scenario, having assumed that the cloud takes the responsibility of managing the clients credential reduces the complexity of such collaboration which normally result in different parties claiming advanced access rights and ownerships of that critical information. This has also been the main difficulty towards standardisation of NFC payment ecosystem.

The first assumption is practically feasible as most NFC payment providers use this approach. However, the service provider may not necessarily be the network operator. In the proposed scenario, it is stated that since the SE is part of the SIM the MNO manages the SE (first and third assumptions). This can be an effective approach if MNOs are willing to provide such services apart from their network operation responsibilities. The second assumption highlights the ownership of the cloud which is under the control of the MNO. Again, this approach is feasible and is already employed by a number of MNOs such as Verizon and AT &T towards providing additional services but NFC payments that can be further considered.

The critical part of the designed scenario is the fourth assumption where the financial institution is integrated with the MNO. This approach has not been deployed yet; nonetheless it can be an interesting area to be looked at. Moreover, the integration is not clearly discussed in the sense that how the access rights are defined and established so that remains as an interesting area for future research.

Designed scenario as a whole introduces a novel and interesting insight towards NFC payments particularly where the proven cloud, GSM and NFC technologies are in action.

4.7.2 Protocol Evaluation

In order to evaluate the proposed protocol, the security of the cryptographic primitives must be reviewed according to their cryptographic definitions.

A) Strength and Weaknesses

The logic of the proposed protocol is based on the initially designed scenario where multiple parties are involved in the protocol execution. The properties used to design the protocol are based on the operation of GSM, NFC and cloud technologies.

Proposing an additional step for mutual authentication of the SIM and the MNO (steps 1 to 12) over the GSM network provides further security as non-repudiation is ensured. In particular, this provides proof of the integrity and origin of data so that neither the SIM nor the MNO can deny sending and receiving messages and those messages cannot be accessed and modified by a malicious third party. Furthermore, security of the protocol is improved against Man-In-The-Middle and phishing attacks. Despite the advantages of adding the extra step for mutual authentication purposes, this approach can increase the execution time of the messages when it comes to measuring the performance features.

Generation of K_c and K_{c1}as a shared key between the MNO and the SIM in step 13 makes the communication secure whilst it crosses over the merchant which is not permitted to access the message content. However, step 14 suggests generating of a new key K_{c2} which is shared between all entities as all parties have to have a form of secure communication amongst them that still must be inaccessible by a third party. As an additional security step, adding PIN verification (step 17) is not necessary as now days most contactless credit cards do not require a PIN which again improves the performance and is indeed a huge security concern for users.

The use of timestamp (TS_U) in step 21 keeps track of the creation and modification of the exchanged message which means that no entity, not even the sender of the message can

modify it once it has been generated provided that the integrity of the timestamp is never compromised. Moreover, the transaction counter which is included in TRM improves the security in a way that it is incremented after each transaction in order to prevent replay attacks so the message cannot be fraudulently repeated and/or delayed in transmission.

B) Implementation

With respect to implementation issues, firstly the integration of the MNO and the financial institution should be clarified in order to define suitable ownership and access right properties. Moreover, since the protocol uses the GSM network the performance of its execution is highly dependable on the strength of the GSM signals as this may cause delays while transaction details are exchanged. From the merchants' viewpoints, POS terminals must be upgraded to support NFC technology which requires significant investment.

4.8 Summary

In this chapter, we discussed an alternative method of using cloud computing in NFC transactions which provides security, flexibility and improves the manageability of applications in terms of personalization and ownership for both users and customers. Accordingly, we proposed the NFC Cloud Wallet model and described the interactions among the involved parties which are carried out in this model. Using this model, and inspired by Chen et al's (2010) protocol we then proposed a novel protocol for NFC transactions. The key fact of the proposed protocol's scenario was the direct communication between the MNO and the merchant in which a shared secret was available to both parties (the first scenario of our ecosystem). In the next chapter, we target the second scenario and assume that there is no direct communication between the MNO and the merchant. Consequently, there won't be a shared secret among them and therefore we will propose a new scenario as an extension to the NFC Cloud Wallet model, Chen et al (2010) protocol, and our first proposed protocol described in this chapter.

Chapter 5 - Second NFC Transaction Authentication Protocol: Merchant's Authentication with Single MNO

5. Overview

This chapter provides an alternative approach based on the NFC Cloud Wallet model which was introduced earlier in chapter 4. Additionally, a novel secure NFC transaction protocol is designed and its execution process is described in detail. Our first protocol was designed based on the direct communication channel that was established between the MNO and merchant through a shared secret; however the protocol which is proposed in this chapter does not support this scenario since it is based on an alternative approach in which the MNO and merchant have no direct communication channel and therefore all communications goes through the NFC phone. Furthermore, a security analysis of the proposed protocol is carried out in order to justify the reliability and validity of our protocol in the security domain.

5.1 Unlinked POS and MNO (Vendor trusts MNO)

In this scenario, we designed our ecosystem model based on the following assumptions:

- The main SE (virtual SE) is part of cloud that is being managed by the MNO;
- Another SE or any other form of a secure and tamper resistant component is in the mobile device used for authentication to merchant's POS. As described in section 2.5.4, SIM as SE is the best approach in this scenario.
- The MNO manages the SE/SIM;
- Banks, etc. have secure connections with the MNO;
- *Vendor trusts the MNO;*

Figure 18 demonstrates the ecosystem scenario in which the POS and MNO communicate through an NFC phone.

Figure 18: POS and MNO Communicating through NFC Phone

The virtual SE can securely store personal data such as debit and credit card information, user identification number, loyalty program data, payment applications, PINs and networking contacts, among other information. However, the SE which is stored in the NFC phone consists of authentication data such as keys, certificates, protocols and cryptographic mechanisms. The SE is in the form of UICC (the SE part of the SIM), therefore the SIM only deals with the authentication of the handset to the MNO and the handset to vendor terminal; moreover, the main transaction data are stored in the virtual SE. During the whole process, the MNO manages the cloud environment and is the only party that has full access and permission to manage confidential data which is stored in the cloud. Since the MNO is the owner of the cloud, it fully manages the SIM in terms of monitoring the GSM network and controlling the cloud's data. The key assumption of this scenario which makes it different from the first scenario discussed in chapter 4 is the trusted relationship between the merchant and the MNO. This improves the complexity of the payment ecosystem since it reduces the interactions between involved parties.

5.2 Proposed Model

We proposed an extension to the previously proposed NFC Cloud Wallet model. Since there are multiple options applicable to this model, we designed our model based on the same assumptions described in section 5.1. The detailed analysis of this assumption is described in section 5.5. Below is the step by step description of the process as illustrated in Figure 19.

Figure 19: The MNO Communicates with the Vendor through the NFC Phone

Step 1) The customer selects a product - purchase request sent to the merchant's terminal
Step 2) The merchant's POS terminal displays the price.
Step 3) If the customer agrees with the price, s/he places his/her NFC phone on the vending machine.
Step 4) The NFC link is established between the merchant POS terminal and the NFC-enabled phone.
Step 5) The customer requests a message from the MNO to use it in order to prove its legitimacy to the merchant. The customer also informs the MNO about the total price.
Step 6) The MNO first authenticates the customer. After a successful authentication, if the MNO agrees with the price, it sends a digitally signed confirmation message to the NFC-enabled phone (the customer).
Step 7) The mobile device then relays the same message to the merchant's POS terminal. Since vendor terminal trusts MNO, it trusts the digitally signed message.
Step 8) The NFC enabled phone displays enter PIN to verify its legitimacy and its ownership of the cell-phone (additional security mechanism).
Step 9) The merchant's terminal sends its banking details in an encrypted form to the NFC enabled phone. This message can only be decrypted by the MNO.
Step 10) The NFC enabled phone transfers the same banking details to the MNO.
Step 11) The MNO performs the transaction.
Step 12) The MNO sends a signed receipt to the merchant's terminal through the NFC enabled phone.
Step 13) The merchant's terminal verifies the receipt.
Step 14) If the verification is successful, the product is delivered and a success message displays on the NFC-enabled phone.

The trusted relationship between the vendor and the MNO comes into play when the MNO sends a confirmation message to the vendor through the NFC enabled phone (steps 6 and 7). This digitally signed message confirms that the customer has enough credit for the transaction.

5.2.1 Scenario Analysis

In this section, we carry out an analysis from a security point of view. Since this protocol is used for monetary transactions, it must be as secure as much as possible. We sketch multiple scenarios where a buyer or a seller is dishonest and then analyse their success probability.

In the first scenario, we assume that a customer is dishonest and wants to purchase a product without payment. The dishonest customer can only be successful if he can successfully generate a signed receipt in step 12 of the protocol. Since this receipt is signed by the MNO, an illegitimate customer cannot generate a valid receipt. Moreover, the dishonest customer cannot replay the old receipt as the receipt contains time information. Therefore, this scenario is not successful.

In another scenario, we assume that the customer is dishonest and just wants to extract the banking details of a vendor. The vendor provides his banking details after it receives a signed confirmation from the MNO. The banking details are encrypted so the customer cannot decrypt and understand this message. This message can only be decrypted by the MNO who needs the banking details for the transaction. So a dishonest customer is again unsuccessful.

In the third scenario, the seller is dishonest and plans to extract more than the required amount from a customer. To perform this action, the seller alters the price information at transaction stage. However, the alteration is deducted in the signed receipt provided by the MNO after transaction. This receipt is provided to both, the customer and the seller. The customer detects any alteration in the price by the seller. So this scenario is also not successful.

In the fourth scenario, the seller is dishonest and records all the legitimate messages of a customer. He plans to replay the recorded messages to the MNO in order to extract money from a customer in his absence. To do this, the dishonest seller intends to pose as a customer to the MNO. This impersonation is detected by the MNO in the initial steps of the model where the MNO authenticates a customer before proceeding to transaction. This scenario is, again, not successful.

5.3 Our Approach

The general overview of the cloud-based NFC payments was described in chapter 4 where the NFC Cloud Wallet model was also proposed. We then proposed an extension to previously proposed NFC Cloud Wallet model and designed an NFC payment protocol which was based on a GSM network.

This protocol was the improved version of Chen's protocol (Chen et al., 2010) in which user interaction with the system was improved making it more user friendly. An additional layer of security was added by introducing PIN authentication by the user. Mutual authentication was improved by adding freshness by the mobile device in order to resist replay attack. We also added digital signatures with the transaction messages for data integrity and non-repudiation. Since there were multiple options applicable to this model, we designed our protocol based on the following assumptions:

- The SE is part of the SIM;
- The cloud is part of the MNO;
- The MNO manages the SE/SIM
- Banks, etc. are linked to the MNO;

The key aspect in this payment model was the connection between the merchant and the MNO, which makes it different from the protocol that we designed in chapter 4. The proposed protocol is designed based on the following assumptions:

- The SE is part of SIM;
- Cloud is part of the MNO;
- The MNO manages the SE/SIM;
- *The financial institution(s) are linked with the MNO;*
- *The merchant has no connection with the MNO;*
- *The communication is carried over a single channel: MNO, mobile device and merchant;*

5.4 The Proposed Protocol

This section describes our proposed protocol for micropayments based on NFC and cloud architecture. The proposed protocol is based on a cloud architecture where the cloud is being managed by the MNO. The SE used in this protocol is divided into two sections: One, being a part of SIM, is used for authentication of a customer, whereas the other section, being a part of cloud, is used to store sensitive banking information of the customer. The customer has registered his credit/debit card details with the respective MNO. Since our protocol supports multiple accounts against a single customer, a customer can register more than one credit/debit card with the MNO. Each customer account is identified by a unique account ID, Acc_{ID}. The Acc_{ID} is intimated to a customer when he registers his debit/credit card with the MNO. The MNO stores these details in a cloud. The mobile device has a valid SIM and is connected to the respective MNO through the GSM network. The communication over the GSM network is encrypted as specified in the GSM standard. The mobile device is connected to the merchant's terminal over an NFC link. The NFC link is not secure and can be eavesdropped.

The shop has no link with the MNO however the shop trusts the MNO. A message digitally signed by the MNO is considered authentic and its contents are trusted by the shop. When dealing with the signed data, one has to distinguish between data authenticity and trust in the message contents. An authentic data may not be true. For example, a valid signature with the message 'Sun revolves around the earth' will prove the message as authentic but its contents are not true. We assume that the messages signed by the MNO are not only authentic but the contents are also considered trustworthy by the shop. For simplicity, we refer to a mobile device and SIM as a single unit 'mobile device'. K_{sign} and K_{ver} are the signing and verification keys respectively of MNO. K_{pr} and K_{pub} are the private and public keys respectively of the MNO. The protocol executes in three different phases, which shall now be described.

5.4.1 Phase 1: Authentication

This phase initiates once the customer agrees with the total price displayed on the shop terminal and places his cell phone on the shop NFC enabled point. An NFC link is established between the mobile device and the shop terminal.

