Secure e-Payment Portal Solutions Using Mobile Technologies and Citizen Identity Scheme

by

Wei-Dar Chen [Calvin]

Thesis submitted to the University of London
for the degree of Doctor of Philosophy

Smart Card Centre
Information Security Group
Department of Mathematics
Royal Holloway, University of London

2013

Declaration

These doctoral studies were conducted under the supervision of Prof. Keith E. Mayes

The work presented in this thesis is the result of original research carried out by myself, in collaboration with others, whilst enrolled in the Department of Mathematics as a candidate for the degree of Doctor of Philosophy. This work has not been submitted for any other degree or award in any other university or educational establishment.

Wei-Dar Chen [Calvin]
March, 2013

Acknowledgements

I have taken efforts in this thesis. However, it would not have been possible without the kind support, encouragement and help of many individuals and organisations. I would like to extend my sincere thanks to all of them.

I would like to express my sincere gratitude to my supervisor, Dr. Keith E. Mayes, for always giving me magnificent guidance, encouragement and support over these years. His versatile and profound knowledge provided me with great suggestions and inspiration on the research. Besides learning academic skills from him, his personality, attitude, positive thinking and perception broadened my mind. Deeply grateful for his time and consideration. A great mentor like Dr Mayes can change your life.

I also would like to thank my Dr. Konstantinos Markantonakis for always giving me nice advices. Deeply thankful to Dr. Gerhard Hancke and Sheila Cobourne for their generous help on the papers and thesis proofreading and English correction. Additionally I would like to thank Smart Card Centre for offering studentship in the periods of my doctoral study, without which I could not have pursued my studies. Both Smart Card Centre and the Information Security Group were forthcoming with financial support for all travel and conference expense related to my studies.

I am most grateful to Dr. Yuan-Hung Lien, he has also given me great advices and inspiration from the ideas and details of the research. And introduced me to Dr. Jung-Hui Chiu and Taiwan Information Security Centre (TWISC), without Dr. Chiu's professional advice and help from TWISC, my research progress could be delayed.

I am indebted to Dr. Char-Shin Miou and his team (Yu-Zhang Soong, Po-Wen Ke) from Chunghwa Telecom Laboratories. The practical work of this thesis was made possible largely through Dr. Miou's great support and gave me the opportunity to learn programming skills and facility supports. The practical work could not be completed without his kind and generous support.

My great gratitude towards my parents and my sister, without their constant

encouragement and support I would not have the will power to finish this long race. Especially to my dad, your meaningful and brilliant quotes gave me constructive mindset to keep pursuing the goal. My mom and my sis, having chat with you always loosened up tenseness whenever I faced difficulties on the research and the life.

Finally, I would like to thank all people who have directly and indirectly helped me during my doctoral study in the UK.

Publications

A number of papers resulting from my work in this thesis have been presented in corresponding conferences. Here is the list of my publications:

1. Wei-Dar Chen; Gerhard P. Hancke; Keith. E. Mayes; Yuan-Hung Lien; Jung-Hui Chiu, "NFC Mobile Transactions and Authentication Based on GSM Network," *Near Field Communication (NFC), 2010 Second International Workshop on* , vol., no., pp.83,89, 20-20 April 2010.

2. Wei-Dar Chen; Gerhard P. Hancke; Keith. E. Mayes; Yuan-Hung Lien; Jung-Hui Chiu, "Using 3G network components to enable NFC mobile transactions and authentication," *Progress in Informatics and Computing (PIC), 2010 IEEE International Conference on* , vol.1, no., pp.441,448, 10-12 Dec. 2010.

3. Wei-Dar Chen; Keith. E. Mayes; Yuan-Hung Lien; Jung-Hui Chiu, "NFC mobile payment with Citizen Digital Certificate," *Next Generation Information Technology (ICNIT), 2011 The 2nd International Conference on* , vol., no., pp.120,126, 21-23 June 2011.

Abstract

The increasing technical capabilities of mobile phones have resulted in several mobile payment (m-payment) methods being proposed. Handsets like smartphones provide powerful computation capability that allow applications such as m-payment transactions to become more secure and intuitive to users. Near Field Communication (NFC) technology has been considered as a potential killer technology that will greatly impact the way mobile devices are used. NFC is a short range wireless communication interface that allows the integration of a mobile device into existing contactless infrastructures. It offers the potential for advanced cryptographic calculations for security protection, with the convenience of mobile phone usage. Within this thesis, a number of existing technologies are introduced and used in conjunction with NFC.

NFC enhances a range of applications such as contactless payment, ticketing, transportation, user identification, and data access. Three different kinds of m-payment systems are proposed in this thesis, all of which are principally Mobile Network Operator (MNO) centric rather than based around a conventional Bank Issuer. The research focus is on achieving secure payment transactions and user authentication within a conventional merchant payment environment. The proposed solutions exploit different existing technologies such as **Second-Generation wireless telephone technology(2G)**, **Third-Generation wireless telephone technology (3G)**, and **Citizen Identity Cards and Public Key Infrastructure (PKI)** combined with NFC to provide strong security and ease of use.

An important design goal was to re-use as much as possible of the existing mobile technology security so that the proposed solutions could be readily implemented into current Infrastructure, and provide secure, manageable, scalable and ubiquitous m-payment services.

This thesis describes the critical technologies and then presents the design and analysis of the proposed m-payment solutions.

Contents

List of Figures

LIST OF FIGURES

List of Tables

Abbreviations

2G:	Second Generation Mobile Communications
3DES:	Triple Data Encryption Standard
3G:	Third Generation Mobile Communications
3GPP:	Third Generation Partnership Project
AES:	Advanced Encryption Standard
AuC:	Authentication Center
BSC:	Base Station Controller
BSS:	Base Station Subsystem
BTS:	Base Transceiver Station
CDC:	Citizen Digital Certificate
CES:	Data Encryption Standard
CLF:	Contactless Frontend
CS:	Circuit-Switched
DoS:	Denial of Service
DSRC:	Dedicated Short Range communications
DSA:	Digital Signature Algorithm
DSS:	Digital Signature Standard
ECC:	Elliptic Curve Cryptography
ECMA:	European Computer Manufacturers Association
EDGE:	Enhanced Data rates for GSM Evolution
EIR:	Equipment Identity Register
EMV:	Europay, MasterCard and VISA
ETSI:	European Telecommunications Standards Institute
FDMA:	Frequency Division Multiple Access
FIPS PUB:	Federal Information Processing Standards