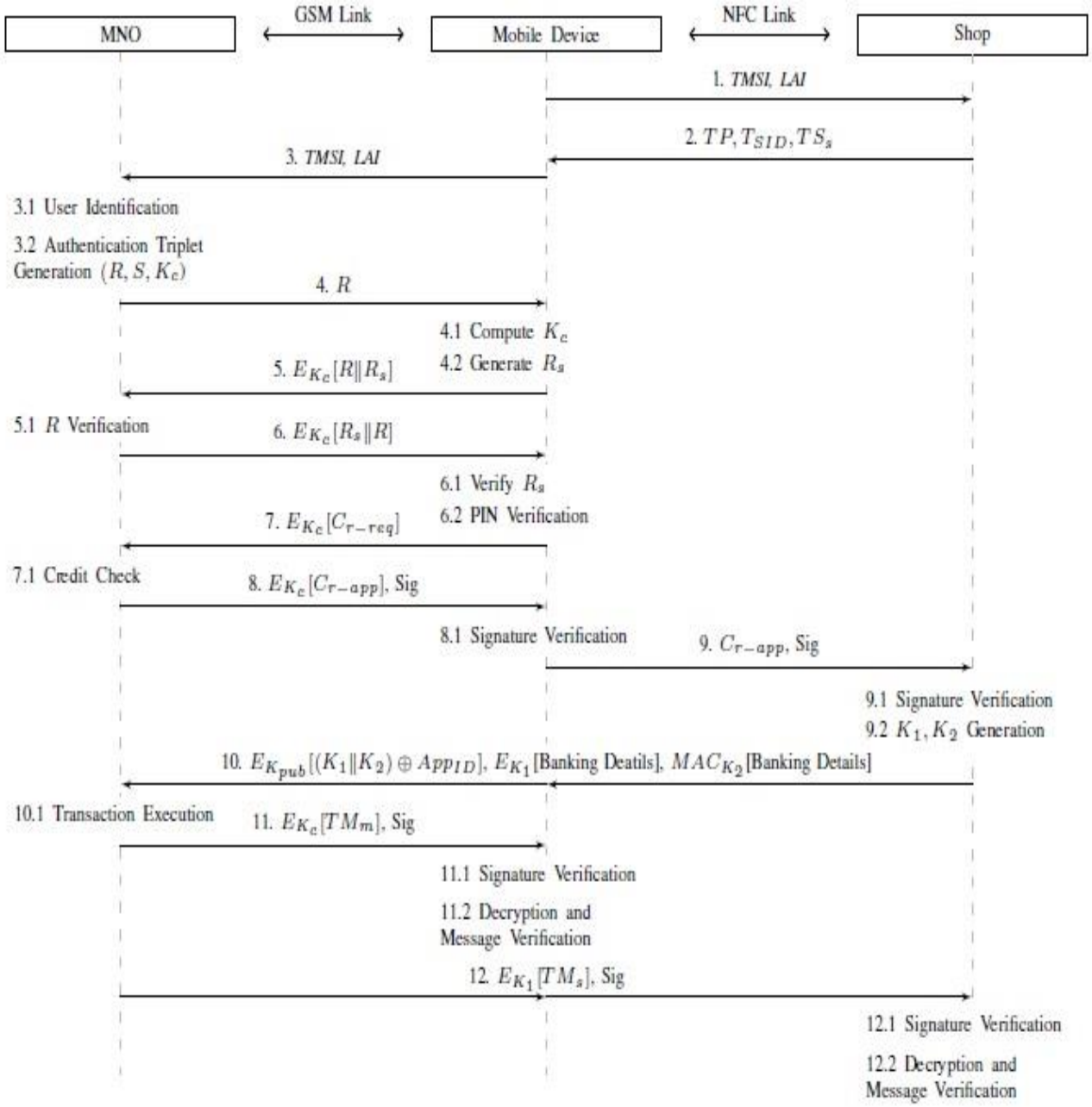

Figure 20: The Proposed Payment Protocol

Step 1: The mobile device sends *TMSI*, *LAI* as its ID to the shop terminal. The shop terminal determines the user's mobile network from this information. The network code is available in *LAI* in the form of the Mobile Country Code (*MCC*) and the Mobile Network Code (*MNC*). An *MNC* is used in combination with the *MCC* (also known as a '*MCC/MNC tuple*') to

uniquely identify a mobile phone operator/carrier (Technical Specification Group Core Network, 1999).

Step 2: The shop terminal sends a message to the mobile device containing the Total Price (*TP*), a temporary shop ID (T_{SID}), and Time Stamp (TS_s) of current time. The T_{SID} acts as one time ID of the shop and gets updated after each transaction.

Step 3: The mobile device initiates a mutual authentication protocol with the MNO. It sends TMSI, LAI as its identifier. The MNO identifies its customer and generates an authentication triplet (R, S, K_c).

Steps 4-5: The MNO sends *R*, a part of the authentication triplet, to the mobile device. The mobile device computes K_c from *R* as explained in section 4.4. The mobile device generates a random number R_s and concatenates with *R*, encrypts with key K_c and sends it to the MNO. The MNO decrypts the message using K_c, the key it already has in the authentication triplet. The MNO compares *R* in the authentication triplet with the *R* in the response. If both *Rs* are same, then the mobile is authenticated for a valid SIM.

Step 6: After successful SIM (or mobile device) authentication, the MNO swaps *R* and R_s, encrypts with K_c and sends it to the mobile device. This step authenticates the MNO to the mobile device. The mobile device receives the response E_{Kc} $(R_s||R)$ and decrypts it with the key K_c already computed in Step 4. The mobile device compares both *R* and R_s. If both are same, then the MNO is authenticated. After successful authentication, the user is asked by the mobile device to enter the PIN. The PIN is stored in the SIM at a secure location. The SIM compares both PINs and if both are same, the user is authenticated as the legitimate user of the mobile device.

5.4.2 Phase 2: Financial Approval

Step 7: After successful authentication, the customer selects the account Acc_{ID} for payment. The mobile device forms a credit request message $C_{r\text{-}req}$ for credit approval from the MNO as:

$$C_{r\text{-}req} = TP||T_{SID}||TS_s||TMSI||Acc_{ID}$$

The mobile device encrypts $C_{r\text{-}req}$ with the key K_c (the encryption key used in GSM communication) and sends it to the MNO. The MNO receives the message, decrypts and communicates with the cloud for a credit check against the account ID Acc_{ID} of the customer.

Step 8: Once the credit is approved from the financial entities through cloud, an approval ID (App_{ID}) is generated by the approving authority. App_{ID} acts as in index to a table storing information about the amount to be credited, destination Shop ID, the time stamp and the customer ID (TMSI). This helps in resolving any disputes in future. The MNO forms a new string $C_{r\text{-}app}$ indicating credit approval as:

$$C_{r\text{-}app} = TP||T_{SID}||TS_s||TMSI||App_{ID}$$

The MNO encrypts the string $C_{r\text{-}app}$ with the key K_c and computes the signature with the signing key K_{sign} over the plaintext. The encrypted $C_{r\text{-}app}$ along with its signature is transmitted to the mobile device.

The mobile device decrypts the message to get $C_{r\text{-}app}$. It compares the contents of $C_{r\text{-}app}$ with the contents of $C_{r\text{-}req}$, as the only difference between both messages is that the Acc_{ID} in the former is replaced by the App_{ID} in the latter. It provides an assurance the $C_{r\text{-}app}$ is generated by a legitimate authority. The mobile device, then, verifies the signature as the signature was computed over the plaintext. The signature provides data integrity, data origin authentication and non-repudiation of the $C_{r\text{-}app}$ message. After successful verification, the mobile device forwards $C_{r\text{-}app}$ to the shop along with the corresponding signature.

Step 9: The shop terminal verifies the signature by the verification key K_{ver} to detect any alteration. In case of an invalid signature, the shop discards the message. A valid signature provides data integrity and data origin authentication. In this case, the shop believes that the message is authentic and that the MNO has agreed to pay for the customer. This is like a three party contract where a middle party, trusted by both other parties, provides an assurance that the other party is willing to pay the price.

5.4.3 Phase 3: Transaction Execution

Step 10: After successful authentication and message contents verification, the shop generates two keys K_1 and K_2 for data encryption and MAC calculation respectively. It forms a string $(K1||K2) \oplus App_{ID}$ and encrypts it with the public key, K_{pub}, of the MNO. The shop encrypts its banking details with the key K_1 and computes its MAC with the key K_2. The banking details may include bank account title, account number, bank code, branch code etc. The MNO needs banking details in order to transfer the necessary amount from the customer account to the shop account. This detail is transmitted to the MNO through the mobile device but the latter cannot decrypt this information. This forms a virtual tunnel between the shop and the MNO through the mobile device.

Once the MNO receives this message, it decrypts the first part to extract the K_1 and K_2. The role of App_{ID} in this step is to bridge the authentication phase to the transaction execution phase. The MNO checks the validity of the MAC and, if successful, it decrypts the banking details. It forwards the banking details to the cloud for the monetary transaction.

Steps 11-12: After a successful transaction, the MNO generates a transaction number TSN and corresponding time stamp TS_t and forms a Transaction Message for mobile device TM_m and Transaction Message for shop TM_s as:

$$TM_m = TSN||TP||T_{SID}||TMSI||TS_t$$
$$TM_s = TM_m \,||\, [Banking\ Details]$$

The MNO encrypts TM_m with the key K_c and computes the signature over the ciphertext. It sends an encrypted TM_m and the corresponding signature to the mobile device. The mobile device first verifies the signature. In case of an invalid signature, the mobile device discards the message without decrypting it. Otherwise, it decrypts the message and verifies the contents.

The MNO forms the Transaction Message for the shop TM_s by appending shop Banking Details to the earlier formed TM_m. It encrypts TM_s with the key K_1 and computes the signature over the ciphertext. The MNO sends the encrypted message along with its signature to the mobile device to further relay it to the shop. The mobile device can neither decrypt this

message as it does not possess K_1, nor alter any contents as they are protected by the signature. The shop verifies the signature and if invalid, discards the message without decrypting the message. Otherwise, the shop decrypts the message and verifies its contents. The contents consist of important transaction information exchanged during the transaction. If the shop wants any clarification, it can approach the MNO quoting the Transaction Number *TSN* and Approval ID App_{ID} received in step 9.

5.5 Protocol Analysis

In this section, we analyse this protocol from multiple perspectives. This analysis encompasses the authentication and security of the messages. We assume that the MNO is trustworthy, whereas the customer or the shop can be dishonest. We analyse multiple attack scenarios to ascertain the strength of our protocol.

5.5.1 Dishonest Customer

Scenario 1: A dishonest customer plans to buy some products with payment from someone else's account. So, s/he sends a fake but valid ID (for example *TMSI, LAI* of a mobile of a target customer) in step 1 to the shop. The shop replies with step 2 providing information about the total price, its temporary ID and the time stamp. In step 3, the dishonest customer has two options in the authentication phase. Either he communicates with his legitimate MNO for authentication or with the target customer's MNO. In the former case, the amount will be deducted from his account (which is what he is not willing to do) whereas, the amount will be deducted from the target customer's account in the latter case. If he goes for the latter option, however, he fails the authentication process in step 5 as he lacks the legitimate K_c. Thus, someone else's ID cannot be successfully used in this protocol.

Scenario 2: A dishonest customer plans to buy goods without any payment. So, s/he provides his/her own banking details, rather than the shop banking details, to the MNO in step 10. In case of a successful transaction, the MNO deducts the amount from the customer account and pays back the amount to the customer (both accounts may be different to avoid detection). The transaction receipt is then transmitted to the shop as a proof of payment. To accomplish this attack, the dishonest customer blocks step 10, in which the shop banking details are transmitted to the MNO through the mobile device. The customer cannot alter this message

as it is encrypted with keys K_1 and K_2. Both these keys are encrypted with the public key K_{pub} of the MNO, so no other entity other than the MNO can get these keys. Therefore, rather than altering this information, the dishonest customer discards this message and designs his own message as:

$$Ek_{pub}\,[(K'_1 \,||\, K'_2) \oplus App_{ID}],\; E_{K'1}\,[Banking\ Details],$$
$$MAC_{K'2}\,[Banking\ Details]$$

Where the banking details are the customer's banking details rather than the shop's, the MNO has to rely on the information provided by the mobile device as the former does not share any secret with the shop prior to the execution of the protocol.

The MNO performs transaction against the information provided by the mobile device. After the transaction execution, the MNO sends 'receipts' in messages 11 and 12. The mobile device blocks message 12 as this message contains the information of the bank that was used during the transaction.

Since the customer's banking details were used during transaction, the dishonest customer needs to replace the banking details in this massage with the shop's banking details. The customer can decrypt the message in step 12 as it is now encrypted with the customer's malicious key K'_1. S/he needs to change the banking details and encrypt with the shop generated key K_1 in step 10. Since the customer lacks this key, he cannot generate a valid ciphertext. Moreover, the original message is protected by the digital signature. If the customer makes any alteration to change the banking details, it will void the signature. If the customer does not alter the message to maintain the validity of the signature, the shop can verify the signature but cannot decrypt the message (as it is encrypted with the customer's malicious key K'_1). In both cases, the shop cannot verify the transaction and a failure message is sent at the end. Hence, a dishonest customer is again unsuccessful.

There may be another approach to accomplish the above attack where the dishonest customer plans to buy some goods without payment. The dishonest customer does not communicate with the MNO since it is not successful as described above; rather the customer impersonates the MNO to the shop in this scenario. The target of the customer is to send fake but

acceptable receipts to the shop at the end of the protocol by replaying old legitimate messages or fabricating new messages. Since the customer is not communicating with the MNO, his account cannot be debited. In the original protocol, the shop receives three messages from the mobile device, namely messages 1, 9 and 12. Message 1 originates from the mobile device, whereas message 9 and 12 are actually originated by the MNO but are relayed by the mobile device to the shop. A dishonest customer needs to design or replay the latter two messages in such a way that they are acceptable to the shop. Both messages are digitally signed by the MNO. These messages contain a Temporary Shop ID (T_{SID}) and a Time Stamp (TS_s). T_{SID} is a random value generated by the shop every time at the start of the protocol. This value does not only serve as a shop ID during protocol, but also it adds freshness to the protocol messages. TS_s is updated too in every protocol round, but it may be predictable to some extent. A combination of these two values, along with the digital signatures of the MNO, does not allow either replay or alteration of the messages. Hence the dishonest customer is again unsuccessful.

Scenario 3: A dishonest customer plans to pay less than the required amount but intimates to the shop of full payment. To accomplish this attack, the mobile device sends TP´ in Credit Request message, $C_{r\text{-}req}$, in step 7 to MNO, where $TP´ < TP$. The mobile device receives Credit Approve message, $C_{r\text{-}app}$, in step 8 from the MNO confirming that the initially requested amount $TP´$ has been approved for transaction. However, the mobile device needs to intimate the shop in step 9 that the original amount, TP, is approved for transaction. Since the approved price is digitally signed, it cannot be amended by the mobile device. So, the actual price that is approved by the MNO is transmitted to the shop. Hence, this attack fails on the proposed protocol.

5.5.2 Dishonest Shop

Scenario 4: The shop is dishonest and plans to draw more than the required amount without intimation to the customer. The information about the amount to be transferred is intimated to the MNO by the mobile device in Credit Request message, $C_{r\text{-}req}$, in step 8. A mobile device cannot send more than the required price unless the device itself is compromised. Therefore, a shop cannot get more than the required amount in this protocol.

Scenario 5: The shop is dishonest and repudiates the receipt of transaction execution message in step 12. In this way, the shop does not deliver goods despite receiving the required amount. In such a scenario, the mobile device has the signed receipt from the MNO indicating a Transaction Serial Number *TSN* in step 11. The *TSN* is linked to the Approval ID App_{ID} generated in step 8. Since both values are digitally signed by the MNO, the mobile device can approach the MNO regarding any dispute.

5.5.3 Messages Security

Apart from the above-mentioned scenarios, we also analyse our protocols from various other angles. The data over the GSM network is encrypted according to the GSM specification. The key K_c used for the data encryption is fresh in each round of transaction. The data over the NFC link in the Authentication and Approval phase (Step 1, 2 and 9) is sent unencrypted. This data, however does not contain any sensitive information. The Total Price may be considered sensitive information but it is also displayed on the shop terminal for visual information of the customer. The read range of the displayed price is much more than the range of the NFC link. Therefore, we graded the TP as not so sensitive information to be protected over NFC link. However, once the TP is transmitted over GSM network, it is encrypted with the key K_c.

Information that is sent in unencrypted over the NFC link is the Credit Approval ID (App_{ID}) in the ($C_{r\text{-}app}$) message (step 9). The App_{ID} is a random string generated by the credit approval authority. From an attacker's perspective, its only significance is its assurance that the customer has, at least, TP amount in his account. This assurance can also be achieved if a customer successfully pays for some goods. Therefore, App_{ID} is also not sensitive information in this scenario.

Role of Approval ID in Message 10: App_{ID} acts as a bridge between the Financial Approval phase and the Transaction phase. It adds freshness to message 10, so it cannot be replayed in the future. App_{ID} is XORed to avoid an increase in the message length. Any alternation in the first part of the message 10 ($Ek_{pub}\ [(K_1||K_2) \oplus App_{ID}]$), results in invalid keys K'_1 and K'_2. This invalidates the MAC and hence detection.

Non-repudiation of Transaction Messages: Transaction Execution messages (Step 11, 12) are digitally signed by the MNO. In case of any dispute about payment, the MNO has to honour both messages. So both the customer and the shop are completely secured about the transaction.

Disclosure of Relevant Information: Shop banking details represent sensitive information as they contains the bank account number etc. It is encrypted not only on the GSM link but also on the NFC link. This information is transmitted after the credit approval information is received by the shop. The banking detail is transmitted through the mobile device to the MNO, yet the former cannot decrypt this information. Since the mobile device does not need this information, it is not disclosed to the mobile device. Similarly, the account information of the customer is not communicated to the shop in the $C_{r\text{-}app}$ message.

New set of Keys for every transaction: The encryption key over GSM network, K_c, is generated from R. Since R is changed in each round of the transaction protocol, the K_c is also fresh. The encryption keys K_1 and K_2 are generated by the shop in each round. So both these keys are also fresh.

Encryption and MAC Keys: Separate keys are used for encryption and MAC calculation making the protocol more secure. Encrypt-then-MAC is an approach where the ciphertext is generated by encrypting the plaintext and then appending a MAC of the encrypted plaintext. This approach is cryptographically more secure than other approaches (Bellare & Namprempre, 2000). Apart from cryptographic advantage, the MAC can be verified without performing decryption. So, if the MAC is invalid for a message, the message is discarded without decryption. This results in computational efficiency.

5.6 Expert Review Evaluation

This section describes the results of an interview conducted by secure protocol experts according to the proposed protocol.

5.6.1 Scenario Evaluation

The scenario is designed based on the following six assumptions:

1) The SE is part of SIM;
2) Cloud is part of the MNO;
3) The MNO manages the SE/SIM;
4) The financial institution(s) are linked with the MNO;
5) The merchant has no connection with the MNO;
6) The communication is carried over a single channel: MNO, mobile device and merchant;

The first four assumptions are similar to the first proposed scenario in chapter 4. However, unlike the first scenario, the merchant and MNO have no means of communication as all messages are exchanged over a single channel: MNO, SIM (mobile device) and merchant. In order to develop the most effective cloud-based NFC payment ecosystem it is important to design and develop alternative payment scenarios. Furthermore, the method of communication is entirely employable by the involved entities as they should agree on the overall payment architecture (lack of standardisation). Despite the positive aspects of designing alternative scenarios, the security of such scenarios is yet to be considered as the first priority; especially when there is no direct communication between the merchant and MNO so that in principle they are communicating through the SIM. This way, the SIM should not be aware of some of the message contents that are exchanging between the merchant and the MNO; therefore, particular cryptographic properties must be in use to ensure the security of the transaction data is met.

5.6.2 Protocol Evaluation

In order to evaluate the proposed protocol, the security of the cryptographic primitives must be reviewed according to their cryptographic definitions.

A) Strength and Weaknesses

Since the merchant and the MNO do not have a direct communication, the MNO digitally signs the messages that it sends to the merchant. The use of digital signature demonstrates the

authenticity of the messages while it gives the merchant the reason to believe that the message was created by the MNO. Accordingly, the above satisfies the assumption used for designing the protocol.

Alike the first protocol, this protocol uses two-factor authentication (mutual authentication) for improved security between the SIM (client) and the MNO. In step 8, the protocol executes in way that once the client has decided to pay with one of his/her accounts, the MNO must either approve or reject the customer request. In case of an approval, the financial department of MNO (bank, etc.) should generate an approval ID ($APP_{ID)}$ which is not essential. Instead, the, MNO can just use the previously client assigned ID in this step rather than executing a new line of code that also have drawbacks in the performance of the protocol execution. However, from the security viewpoint, the approval ID along with freshness adds an extra layer of security which prevents replay attacks.

In the transaction execution phase (step 10), the merchant uses encrypt-then-MAC technique; the encryption key is K_1 and the MAC key is K_2. This is particularly secure since the attacker must retrieve both keys to access the message content. This is reasonably accepted since confidential information such as clients credentials are exchanged in this phase so that the performance aspects of this line of the protocol are not as critical as its security characteristics.

In steps 11-12, since the SIM (mobile device) lacks the K_1 while the MNO sends the transaction authorisation message to the shop, the SIM cannot decrypt the message to access the encrypted data. This is the way that the MNO ensures the message is only decrypted by the genuine recipient which in this case is the merchant - the same procedure applies to the merchant in general. When the MNO aims to communicate with the SIM, it encrypts the message with K_c (shared key between the MNO and SIM) so that the merchant or a potential malicious third party has no chance of decrypting the message.

B) Implementation

The proposed protocol is designed to support only a single MNO that may introduce some limitations. This potential approach would be beneficial for the stakeholders i.e. banks who

aim to cooperate with one MNO of their own choice since the proposed model does not develop a scenario in a global scale. For example, the MNO would only be able to offer its services in countries in which it operates. It would not be possible to use the mobile payment services offered by a particular MNO in a country that they do not operate. This is because the architecture does not allow the MNO to use the base station of another network carrier. Despite the limitations of this approach, most NFC payment architectures are still based on the operation of a single MNO as there has not been a standardised architecture for all the MNOs and banks to follow. Moreover, the performance measures of such protocol remain as the main concern when it comes to implementing such architecture.

5.7 Summary

In this chapter, we proposed a transaction protocol which provides a secure and trusted communication channel to the communication parties. The proposed protocol was based on the NFC Cloud Wallet model, the first proposed protocol described in chapter 4 and Chen et al.'s (2010) protocol for secure cloud-based NFC transactions. We considered a cloud-based approach for managing sensitive data to ensure the security of NFC transactions over the use of an SE within the cloud environment. In addition, we described the detailed execution of the protocol and determined that our protocol performs reliably from the security point of view in the cloud-based NFC transaction architecture. The main advantage of this protocol is the elimination of a shared secret between the MNO and merchant, which reduces the number of exchanging messages among entities which therefore improves the security of the process. However, in this protocol, the merchant can only authenticate a single MNO. This might be the case for companies who are not looking to expand their collaboration on a larger scale. In the next chapter, we propose an alternative protocol based on the similar scenario used in this chapter, but we aim to improve the limitation that our second protocol provides by designing a transaction authentication protocol which enables the merchant to authenticate multiple MNOs.

Chapter 6 - Third NFC Transaction Authentication Protocol: Merchant's Authentication with Multiple MNOs

6. Overview

Here we extend the proposed mobile transaction mechanisms described earlier in chapters 4 and 5. Accordingly, in this chapter, we propose an extended version of the second proposed protocol that enables the merchant to authenticate multiple MNOs. The major contributions of our work in this chapter are:

- The elimination of the requirement for a shared secret key between the merchant's POS and the MNO, a prerequisite in the first proposed protocol.

- The banking details or the shopping details are not disclosed to the BS. This is because the Base Station (BS) may belong to another MNO and therefore an un-trusted party.

This makes our work more practicable as a shop does not need to have itself registered with the MNO to perform mobile transaction. We partition the SE into two sections: one stored in the SIM for authentication of a customer and the other stored in the cloud to hold credit/debit card details of the customer. This helps in managing multiple cards for a single customer. The authentication of the customer by the MNO is based on a GSM authenticating mechanism with improved security features. Our protocol works on a similar pattern to that of 'PayPal': the MNO, acting in the same way as PayPal, registers multiple banking cards against a user for monetary transactions. The user, then, selects a single card at the time of the payment.

6.1 The Proposed Protocol

This section describes our proposed protocol for micropayments based on NFC and cloud architecture. The proposed protocol is based on a cloud architecture where the cloud elements are managed by the MTD (the MNO Transaction Department). The MTD, under control of the respective MNO, is a dedicated financial department that deals with NFC transactions of the customers. The SE used in this protocol is divided into two sections: one part, residing in the SIM, is used for authentication of a customer, whereas the other part, residing in the cloud, is used to store sensitive banking information of the customer. The customer registers his credit/debit card details with the MTD through respective MNO. Since our protocol supports multiple accounts for a single customer, a customer can register more than one credit/debit card with the MTD. Each account of a customer is identified by a unique account ID, Acc_{ID}. The Acc_{ID} is intimated to a customer when he registers his debit/credit card with the MTD, and this is stored in the SE of his SIM. The MTD stores these details in the cloud. The mobile device has a valid SIM and is connected to the respective MNO through the GSM network. Communication over the GSM network is encrypted as specified in GSM standard. The communication between different entities of the GSM network is considered to be secure. The MNO may be linked to the customer through its own Base Station or *through a Base Station of some other network*. In the latter case, the proposed protocol should not disclose any sensitive information to the Base Station. The mobile device is connected to the shop terminal over an NFC link; however the NFC link is not secure and can be eavesdropped. The shop does not use any link with the MNO for transactions. Nonetheless, the shop needs to trust the MNO so that a message digitally signed by the MNO is considered authentic and its contents are trusted by the shop. For simplicity, we refer to the mobile device and SIM as a single unit called the 'Mobile Device (MD)'. K_{sign}; K_{ver} are the signing and verification keys respectively of the MTD, whereas K_{pr}; K_{pub} are the private decryption and public encryption keys respectively of the MTD.

The protocol executes in three different phases: customer identification and credit check, customer authentication, and transaction execution (Figure 21).

A. Customer Identification and Credit Check

This phase is initiated once the customer agrees to pay the total price displayed on the shop terminal and places his/her cell phone on the shop NFC enabled point. An NFC link is established between the mobile device and the shop terminal.

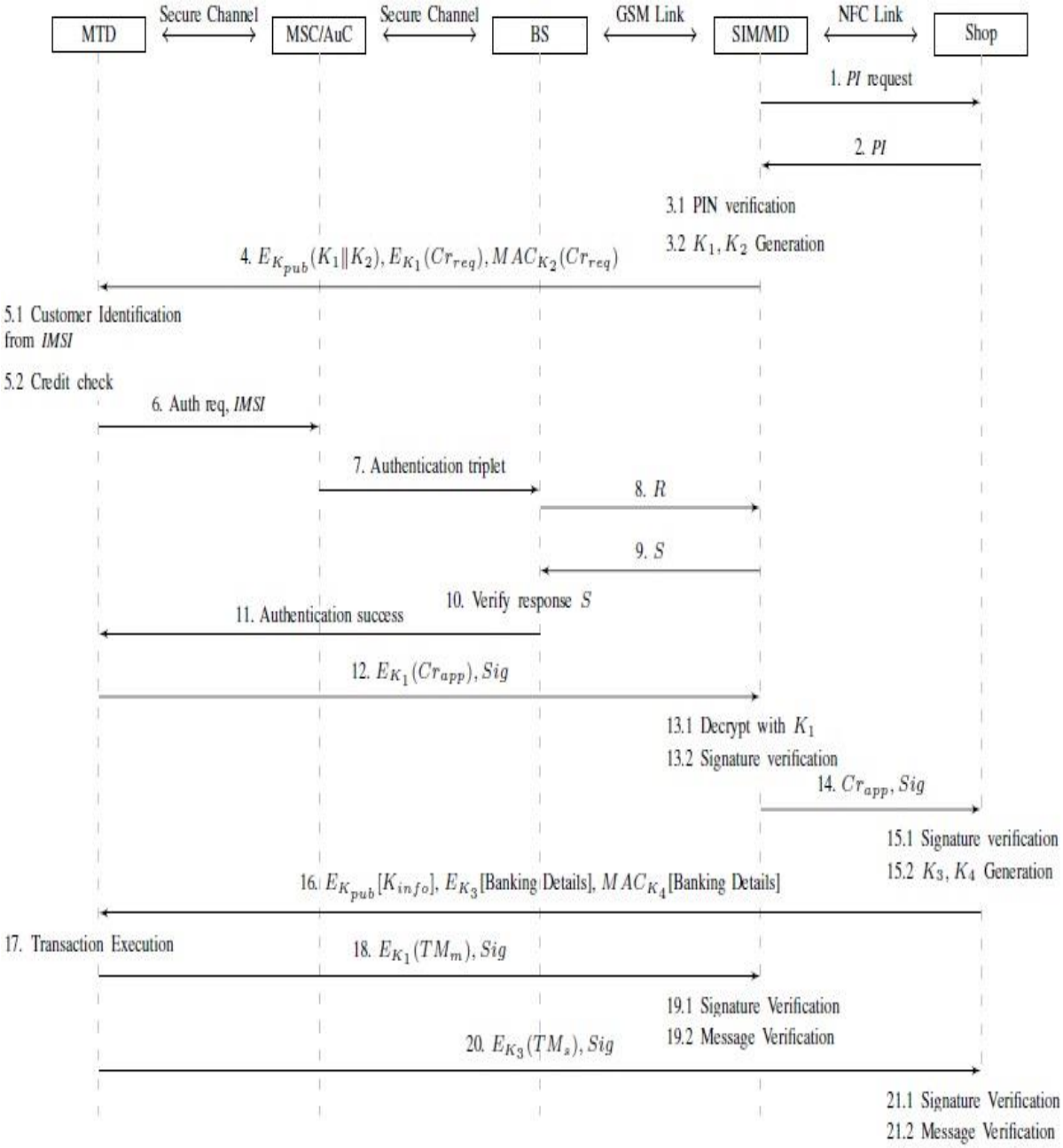

Figure 21: The Proposed Customer Authentication Protocol

Step 1: The mobile device sends payment Information *PI* request message to the shop terminal.

Step 2: The shop terminal forms *PI* message containing Total Price (*TP*), a temporary shop ID (T_{SID}), and a Time Stamp (TS_s) and sends it to the mobile device.

$$PI = TP||T_{SID}||TS_s$$

The T_{SID} acts as one time ID of the shop and gets updated after each transaction.

Steps 3-4: Once the payment information is received from the shop, the application installed on the mobile device asks for PIN authentication from the user. This is for assurance that the customer is the legal owner of the mobile device. After a successful PIN verification, the mobile device needs credit approval from the respective MTD indicating that the customer has sufficient funds in his account to pay the required amount. This information does not need to be disclosed to BS or any other entity of GSM network other than the MTD. As assumed earlier, the communication over the GSM link in encrypted according to GSM standard, but BS decrypts all information. To avoid decryption at BS level, the mobile device generates two keys K_1; K_2 for encryption and MAC respectively. The mobile device forms a credit request message Cr_{req} for credit approval from the MTD, namely,

$$Cr_{req} = PI||IMSI||Acc_{ID}$$

The Cr_{req} message is encrypted with the key K_1 and MAC is computed with the key K_2 to provide data integrity. Both the keys, K_1 and K_2, are digitally signed with the public key of the MTD and the entire message is sent to the MTD.

Step 5: On receipt of this message, the MTD first decrypts it with its private key K_{pr} to extract the encryption and MAC keys, K_1 and K_2. It verifies the MAC and if successful, decrypts the Cr_{req} message. The MTD identifies the customer from IMSI in the Cr_{req} and communicates it to the cloud for a credit check against the account ID of the customer. If the customer has sufficient funds in his mentioned account, the MTD requests a fresh authentication of the customer prior to proceed to any transaction process.

B. Customer Authentication

Steps 6-11: The MTD sends an authentication request message to MSC/AuC. The MSC follows standard procedure to authenticate a customer as described in the GSM standard. In case of successful authentication, an authentication success message is sent to the MTD.

Step 12: Once the customer is authenticated, an approval ID (App_{ID}) is generated by the MTD. App_{ID} acts as in index to a table storing information about the amount to be credited, the destination Shop ID, the time stamp and the customer ID (IMSI). This helps in resolving any disputes in future. The MTD forms a new string Cr_{app} indicating credit approval, namely,

$$Cr_{app} = PI||TS_a||App_{ID}$$

The MTD computes a signature with the signing key K_{sign} over the plaintext and encrypts the string Cr_{app} with the key K_1. The encrypted Cr_{app} along with its signature is transmitted to the mobile device. Cr_{app} cannot be decrypted by the BS as the BS lacks the encryption key K_1.

Steps 13-16: The mobile device decrypts the message with the encryption key K_1 to obtain Cr_{app}. It compares the *PI* contents in both Cr_{req} and Cr_{app} messages. Moreover, the approval time stamp, TS_a, must be in a defined time window.

The mobile device also verifies the signature which was computed over the plaintext. This provides data integrity, data origin authentication and non-repudiation of the Cr_{app} message. After successful verification, the mobile device forwards Cr_{app} to the shop along with the corresponding signature.

The shop verifies the signature sing K_{ver} to detect any alteration and compares the *PI* contents in the Cr_{app} message to the one it initially sent in message 2. In the case of an invalid signature, the shop discards the message and rejects the payment. A successful verification indicates that the customer is legitimate and that the MTD has obtained agreement from the customer to pay. This is like a three party contract where a middle party, trusted by both other parties, provides an assurance that the other party is willing to pay the price. The shop now needs to send its banking details to the MTD for transaction.

The banking details may include bank account title, account number, bank code, branch code etc. The banking details are sensitive information and should not be disclosed to any entity other than the MTD, even the mobile device. The shop generates encryption and MAC keys, K_3 and K_4 to secure banking details. It encrypts the banking details with the key K_3, and computes MAC over the ciphertext with the key K_4. It also forms a string, K_{info}, containing the information about the keys as follows:

$$K_{info} = (K_3||K_4) \oplus App_{ID}$$

The role of App_{ID} in this step is to bridge the authentication phase to the transaction execution phase. The shop encrypts the string K_{info} with the public key of the MTD K_{pub} and sends it to the MTD. This detail is transmitted to the MTD through the mobile device but the latter cannot decrypt this information. This forms a virtual tunnel between the shop and the MTD through the mobile device.

C. Transaction Execution

Step 17: Since the MTD knows the App_{ID}, it can get K_3 and K_4 to decrypt the banking details of the shop. The MTD transfers the requested amount from the customer account to the shop account.

Steps 18-21: After a successful transaction, the MTD generates a Transaction Serial Number *TSN* and corresponding time stamp TS_t and forms a Transaction Message for the mobile device TM_m and a Transaction Message for shop TM_s as follows:

$$TM_m = PI||TSN||TS_t$$
$$TM_s = TM_m||[\text{Banking Details}]$$

The MTD encrypts TM_m with the key K_1 and computes a signature over the ciphertext. It sends the encrypted TM_m and corresponding signature to the mobile device. The mobile device first verifies the signature. In case of an invalid signature, the mobile device discards

the message without decrypting it and exits the transaction. Otherwise, it decrypts the message and verifies the contents.

The MTD forms the Transaction Message TM_s for the shop by appending the Shop Banking Details to the previously formed TM_m. It encrypts TM_s with the key K_3 and computes a signature over the ciphertext. The MTD sends the encrypted message along with its signature to the mobile device which relays it to the shop. The mobile device can neither decrypt this message as it does not possess K_3, nor alter any contents as they are protected by the signature. The shop verifies the signature and if invalid, discards the message without decrypting the message. Otherwise, the shop decrypts the message and verifies its contents. The contents consist of important transaction information exchanged during the transaction. If the shop wants any subsequent clarification, it can approach the MNO quoting the Transaction Number *TSN* and Approval ID App_{ID} received in step 14.

6.2 Protocol Analysis

In this section, we analyse this protocol from multiple perspectives. This analysis encompasses the authentication and security of the messages. We assume that the MNO is trust worthy, whereas the customer or the shop can be dishonest. We analyze multiple attack scenarios to ascertain the strength of our protocol.

6.2.1 Dishonest Customer

Scenario 1: A dishonest customer plans to buy some products with payment from someone else account. Let's assume that the dishonest customer knows the IMSI and Acc_{ID} (*IMSI´*, $Acc´_{ID}$) of the target victim. The dishonest customer fabricates $Cr`_{req}$ message in step 4 as:

$$Cr´_{req} = PI||IMSI´||Acc´_{ID}$$

As this message can be decrypted only by the MTD, the malicious contents remain undetected by all other entities of the GSM network. The MTD decrypts the message identifies the customer from *IMSI´*. Since the target victim is a legitimate customer and has sufficient funds in his account, the MTD proceeds to fresh authentication of *IMSI´*. The MSC/AuC provides the authentication triplet in step 7 corresponding to *IMSI´*. The attacker

cannot compute a valid response S as he lacks the valid key K_i to compute the response. So, the attacker's response S' in step 9 to the random challenge R is different from the S in the authentication triplet. This fails the authentication and the protocol stops. Thus, someone else's ID cannot be successfully used in this protocol.

Scenario 2: A dishonest customer plans to buy goods without any payment. He accomplishes this plan by providing his own banking details, instead of the shop's, as the recipient. He blocks the legitimate message 16. The attacker, then, generates his own set of keys, K'_3 and K'_4, and fabricates message 16 with own banking details and sends it to the MTD. The MTD performs transaction against the information provided by the mobile device by deducting the amount from the customer account and paying it back to the same customer's account (both accounts may be different to avoid detection).

After the transaction execution, the MTD sends 'receipts' in message 18 and 20. The mobile device blocks message 20 as this message contains the information of the customer bank details as it was used during the transaction. The dishonest customer needs to replace the banking detail in this massage with the shop banking details. The customer can decrypt message 20 as it is now encrypted with the customer's malicious key K'_3. He needs to change the banking details and encrypt them with the shop-generated key K_3 in step 15.2. Since the customer lacks this key, he cannot generate a valid ciphertext. Moreover, the original message is protected by the digital signature. If the customer makes any alteration to the banking details, it will void the signature. If the customer does not alter the message in order to keep the validity of the signature, the shop can verify the signature but cannot decrypt the message (as it is encrypted with the customer's malicious key K'_3). In both cases, the shop cannot verify the transaction and a failure message is sent at the end. Hence, a dishonest customer is again unsuccessful.

There may be another approach to accomplish the above attack, where the dishonest customer plans to buy some goods without payment. The dishonest customer does not communicate with the MTD since it is not successful as described above; rather the customer impersonates the MTD to the shop in this scenario. The target of the customer is to send fake but acceptable receipts to the shop at the end of the protocol by replaying old legitimate messages or fabricating new messages. Since the customer is not communicating with the MTD, his

account cannot be debited. In the original protocol, the shop receives three messages from the mobile device, specially, messages 1, 14 and 20. Message 1 originates from the mobile device, whereas messages 14 and 20 actually originate from the MTD but are relayed by the mobile device to the shop. A dishonest customer needs to design or replay the latter two messages in such a way that they are acceptable to the shop. Both messages are digitally signed by the MTD. These messages contain a Temporary Shop ID (T_{SID}) and a Time Stamp of the shop (TS_s). T_{SID} is a random value generated by the shop every time in the start of the protocol. This value does not only serve as a shop ID during protocol, but it also adds freshness to the protocol messages. TS_s is updated too in every protocol round, but it may be predictable to some extent. A combination of these two values, along with the digital signatures of the MTD, does not allow either replay or alteration of the messages. Hence the dishonest customer is again unsuccessful.

Scenario 3: A dishonest customer plans to pay less than the required amount but intimates to shop of full payment. To accomplish this attack, the mobile device sends TP' in the Credit Request message, Cr_{req}, in step 4 to MTD, where $TP' < TP$. The mobile device receives the Credit Approve message, Cr_{app}, in step 12 from the MTD confirming that the initially requested amount TP' has been approved for transaction. But the mobile device needs to intimate the shop in step 14 that the original amount, TP, is approved for transaction. Since the approved price is digitally signed, it cannot be amended by the mobile device. So the actual price that is approved by the MTD is transmitted to the shop. Hence, this attack fails on the proposed protocol.

Scenario 4: A dishonest customer wants to pay through a mobile device which he does not own. S/he might have stolen that device or found it as lost property. If the SIM is still valid, it can be used for a transaction. After the device receives Payment Information (*PI*) from the shop in step 2, the application installed on the mobile device requires PIN verification from the customer. Since the customer does not own the mobile device, s/he does have the knowledge about the PIN. So the protocol does not proceed further. Additionally, the application can be designed to get blocked after a limited number of failed attempts of PIN verification. This provides security to the customers who feel secure that their lost mobile device could not be used for any monetary transaction even if the SIM is active.

6.2.2 Dishonest Shop

Scenario 5: The shop is dishonest and plans to draw more than the required amount without intimation to the customer. The information about the amount to be transferred is intimated to the MNO by the mobile device in the Credit Request message, Cr_{req}, in step 4. A mobile device cannot send more than the required price unless the device itself is compromised. Therefore, a shop cannot get more than the required amount in this protocol.

Scenario 6: The shop is dishonest and repudiates the receipt of transaction execution message in step 20. In this way, the shop does not deliver goods despite receiving the required amount. In such a scenario, the mobile device has the signed receipt from the MTD indicating a Transaction Serial Number *TSN* (received in step 18). The *TSN* is linked to the Approval ID App_{ID} generated in step 12. Since both values are digitally signed by the MTD, the mobile device can approach the MTD regarding any dispute.

6.2.3 Messages Security

Apart from the above-mentioned scenarios, we also analyse our protocols from various other angles. The data over the GSM network is encrypted according to the GSM specification.
The key K_c used for the data encryption over GSM link. The data over NFC link in Authentication and Credit Approval phase (Step 1, 2 and 14) is sent in clear. This data does not contain any sensitive information. Total Price may be considered as sensitive information but it is also displayed on the shop terminal for visual information of the customer. The read range of the displayed price is much more than the range of the NFC link. Therefore, we considered *TP* as not so sensitive information to be protected over NFC link.

Other information that is sent unencrypted over the NFC link is the Credit Approval ID (App_{ID}) in the (Cr_{app}) message (step 14). The App_{ID} is a random string generated by the credit approval authority. From an attacker's perspective, its only significance is its assurance that the customer has, at least, *TP* amount in his account. This assurance can also be achieved if a customer successfully pays for some goods. Therefore, App_{ID} does not represent sensitive information in this scenario.

Role of Approval ID in message 16: App_{ID} acts as a bridge between the Financial Approval phase and the Transaction phase. It adds freshness to message 16, so it cannot be replayed in future. App_{ID} is XORed to avoid an increase in the message length. Any alternation in the first part of the message 16 (K_{info}) results in invalid keys K'_3 and K'_4. This invalidates the MAC and hence detected.

Non-repudiation of Transaction Messages: Transaction Execution messages (Step 18, 20) are digitally signed by the MTD. In case of any dispute about payment, the MTD has to honour both messages. So both the customer and the shop are completely secured about transaction.

Disclosure of Relevant Information: The Cr_{req} message containing price information is not disclosed to the base station or any other GSM entity apart from the MTD.

Shop banking detail is a sensitive information as it contains the bank account number etc. It is encrypted not only over the GSM link but also over the NFC link. This information is transmitted after the credit approval information is received by the shop. The banking detail is transmitted through the mobile device to the MTD, yet the former cannot decrypt this information. Similarly, the account information of the customer is not communicated to the shop in Cr_{app} message.

New set of Keys for every transaction: The encryption and MAC keys for Cr_{req} message, K_1 and K_2, are freshly generated by the mobile device in each round. Similarly, the keys K_3 and K_4, generated by the shop are fresh for each transaction.

Encryption and MAC Keys: refers to the corresponding section (5.5.3) in chapter 5.

6.3 Expert Review Evaluation

This section describes the results of an interview conducted by secure protocol experts with respect to the proposed protocol.

6.3.1 Scenario Evaluation

The scenario is designed based on the following six assumptions:

1) The SE is part of the SIM;
2) Cloud is part of the MNO;
3) The MNO manages the SE/SIM;
4) The financial institution(s) are linked with the MNO;
5) The merchant has no connection with the MNO;
6) The communication is carried over a single channel: MNO, mobile device and merchant;
7) The banking details or the shopping details are not disclosed to the Base Station (BS). This is because the BS may belong to another MNO and therefore an un-trusted party;

The first six assumptions made to design this payment scenario are similar to the second proposed scenario. However, there is a great difference between them that is addressed in the seventh assumption. This scenario is designed to support multiple MNOs during the transaction initiation and execution which can be taken into consideration by the stakeholders in order to deploy such payment scenario in a global scale. For example, a particular MNO may not operate in certain countries; nonetheless, this scenario provides the opportunity for the service provider - which in all proposed scenarios is the MNO - to utilise the BS of the network operators functioning in those countries. This scenario enables clients to use their mobile payment services while travelling worldwide even if their MNO only operates in their home country. Despite the fact that this approach increases the flexibility of the state-of-the-art technology, it requires the roaming cooperation of network carriers in different countries so as it is the case now days. With respect to the other assumptions that has been made to design this scenario, the integration of MNO and the financial institution remains as an interesting area to be explored. Moreover, again all communications between the merchant and the MNO transmits through the SIM (mobile device) that reduces the number of exchanged messages in its respective protocol and makes it more feasible in terms of timing issues.

6.3.2 Protocol Evaluation

In order to evaluate the proposed protocol, the security of the cryptographic primitives must be reviewed according to their cryptographic definitions.

A) Strength and Weaknesses

Unlike the previously proposed protocols, the third protocol is designed based on five entities and the detail interactions of these entities are described in greater depth. The MNO as a single entity consists of three sub-entities named as MTD, MSC and BS which operates on GSM network. The two-factor authentication is executed similarly to the previously proposed protocols that add additional security since the SIM correspondingly validates the MNO. Likewise, the PIN verification stage is also included in this protocol that is not utilised in contactless payments now days; however, it acts as a supplementary step that enhances the security of protocol execution.

Although all communications are transmitted through the SIM, the SIM has not been given the permission to decrypt the all messages. This is because of the generation of different keys that is shared and used amongst the intended parties which ensures the confidentiality of the exchanged messages. For instance, in step 3.2, the SIM generates K_1 and K_2 to encrypt and MAC the message that is intended to send and decrypt by the MTD. In this case, as the BS lacks those keys, it is unable to decrypt the information; this is important particularly when for example a UK based MNO decides to connect to the BS of another network carrier in a different country. The use of T_{SID} (step 2) that is contained in the payment information also improves the security as it gets updated after each transaction which also prevents the intruder from resending the same but this time as a fake message.

The use of digital signatures by the MTD in steps 12 to 15.1 provides integrity, data origin authentication and non-repudiation of the message. Consequently, the message remains accurate and complete while the sender of the message cannot deny sending the message. Likewise, in the transaction execution phase, the MNO signs the message and sends it to the SIM through the BS. Since BS does not have the decryption key, the content of the message remains unknown to the BS. The cryptographic properties used in this protocol meet the

objectives of the developed scenario; however, a proof of concept prototype could be implemented in order to effectively determine the reliability of the proposed protocol.

B) Implementation

One of the greatest aspects of such scenario and its respective protocol that may become an issue during the implementation is the roaming agreement amongst the network carriers that are based in different countries which should also deal with clients' payment information. Having to deal with the bank account information of millions of users from a variety of countries should be explicit within the agreement of the network carriers. Despite these concerns, the proposed protocol clearly addresses these issues from the security viewpoint that can be put in trial by potential stakeholders. Moreover, the concept of the proposed protocol can also be extended to a multi-party protocol which may increase the flexibility and ease the cooperation of different carriers. Furthermore, other possible architectures in this scenario can be designed to conclude with the most reliable architecture for implementation purposes.

6.3 Summary

In this chapter, we proposed our third transaction authentication protocol which provides a secure communication channel to the involved payment parties. The proposed protocol was based on the idea of NFC Cloud Wallet model and is considered as an extension to our proposed first and second protocols. This protocol works well with the merchants who wish to collaborate with wide range of MNOs in a global scale since the payment service provider (MNO in our case) is able to use the BS of other MNO instead of only using its own to reach the merchant. For example, a UK based MNO (i.e. Orange) may not have its own BS in a specific country (i.e. Iran) to provide cloud-based NFC services to its customers. However, since it does collaborate with the national telecom of Iran (Iran-cell), it can use Iran-cell's BS to authenticate the Iranian based merchant in order to provide payment services to its customers. The major advantage of our proposed payment scenarios is to demonstrate a different method of payment for all those people who wish to use fast and easy payment services. This way of making payments eases the process of purchasing for ordinary people as they only have to top up with their MNO without having to follow all the banking procedures.

Chapter 7 - Conclusions and Future Work

7. Overview

As the standardization of NFC technology shows, many different parties are involved in the transaction process. This kind of distributed standardization causes a significant overhead for dividing up tasks and the definition of interfaces. Additionally, the participation of groups with different interests make the process of standardization tough, as it moves back and forward without a common agreement. On the other hand, many different views and opinions are considered during the standardization. Contactless technology for the Internet of Things requires all parties to agree one common definition and implementation. Having different implementations of one technology blocks interoperability, confuses users and raises the market entry barrier for companies. The idea of having a technology in mobile phone allowing everybody to participate in the Internet of Things will only work if tags, devices, readers and application work seamlessly together and if there is an open market for these components. Therefore, we described the aim of this thesis as to explore the problems with existing NFC transaction ecosystem models, design three novel transaction authentication protocols based on our proposed transaction architectures, and to carry out detailed security analysis of the proposed protocols.

This chapter concludes the findings of this research and provides a summary of the contents discussed in each chapter of this thesis. Moreover, the research limitations are identified and discussed in order to provide future research guidelines.

7.1 Thesis Overview and Findings

This thesis was ordered in seven chapters. This section briefly reviews the past first six chapters:

Chapter 1 described the introduction of this thesis that mainly explored the motivations for directing this research. The discussion focused on the current issues concerning the standardization of NFC payments, most of which originate due to stakeholders not disclosing their intention in the beginning. Thus a top - down standardization with a holistic overview is not possible. This emphasised the major challenges in standardization, primarily the synchronization with other consortia as well as different views of NFC-Forum members. The standardization of NFC goes hand-in-hand with the applications and services. Therefore, many different institutions with different core-competences are involved. The major problem is that there is no central institution coordinating the standardization approaches. Consequently, the aim of this research was to explore the problems with existing NFC transaction ecosystem models, design three novel transaction authentication protocols based on our proposed transaction architectures, and to carry out detailed security analysis of the proposed protocols. Subsequently, the objectives of this research were clarified and described as the stages to achieve the aim of this thesis.

Chapter 2 delivered an overview of e-payment with its associated processes. A number of approaches concerning managing the mobile wallet technology and NFC transaction services were examined and security and manageability were identified as the main challenges that have delayed the adoption of NFC payment services. A comprehensive overview of the literature revealed that the level of security and manageability differ based on the model that stakeholders select in order to provide their payment services, which provides an opportunity to conduct the research presented in this thesis.

Chapter 3 highlighted the approach used while conducting this research. Thereafter, Design Science Research (DSR) was theoretically described and justified as an appropriate methodology for this research. Subsequently, the conducted research in this thesis was described in accordance to the DSR research cycles. Four iterations were identified and presented to accomplish the development of the selection model: (1) *Library Research*, (2) *Initial Design Requirements (Ecosystem/Model design),* (3) *Protocol Design,* (4) *Security Analysis and Validation*.

Chapter 4 proposed a transaction protocol that provides a secure and trusted communication channel to the communication parties. The proposed protocol was based on the NFC Cloud

Wallet model where there is a direct link between the merchant's POS and the MNO (via a shared secret) for secure cloud-based NFC transactions. The operations performed by the vendor's reader, an NFC enabled phone and the cloud provider are provided and such operations are maybe possible by the current state of the technology, as most of these measures are already implemented to support other mechanisms. We considered the detailed execution of the protocol and showed our protocol performs securely in the cloud-based NFC transaction architecture. The main advantage of this chapter was to demonstrate another way of payment for all those people who do not have bank accounts. This way of making payments eases the process of purchasing for users as they only have to top up with their MNO without having to follow all the banking procedures.

Chapter 5 discussed the NFC ecosystem scenario where cloud computing plays a major role in the payment architecture and the MNO and merchant's POS are have no direct communication. Therefore, the merchant's POS and the MNO communicate through the NFC phone (the merchant trusts MNO). We introduced a different insight which proposed a new integrated framework based on trusted integrations of cloud-based NFC transaction players, namely the MNO, the NFC phone user and the merchant. We considered a cloud-based approach for managing sensitive data to ensure the security of NFC transactions over the use of a SE within the cloud environment in addition to considering the role of SE within the NFC phone architecture. We then proposed a secure transaction protocol based on the above scenario and developed a detailed security analysis of the protocol in order to validate its security and reliability. The proposed protocol was based on the NFC Cloud Wallet model, the first proposed protocol (chapter 4), and Chen's protocol (Chen et al., 2010) for secure cloud-based NFC transactions. We considered a cloud-based approach for managing sensitive data to ensure the security of NFC transactions over the use of a SE within the cloud environment as well as considering the role of the SE within the NFC phone architecture.

Chapter 6 provided an alternative protocol similar to the scenario used to design the protocol which is proposed in chapter five. The main difference of this protocol with the previous one is that this protocol enables the merchant to authenticate with multiple MNOs. This capability is provided through the introduction of a new entity called a BS that is considered as an un-trusted party during the execution of our proposed protocol. The structure, execution and generally design of this protocol are modified since the MNO and merchant must

communicate through a BS. Furthermore, a detailed security analysis of this protocol is provided to examine the strength of our protocol against different attacks.

7.2 Research Contributions

The aim and objectives described in chapter 1 of this thesis provide the research contributions in chapters 4,5 and 6 respectively. In this section, we discuss a summary of the research contributions that each of the mentioned chapters present.

7.2.1 NFC Cloud Wallet Model

This model provides an overview of our alternative approaches for managing payment applications by using the cloud environment and NFC technology. Stakeholders can extend their existing models using the idea of NFC Cloud Wallet when deciding on their final NFC transaction approaches for service delivery. This model introduces a flexible approach to effectively control the security and management of payment applications in the area of mobile payments through describing the interactions between involved parties.

Several studies tried to tackle the problem of managing the SE (Van Damme et al, 2009; Francis et al., 2010a; Alpar et al, 2012; Madlmayr et al., 2008; Aldershof, P., 2012), however they all proposed their own solutions without using existing standards and their specifications which was not necessarily accepted by other ecosystem players. Hence, we did not consider the standard specifications, as our focus was to evaluate the major proposed models in order to develop ours. This approach helps the developer to use the current standards without having to consider the complexities of them in order to directly propose new ecosystem models to improve the security and manageability of the mobile payment services.

Furthermore, our proposed scenarios are more realistic than those developed in previous research as we used real time scenarios which eases the collaboration between ecosystem players by combining the cloud technology in order to provide a more flexible and manageable SE environment.

7.2.2 First NFC Transaction Authentication Protocol: Direct Communication between the MNO and Merchant

The second contribution has provided a novel NFC transaction protocol based both on the NFC Cloud Wallet model as well as the first proposed ecosystem scenario in which the merchant and MNO have direct communications through a secure channel. The approach we followed to develop this ecosystem scenario is to focus on the MNO as a cloud provider during the protocol execution process. This is different from other related work that studied NFC ecosystem scenarios (Aldershof, P., 2012; Benyo et al., 2009; Benyo et al., 2007; Kerem et al., 2013; Madlmayr et al., 2008; Madlmayr et al., 2009; Ozdenizci et al., 2010; Reveilhac et al., 2009; Ulvedal, J. E., 2013), and therefore focused on the role of cloud as the central component for managing the payment credentials. The proposed protocol provides mobile payment stakeholders with a detailed service execution process in three phases. Phase 1: authentication; phase 2: keys generation and PIN verification; and phase 3: transaction. The security analysis of our proposed protocol was then provided from multiple security aspects. This analysis encompassed the authentication and security of the messages among customer, merchant's POS terminal and the MNO. The analysis also included multiple attack scenarios, such as a customer being dishonest and having the intention to pay less, or the shopkeeper being dishonest and planning to receive more money. This analysis demonstrates the protocol's validity and effectiveness to match the security requirements for the proposed mobile transaction scenario. This is mainly valuable in new or rare circumstances, where no or very little documentations of best practice are presented. As discussed previously in chapter 2 of this thesis, there are cases where several models are implemented and not all of them could entirely satisfy all expectations of every involved party in the payment ecosystem. Hence the NFC Cloud Wallet scenario with the proposed protocols can help to determine the best option.

7.2.3 Second NFC Transaction Authentication Protocol: Merchant's Authentication with Single MNO

In this thesis, we also provided another novel NFC transaction protocol based on the NFC Cloud Wallet model which meets the requirements of second proposed scenario in which there is no communication link between the merchant and the cloud provider (MNO) and their communication passes through the NFC enabled phone. The focus of this approach is

on the trusted relationship between the vendor and the MNO which enables the communication to be carried over a single channel: the MNO, mobile device and the merchant's POS. The key issue in the first ecosystem scenario and its designed protocol is the connection between the merchant's POS and the MNO which differs from the concept of the second proposed protocol. This makes the protocol execution process different from the first protocol. The proposed protocol provides a detailed service execution process in three phases. Phase 1: authentication; phase 2: Financial Approval; and phase 3: transaction execution. We then analysed this protocol from multiple security perspectives. This analysis encompasses the authentication and security of the messages. We assume that the MNO is trustworthy, whereas the customer or the merchant can be dishonest. We analysed multiple attack scenarios to ascertain the strength of our protocol and found that the protocol is robust against such attacks.

7.2.4 Third NFC Transaction Authentication Protocol: Merchant's Authentication with Multiple MNOs

We proposed an extension to the earlier proposed transaction protocol mentioned in chapter 5. The major contribution of this chapter is the elimination of the requirement for a shared secret between the merchant's POS and the MNO (same as the second protocol), a prerequisite in the initially proposed protocol in chapter 4. This has also made the third protocol more practicable as the merchant does not need to have itself registered with the MNO to perform mobile transaction. Moreover, we considered the real-life collaboration of network operators while designing the protocol. This has resulted in bringing the concept of BS into the design process of the protocol in which the BS may be of another MNO. We had to change the initial design because of this assumption. Initially, we used key K_c between the mobile device and the MNO in the second protocol, but now we cannot use this key. The reason is that we want to hide information from BS as well to increase the security since BS is considered as an un-trusted entity which might be part of a different MNO. Furthermore, this protocol performs on the GSM network for both customer and MNO authentication mechanisms. The key advantage of this protocol is that it makes the merchant capable of authenticating with the BS of a different MNO that cooperates with the main MNO that is the service provider of the payment process. This method increases the flexibility among the payment ecosystem participants and improves the payment application management from the

service provider's perspective as now it can use the BS of another MNO anywhere in the world. Table 10 shows how this research successfully accomplished the objectives established in section 1.3.

Table 10: Accomplishments of the Research Objectives

Research Objective	Accomplishments
Objective 1: To consider the existing NFC transaction models in order to understand the limitations which have been raised regarding the adoption of this technology.	The first objective was achieved in Chapter 2: Several studies were conducted based on the available literature to understand the limitations of existing NFC ecosystem models.
Objective 2: To develop a payment model based on the results and limitations obtained from consideration of the existing models and to propose an ecosystem architecture and its respective authentication protocol so as to indicate the framework's utility and value.	This objective was met in Chapter 4: A cloud-based NFC payment model (NFC Cloud Wallet) was developed and its respective protocol was designed and analysed from the security point of view.
Objective 3: To design and evaluate a novel secure NFC transaction authentication protocol based on our second developed model in which it proposes a trusted relationship between a single MNO and the merchant in the transaction architecture.	We accomplished this objectives in Chapter 5: A sub-model of the initially NFC Cloud wallet was developed in which proposed a new method for transaction execution. Thereafter, its respective protocol was designed and a detail security analysis was provided to justify its utility and reliability.
Objective 4: To design and evaluate a novel secure NFC transaction authentication protocol based on our third developed model in which it proposes a trusted relationship between multiple MNOs and the merchant in order to provide a complete transaction solution based on the second and third models.	This objective was achieved in chapter 6: A secure transaction authentication protocol was designed based on the same scenario as the second proposed protocol. However, the interactions architecture among transaction players differs with the second protocol since this protocol considers authenticating multiple MNOs. a detail security analysis is thus provided to justify the utility and reliability of such protocol.

7.3 Research Limitations and Future Work

The research in this thesis was based on a number of assumptions enumerated in chapters 4, 5 and 6. Different directions of future work have been identified, some to reduce or eliminate some of these assumptions. Some areas of future work are summarised as follows.

Promising benefits have been presented by cloud computing for both users and service providers, thus there is a high possibility for smart phones to be widely used in access points. There are several similarities between cloud computing and web servers (Avmerich et al., 2008) and so similar web server attacks are possible on the cloud environment accordingly. Therefore the servers must be protected by appropriate security mechanisms. However, the cloud approach must be highly protected since a successful attack on a cloud environment can have serious impacts on both users' personal information as well as service providers. A secure authentication mechanism that should not interfere with existing SIM authentication can be developed to secure the cloud's authentication with the NFC device in the second and third protocols (chapter 5 and 6).

A proof of concept prototype can be implemented in order to determine the reliability of the proposed protocols in terms of number of factors such as timing issues. This implementation refers to the performance domain of the proposed protocols which can be taken into the account to consider the performance of the protocols rather than their security, which is discussed in this thesis. The idea of the proposed protocols can also be extended to a multi-party protocol. Furthermore, other possible architectures in this area should be explored and defined in order to finalize the most reliable architecture for cloud-based NFC payment applications. In addition, this thesis provides related issues that are essential to investigate, such as other possible ecosystem architectures, players with their roles, different access controls and ownership issues in NFC ecosystem. Although this research suggests a new payment method, we do not recommend it for large transactions (over £50.00) to avoid security limitations imposed by technology providers. In return, our work offers a faster and more streamlined purchasing process.

The proposed protocols in this thesis are designed to exchange digital transaction data. However, these protocols can be extended to be support contract signing, certified digital product delivery, and certified email. Moreover, further research can be carried out to

consider the possibilities of enforcing honest transaction party(s) to the proposed NFC transaction protocols which might decrease the number of exchanged messages in these protocols. Thus, enforcing honest party(s) may result in more efficient NFC transaction protocols. In addition, the origin of customers is known to merchants in the protocols proposed in this thesis in which ensures the identity of customers while making the payment. However, some customers may prefer to stay anonymous to merchants; therefore, for future research, anonymity can be taken into consideration towards extending the proposed protocols.

7.4 Summary

In order to provide an interoperable service for consumers, having a bottom layer standardized approach is required. A device that features ISO 18092 may not be able to act as a contactless credit card or a reading device for a smart poster. Therefore, all layers above require a clear definition of data exchange format, interfaces, and Application Programming Interfaces (APIs). The present problem during the standardization of a technology is that a stakeholder may not disclose their intention in the beginning.

According to the present trials in developing industries, users have started paying with their mobile phones and it seems that they have found it convenient. Assuming these services meet the majority of client expectations, NFC mobile payments will rapidly get adopted and used within societies. In all cases, the technology is in the position to go live. However, the concentration should be on developing standards and understanding the best practices within the industry. From a business perspective, more implementation models should be explored in order to fit the needs of each stakeholder and support their commercial requirements. Thus a particular consideration should be on the SE which is rapidly evolving. For example, something that was just a theory and hard to achieve two years ago, is now becoming a common practice. Mobile devices may have more than one type of SE and therefore potentially, more than one type of SE issuer. Although this offers an increased choice to stakeholders, it also makes the ecosystem more complex.

References

Agar, J. (2013). *Constant touch: A global history of the mobile phone*. Icon Books.

Ahson, S. A., & Ilyas, M. (Eds.). (2012) *Near field communications handbook* (Vol. 13). CRC Press.

Akram, R.N., Markantonakis, K., & Mayes, K.E. (2010a) 'A Paradigm Shift in Smart Card Ownership Model', in *Proceedings of the 2010 International Conference on Computational Science and Its Applications (ICCSA)*, B. O. Apduhan, O. Gervasi, A. Iglesias, D. Taniar, and M. Gavrilova, Eds. Fukuoka, Japan: IEEE Computer Society. pp. 191–200.

Akram, R.N., Markantonakis, K., & Mayes, K.E. (2010b) 'A Dynamic and Ubiquitous Smart Card Security Assurance and Validation Mechanism', in proceedings of the *25th IFIP International Information Security Conference (SEC)*, ser. IFIP AICT Series, K. Rannenberg and V. Varadharajan, Eds. Brisbane, Australia: Springer. pp. 161–172.

Aldershof, P. (2012) 'Kick Start the NFC Ecosystem', in *IT-Trans, IT Solutions for Public Transport* (No. Session 1).

Alliance, S. C. (2011) 'The Mobile Payments and NFC Landscape: A US Perspective', *Smart Card Alliance*.

Alpar, G., Batina, L., and Verdult, R. (2012) 'Using NFC phones for proving credentials', In *Measurement, Modelling, and Evaluation of Computing Systems and Dependability and Fault Tolerance*, Springer. pp. 317-330.

Asokan, N., Janson, P., Steiner, M., Waidner, M. (1997) 'State of the Art in Electronic Payment Systems', *IEEE Computer Society Press*, Vol. 30 (9), pp. 28- 35.

Association. G. (2007) *Mobile NFC technical guidelines*, GSM Association, 1st Floor, Mid City Place, 71 High Holborn, London WC1V 6EA, United Kingdom, Tech. Rep.

AT&T (2013) *AT&T Cloud News*. Available at: http://www.att.com/gen/press-room?pid=20106 [Accessed November 7, 2013].

Aydin, M. N. (2013) *Design Science Perspective on NFC Research: Review and Research Agenda*, Informatica. pp. 203-218.

Aymerich, F. M., Fenu, G., & Surcis, S. (2008) 'An approach to a cloud computing network', in *proceedings of the 1st International Conference on the Applications of Digital Information and Web Technologies (ICADIWT)*, IEEE. pp.113-118.

BBC News (2007) *Hackers target TK Maxx customers.* Available at: http://news.bbc.co.uk/1/hi/business/6508983.stm [Accessed April 13, 2013].

Bellare, M., Namprempre, C. (2000) 'Authenticated encryption: relations among notions and analysis of the generic composition paradigm', in proceedings of the *International Conference on Advances in Cryptology ASIACRYPT*, Springer Berlin Heidelberg. pp. 531–545.

Bender, H., Kolehmainen, M., Lehmann, G., Parantainen, J., Staufer, M., & Tong, M. (2011). 'Business transformation of the provisioning process for Machine-to-Machine', in proceedings of the *15th International Conference on Intelligence in Next Generation Networks (ICIN)*, IEEE. pp. 175-180.

Benyo, B., Vilmos, A., Kovacs, K., & Kutor, L. (2007) 'NFC applications and business model of the ecosystem', in proceedings of the *16th IST Mobile and Wireless Communications Summit, 2007.* IEEE. pp. 1-5.

Benyó, B. (2007) 'Near Field Communication Technology: Contactless Applications in Mobile Environment', In proceedings of the *8th International Symposium of Hungarian Researchers on Computational Intelligence and Informatics*.

Benyó, B., Vilmos, A., Fordos, G., Sódor, B., & Kovács, L. (2009) 'The StoLPan view of the NFC ecosystem', in *Wireless Telecommunications Symposium, 2009*, IEEE. pp. 1-5.

Boly, J.P, Bosselaers, A., Cramer, R., Michelsen, R., Mjolsnes, S.F., Muller, F., Pedersen, T.P., Pfitzmann, B., Rooij, P., Schoenmakers, B., Matthias, S., Vallee, L. & Waidner, M. (1994) 'The ESPRIT project CAFÉ – high security digital payment systems', in *ESORICS*, pp. 217 – 230.

Bodhani, A. (2013) 'New ways to pay [Communications Near Field]', *Engineering & Technology*, 8(7), pp. 32-35.

Bouwman, H., de Vos, H., & Haaker, T. (Eds.) (2008). *Mobile service innovation and business models [electronic resource]*. Springer.

Brian, H. A. Y. E. S., Brunschwiler, T., Dill, H., Christ, H., Falsafi, B., Fischer, M., & Zollinger, M. (2008) 'Cloud computing', *Communications of the ACM*, *51*(7), pp. 9-11.

Brookson, C. (1994) *GSM (and PCN) Security and Encryption*. Available at: www.brookson.com/gsm/gsmdoc.pdf [Accessed September 9, 2011].

Bugiotti, F., Goasdoué, F., Kaoudi, Z., & Manolescu, I. (2012) 'RDF data management in the Amazon cloud', in *Proceedings of the 2012 Joint EDBT/ICDT Workshops*. ACM. pp. 61-72.

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009) 'Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility', *Future Generation computer systems, 25*(6), pp. 599-616.

Chaum, D. (1985) 'Security without identification: transaction systems to make big brother obsolete', *Communication of the ACM*, 28(10), pp. 1030-1044.

Chen, W., Hancke, G., Mayes, K., Lien, Y., Chiu, J.H. (2010) 'NFC mobile transactions and authentication based on GSM network', in *International Workshop on Near Field Communication*, IEEE Computer Society, pp. 83-89.

Choudhary, B. & Risikko, J. (2006) 'Mobile Financial Services Business Ecosystem Scenarios & Consequences', *Mobey Forum*, c/o Nordea Bank, Satamaradankatu 3 B, 3rd floor, 00020 Nordea, Helsinki/Finland.

Coskun, V., Ok, K., & Ozdenizci, B. Secure Element Management. *Near Field Communication: From Theory to Practice*, pp. 311-329.

Curran, K., Millar, A., and Garvey, C.M (2012) 'Near Field Communication', in *International Journal of Electrical and Computer Engineering*, Institute of Advanced Engineering and Science Press. 2(3). pp. 371-382.

Desai, E., and Shajan, M., G. (2012) *International Journal of Engineering and Advanced Technology (IJEAT),*Vol. 2 (2). pp. 322-325.

Dix, A., Rodden, T., Davies, N., Trevor, J., Friday, A. & Palfreyman, K. (2000) 'Exploiting space and location as a design framework for interactive mobile systems', *ACM journal of Transaction on Computer Human Interaction*, 7(3), pp. 285 – 321.

Eberspaecher, J., Voegel, H. J., & Bettstetter, C. (2008) 'GSM - Architecture, Protocols and Services', 3rd Ed., *Wiley*, New York.

EMV 4.2(2008) *Book 1 Application Independent ICC to Terminal Interface Requirements, Book 2 - Security and Key Management, Book 3 - Application Specification, Book 4 - Cardholder, Attendant, and Acquirer Interface Requirements*, EMVCo Std. 4.2.

EMVCo (2007) *EMV mobile contactless payment technical issues and position paper EMVCo*, Tech. Rep.

Erin Biba (2005) *Does Your Wi-Fi Hotspot Have an Evil Twin?*, PC World, Medill News Service. Available at: http://www.pcworld.com/article/id,120054-page,1/article.html [Accessed April 12, 2014].

ETSI Specification of the Subscriber Identity Module (1996) 'Mobile Equipment (SIM - ME) interface (GSM 11.11)', *European Telecommunications Standards Institute (ETSI Std. Version 5.3.0)*, Available at: http://www.etsi.org/deliver/etsi_gts/11/1111/05.03.00_60/gsmts_1111v050300p.pdf. [Accessed January 8, 2012].

Evans, E. (2003) *Domain-Driven Design: Tackling Complexity in the Heart of Software* 1st ed., Addison-Wesley Professional.

Fisher, M., & Guha, R. (2013) *U.S. Patent No. 20,130,023,209*. Washington, DC: U.S. Patent and Trademark Office.

Francis, L., Hancke, G., Mayes, K., and Markantonakis, K. (2010) 'On the security issues of NFC enabled mobile phones', In *International Journal of Internet Technology and Secured Transactions*, Inderscience Enterprises Ltd. 2 (3-4). pp. 336-356.

Francis, L., Hancke, G., Mayes, K. & Markantonakis, K. (2010a) 'A Security Framework Model with Communication Protocol Translator Interface for Enhancing NFC Transactions', in proceedings of the 6th *Advanced International Conference on Telecommunications (AICT)*, pp. 452.

Geer, D. (2003) 'Taking Steps to Secure Web Services', *Computer*, 36 (10), pp. 14-16.

Gemalto (2011) *What is GlobalPlatform?* Available at: http://gemalto.com/nfc/global_platform.html [Accessed January 22, 2012].

Girard, P. (1999) 'Which Security Policy for Multiplication Smart Cards?' in *proceedings of the USENIX Workshop on Smartcard Technology*. Berkeley, CA, USA: USENIX Association, pp. 3–3.

GlobalPlatform (2006): GlobalPlatform Card Specification, Version 2.2,, GlobalPlatform Std.

Google (2013). Goole Wallet. Available at: http://www.google.co.uk/wallet/faq.html. [Accessed 3 April 2013].

Gregg, D.G., Kulkarni, U.R. & Vinzé, A.S., (2001) 'Understanding the Philosophical Underpinnings of Software Engineering Research in Information Systems', *Information Systems Frontiers*, 3(2), pp.169–183.

GSM Association (2007) *Pay-Buy-Mobile: Business Opportunity Analysis*. White Paper 1.0.
GSM Association (2011). *Requirements for SWP NFC Handsets V4.0*, Available: http://www.gsma.com/mobilenfc/wpcontent/uploads/2012/03/gsmarequirementsforswpnfchandsetsv4.pdf [Accessed June 2, 2011].

Guadamuz, A. (2003) 'PayPal and eBay- The legal implications of the C2C electronic commerce model', in *proceedings of the 18'h BILETA Conference: Controlling Information in the Online Environment*, UK. Available at: http://www.bileta.ac.uk/content/files/conference%20papers/2003/PayPal%20and%20eBay%20%20The%20Legal%20Implications%20of%20the%20C2C%20Elctronic%20Commerce%20Model.pdf [Accessed October 2, 2012].

Guaus, J., Kanniainen, L., Koistinen, P., Laaksonen, P., Murphy, K., Remes, J., Taylor, N., and Welin, O. (2008) *Best Practice for Mobile Financial Services: Enrolment Business Model Analysis*, Mobey Forum Mobile Financial Services Ltd., Helsinki, Finland. Available at: http://www.mobile-ecosystem.org/2008/1648/best-practice-for-mobile-financialservices.html [Accessed November 14, 2012].

Guba, E.G. & Lincoln, Y.S. (1994) 'Competing paradigms in qualitative research'. In *Handbook of qualitative research*, eds. N.Y.K. Denzin & Y.S. Lincoln,Thousand Oaks: Sage publications, pp. 105-117.

Hang, A., Broll, G., & Wiethoff, A. (2010) 'Visual design of physical user interfaces for NFC-based mobile interaction', in *proceedings of the 8th ACM Conference on Designing Interactive Systems* (DIS '10). New York, NY, USA. ACM. pp. 292-301.

Henssey, D. (2003) *The value of the mobile wallet*, White paper. Available at: www.valista.com [Accessed September 16, 2012].

Hevner, A.R., March, S.T., Park, J. & Ram, S. (2004) 'Design Science in Information Systems Research', *Management Information Systems Quarterly*, 28 (1), pp. 75-105.

Hevner, A. & Chatterjee, S. (2010). *Design Research in Information Systems: Theory and Practice* 1st ed., Springer.

Hsieh, C. (2001) 'E-commerce payment systems: critical issues and management strategies', *Human Systems Management*, Vol. 20(2), pp 131-138.

Iivari, J. (2007) 'A Pragmatic Analysis of Information Systems as a Design Science', *Scandinavian Journal of Information Systems*, 19 (2), pp. 39-64.

Innovation Research and Technology (2011), *NFC in real world: Turning the NFC promise into profitable, everyday applications.* Available at: http://innovation-group.com [Accessed March 2, 2012].

Iosup, A., Yigitbasi, N., & Epema, D. (2011) 'On the performance variability of production cloud services' In proceedings of the 11th *International Symposium on Cluster, Cloud and Grid Computing (CCGrid),*IEEE. pp. 104-113.
ISO/IEC 18092 (2004) *Near Field Communication - Interface and Protocol (NFCIP-1),* International Organization for Standardization (ISO) Std.

Java Card Platform Specification (2009): *Classic Edition; Application Programming Interface, Runtime Environment Specification, Virtual Machine Specification, Connected Edition; Runtime Environment Specification, Java Servlet Specification, Application Programming Interface, Virtual Machine Specification, Sample Structure of Application Modules,* Sun Microsystem Inc Std. Version 3.0.1.

Jendricke, U., Kreutzer, M. & Zugenmaier, A. (2002) *Mobile identity management*, Technical Report 178, Institute fur Informatik, Universitat Freiburg.

Jones, R. (2001) 'The PayPal phenomenon: Lessons from the Leading Edge of Online Payments', *CommerceNet Security and Internet Payments Research*, pp. 6-11.

Kadambi, K., S., Li, J. and Karp., A. H. (2009) 'Near-field communication-based secure mobile payment service', in *proceedings of the 11th International Conference on Electronic Commerce* (ICEC '09),. New York, NY, USA, ACM. pp. 142-151.

Kandukuri, B. R., Paturi, V. R., & Rakshit, A. (2009) 'Cloud security issues', in proceedings of the *International Conference on Services Computing, (SCC'09*). IEEE. pp. 517-520.

Kanniainen, L. (2010) 'Alternatives for banks to offer secure mobile payments', *International Journal of Bank Marketing,* 28(5), pp. 433-444.

Kauffman, R. J., Liu, J., & Ma, D. (2013) 'Technology investment decision-making under uncertainty: the case of mobile payment systems', in *proceedings of the 46th Hawaii International Conference on System Sciences (HICSS)*. Maui, Hawaii. IEEE. pp. 4166-4175.

Kerem, O. K., Coskun, V., Ozdenizci, B., & Aydin, M. N. (2013) 'A Role-Based Service Level NFC Ecosystem Model', *Wireless Personal Communications*, *68*(3), pp. 811-841.

Kiselev, S. A., & Tokareva, N. N. (2012) 'Reduction of the key space of the cipher A5/1 and invertibility of the next-state function for a stream generator', *Journal of Applied and Industrial Mathematics*, *6*(2), 194-202.

Klein, K.K. & Myers, M.D. (1999) 'A Set of Principles for Conducting and evaluating Interpretive Field Studies in Information Systems', *MIS Quarterly,* 23 (1), pp. 67-94.

Ko, R. K., Lee, B. S., & Pearson, S. (2011) 'Towards achieving accountability, auditability and trust in cloud computing' in *Advances in Computing and Communications*. Springer Berlin Heidelberg. pp. 432-444.

Konidala, D., M., Dwijaksara, M., H., Kim, K., Lee, D., Lee, B., Kim, D. and Kim, S. (2012) 'Resuscitating privacy-preserving mobile payment with customer in complete control', *Personal Ubiquitous Computing*, 16(6), pp. 643-654.

Kounelis, I., Loschner, J., Shaw, D., & Scheer, S. (2012) 'Security of service requests for cloud based m-commerce' in *proceedings of the 35th International Convention*. IEEE. pp. 1479-1483.

Kranz, M., Murmann, L., & Michahelles, F. (2013) 'Research in the Large: Challenges for Large-Scale Mobile Application research: A Case Study about NFC Adoption using Gamification via an App Store' *International Journal of Mobile Human Computer Interaction (IJMHCI), 5*(1), pp. 45-61.

Kuhn, T. (1996) *The Structure of Scientific Revolutions*, Chicago: University of Chicago Press.

Laugesen, J. & Yuan, Y. (2010) 'What Factors Contributed to the Success of Apple's iPhone?' in *proceedings of the 9th International Conference on Mobile Business / 9th Global Mobility Roundtable*, ser. ICMB-GMR . Washington, DC, USA: IEEE Computer Society, pp. 91–99.

Leavitt, N. (2009) 'Is cloud computing really ready for prime time', *Growth*, 27(5).

Lee, Y. K., Park, J. H., Chung, N., & Blakeney, A. (2012). 'A unified perspective on the factors influencing usage intention toward mobile financial services', *Journal of Business Research, 65*(11), 1590-1599.

Lehdonvirta, V., Soma, H., Ito, H., Yamabe, T., Kimura, H. and Nakajima, T. Ubipay (2009) 'Minimizing transaction costs with smart mobile payments', in *proceedings of the 6th International Conference on Mobile Technology, Application; Systems, Mobility*. New York, NY, USA, ACM. pp. 1-7.

M'Chirgui, Z. (2005) 'The Economics of the Smart Card Industry: Towards Coopetitive Strategies', *Economics of Innovation and New Technology*, 14(6), pp. 455–477.

Madlmayr, G. (2008) 'A mobile trusted computing architecture for a near field communication ecosystem', In *Proceedings of the 10th International Conference on*

Information Integration and Web-based Applications & Services(iiWAS '08), pp. 563-566, New York, NY, USA, ACM.

Madlmayr, G., Langer, J., Scharinger, J. (2008) 'Managing an NFC ecosystem', in *Proceedings of the 7th International Conference on Mobile Business*, Washington, DC, USA: IEEE Computer Society, pp. 95–101.

Madlmayr, G., Langer, J., Kantner, C., Scharinger, J., & Schaumuller-Bichl, I. (2009) 'Risk analysis of over-the-air transactions in an NFC ecosystem', in *proceedings of the 1st International Workshop on Near Field Communication, NFC'*. IEEE. pp. 87-92.

March, S.T. & Smith, G.F. (1995) 'Design and Natural Science Research on Information Technology', *Decision Support Systems,* 15 (4), pp. 251-266.

March, S.T. & Storey, V.C. (2008) 'Design Science in the Information Systems Discipline: An Introduction to the Special Issue on Design Science Research', *Management Information Systems Quarterly,* 32 (4), pp. 725-730.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011) 'Cloud computing: The business perspective', *Decision Support Systems*, *51*(1), pp. 176-189.

MasterCard (2013). MasterPass. Available at: https://masterpass.com/online/Wallet/Help?cid=127568. [Accessed November 12, 2013].

Matsuo, S. I., Miyazaki, K., Otsuka, A., & Basin, D. (2010). *How to Evaluate the Security of Real-Life Cryptographic Protocols?*. In Financial Cryptography and Data Security (pp. 182-194). Springer Berlin Heidelberg.

Mayes, K.E. & Markantonakis, K. (2008) *Smart cards, tokens, security and applications,* Springer-Verlag New York Inc.

Mell, P. & Grance, T. (2009) *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology, Information Technology Laboratory, USA.

Meyer, U., and Wetze, S. (2004), 'On the Impact of GSM Encryption and Man-in-the-Middle Attacks on the Security of Interoperating GSM/UMTS Networks', *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 2876-2883.

Mingers, J. (2001) 'Combining IS Research Methods: Towards a Pluralist Methodology', *Information Systems Research,* 12 (3), pp. 240-259.

Chua, W.F. (1986) 'Radical Developments in Accounting Thought', *The Accounting Review*, 61 (4), pp. 601-632.

Mjolsnes, S.F., & Rong, C. (2001) 'Localized credentials for server assisted mobile wallet', in *proceedings of International Conference on Computer Networks and Mobile Computing (ICCNMC)*. IEEE. pp. 203-208.

Mobey Forum (2008) *Best practices for mobile financial services, enrolment business model analysis*. Available at: http://mobeyforum.org/files/bestpractice/Best%20Practices%20for%20MFS%20Enrolment%20Business%20model%20analysis%20final.pdf [Accessed June 2, 2011].

Mobey Forum (2009) *Why aren't banks rushing for NFC payments?* Available at: http:// mobeyforum.org [Accessed May 28, 2011].

Mobey Forum (2011) *Business models for NFC payments*. Available at: http://www.mobeyforum.org/whitepaper/business-models-for-nfc-payments/ [Accessed August 5, 2012]

Morse, E., A. and Raval, V. (2008) 'Payment card industry data security standards in context', *Computer Law Security Review*, 24(6), pp. 540-554.

Nakamur, Y., Hada, S. & Neyama, R. (2002) 'Towards the Integration of Web Services Security on Enterprise Environments', in *proceedings of the 2002 Symposium on Applications and the Internet (SAINT'02w)*, Nara, Japan. IEEE, pp. 166-175.

NFC Forum (2008) *Essentials for successful NFC mobile ecosystems*, Available at: www.nfcforum.org/resources/white papers/NFC Forum Mobile NFC Ecosystem White Paper.pdf. [Accessed March 12, 2011].

NFC Forum (2013) *What are the operating modes of NFC devices?*, Available at: http://nfc-forum.org/resources/what-are-the-operating-modes-of-nfc-devices/. [Accessed April 12, 2014].

NFC World (2012), *Fujitsu puts NFC into cloud-based data transfer service*. Available at: http://www.nfcworld.com/2011/07/22/38759/fujitsu-puts-nfc-into-cloud-based-data-transfer-service [Accessed September 3, 2011]

NFC World (2012a) *McDonald's to test cloud-based NFC payments in Austria*. Available at: http://www.nfcworld.com/2012/04/24/315260/mcdonalds-to-test-cloud-based-nfc-payments-in-austria [Accessed April 25, 2012].

NFC World (2013). *MasterCard unveils MasterPass digital wallet and mobile payments platform*. Available at: http://www.nfcworld.com/2013/02/25/322610/mastercard-unveils-masterpass-digital-wallet-and-mobile-payments-platform/. [Accessed March 3, 2013].

NFC World (2013a). *NFC Trials, Pilots, Tests and Live Services around the World.* Available at: http://www.nfcworld.com/list-of-nfc-trials-pilots-tests-and-commercial-services-around-the-world/ [Accessed October 11, 2013].

NFC World (2013b). *Bell ID launches NFC secure element in the cloud platform*. Available at: http://www.nfcworld.com/2013/06/05/324381/bell-id-launches-nfc-secure-element-in-the-cloud-platform/ [Accessed April 14, 2014].

O'Neill, M., Hallam-Baker, P., Cann, S.M., Shema, M., Simon, E., Watters, P.A. & White, A. (2003) *Web Services Security*, 1st edn, New York. USA: McGraw-Hill.

Orlikowski, W.J. & Baroudi, J. (1991) 'Studying information technology in organizations: Research approaches and assumptions', *Information Systems Research*, 2 (1), pp. 1-28.

Owen, C. (1997) 'Design Research: Building the Knowledge Base', *Journal of the Japanese Society for the Science of Design*, 5 (2), pp.36-45.

Ozdenizci, B., Aydin, M. N., Coskun, V., & Ok, K. (2010) 'NFC research framework: a literature review and future research directions', in *14th IBIMA Conference*, pp. 23-24.

Ozdenizci, B., Aydin, M. N., Coskun, V., & Kerem, O. (2010a) 'Design science in NFC research', in *proceedings of the International Conference for Internet Technology and Secured Transactions (ICITST)*,IEEE. pp. 1-6.

Pailles, J., Gaber, C., Alimi, V., and Pasquet, M. (2010) 'Payment and Privacy: A Key for the Development of NFC Mobile', in *proceedings of the International Symposium Collaborative Technologies and Systems (CTS).* IEEE. pp. 378 –385.

PayPal (2013). New Digital Wallet. Available at: www.paypal.com [Accessed November 17, 2013]

Pries-Heje, J. & Baskerville, R. (2008) 'The Design Theory Nexus', *Management Information Systems Quarterly*, 32 (4), pp. 731-755.

Purao, S. (2002) *Design Research in the Technology of Information Systems: Truth or Dare*, Pennsylvania State University, Atlanta. Available at: http://purao.ist.psu.edu/working-papers/dare-purao. pdf. [Accessed April 2, 2013].

Rannenberg, K. (2004) *Identity management in mobile cellular networks and related applications*, Information Security Technical Report 9, Johann Wolfgang Goethe University Frankfurt. Elsevier. 9(1). pp. 77-85.

Rao, Y., Feng, B.Q., Han, J.C. & Li, Z.C. (2004) 'SX-RSRPM: a Security Integrated Model for Web Services', in *proceedings of the 3rd International Conference on Machine Learning and Cybernetics*. Shanghai, China, IEEE. Vol. 5. pp. 2953-2958.

Reveilhac, M. & Pasquet, M. (2009) 'Promising Secure Element Alternatives for NFC Technology', in *proceedings of the 1st International Workshop on Near Field Communication, 2009. NFC '09*, pp. 75.

Roland, M., Langer, J., and Scharinger, J. (2013) 'Applying relay attacks to Google Wallet', in *proceedings of the 5th International Workshop on Near Field Communication (NFC)*. IEEE. Zurich, Switzerland.

Schamberger, R., Madlmayr, G. and Grechenig, T. (2013) 'Components for an interoperable NFC mobile payment ecosystem', in *proceedings of the 5th International Workshop Near Field Communication (NFC)*, pp. 1-5.

Schneiderman, R. (2011) 'For Cloud Computing, the Sky Is the Limit' [Special Reports]. *Signal Processing Magazine*, IEEE. 28(1), pp. 15-144.

SecureIDNews (2013) *Bell ID releases new NFC secure element for the cloud*. Available at: http://secureidnews.com/news-item/bell-id-releases-new-nfc-secure-element-for-the-cloud/ [Accessed April 14, 2014].

Smart Card Alliance Mobile and NFC Council (2012) *NFC Application Ecosystems: Introduction, Peer-to-Peer, NFC Tags/Posters and Product Label Applications*, Available at: http://www.smartcardalliance.org/resources/webinars/nfc_app_ecosystem/20120927_NFC_Application_Ecosystems.pdf [Accessed April 12, 2014]

Stolplan (2011), *Dynamic management of multi-application secure elements*. Available at: http://www.nfc-forum.org/resources/white_papers/Stolpan_White_Paper_08.pdf [Accessed February 19, 2012]

Subashini, S., & Kavitha, V. (2011) 'A survey on security issues in service delivery models of cloud computing', *Journal of Network and Computer Applications, 34*(1), pp. 1-11.

Technical Specification Group Core Network (1999) *Numbering, addressing and identification*. Available at: www.arib.or.jp/english/html/overview/doc/STD-T63v9_30/5Appendix/R99/23/23003-3f0.pdf [Accessed June 6, 2011]

TheShmooGroup (2008) *Airsnarf-A Rogue APSetup Utility, Version0.2*. Available at: http://airsnarf.shmoo.com/ [Accessed April 12, 2014].

Tiwari, R., Buse, S., & Herstatt, C. (2007). *Mobile services in banking sector: the role of innovative business solutions in generating competitive advantage* (No. 48). Working Papers/Technologie-und Innovationsmanagement, Technische Universität Hamburg-Harburg.

Tsiakis, T. & Sthephanides, G. (2005) 'The concept of security and trust in electronic payments', *Computers & Security*, Vol. 24(l), pp. 10- 15.

Turban, E., King, D., Lee, J., & Viehland, D. (2004) 'Electronic Commerce: A Managerial Perspective', *Upper Saddle River,* New Jersey: Prentice Hall, ISBN 0131230158.

Ulvedal, J. E. (2013) *The implementation of NFC-based mobile payment in Norway: a case study of the emerging NFC business ecosystem in Norway*. University of Agder. Available at: http://brage.bibsys.no/hia/handle/URN:NBN:no-bibsys_brage_43709 [Accessed 12, February 2011].

Vaishnavi, V. & Kuechler, W. (2009) *Design Science Research in Information Systems.* DESRIST.org. Available at: http://desrist.org/desrist [Accessed August 3, 2013].

Van Damme, G., Wouters, K. M., Karahan, H., & Preneel, B. (2009) 'Offline NFC payments with electronic vouchers', in *Proceedings of the 1st ACM workshop on Networking, systems, and applications for mobile handhelds*, pp. 25-30. ACM.

Verzion (2013) *Tap into Endless Possibilities with the Cloud*. Available at: http://www.verizonenterprise.com/us/solutions/dynamic-cloud/ [Accessed November 4, 2013].

Visa (2013). Visa Mobile Wallet. Available at: http://www.myvisawallet.com/ [Accessed October 8, 2013].

Waris, F., Mubarik, F., & Pau, L. F. (2006) *Mobile Payments in the Netherlands: Adoption Bottlenecks and Opportunities, Or & Throw Out Your Wallets*. SSRN. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=898921 [Accessed August 11, 2013].

Webster Dictionary (2013). Methodology. Available at: http://www.merriamwebster.com/dictionary/methodology [Accessed December 16, 2013].

Widmann, R., Grunberger, S., Stadlmann, B., & Langer, J. (2012) 'System Integration of NFC Ticketing into an Existing Public Transport Infrastructure', in *proceedings of the 4th International Workshop on Near Field Communication (NFC),*IEEE. pp. 13-18.

Wright, D. (2002) ‘Comparative Evaluation of Electronic Payment Systems’, *Journal of Information Systems and Operational Research*, Vol. 40(l). pp. 71-85.

Yang, A. (2002) 'Web Services Security', *Journal of European Alliance for Innovation (EAI)*, September (1), pp. 19-23.

Yarbrough, S., and Taylor, S. (2012) *The future of NFC payments: Is it in the Cloud or NFC?* TSYS. Available at: http://www.tsys.com/Downloads/upload/Future-of-Payments-Cloud-of-NFC-WP-2.pdf [Accessed December 8, 2012].

Zissis, D., and Lekkas, D. (2012) ‘Addressing cloud computing security issues’, *Future Generation Computer Systems*, 28(3), pp. 583-592.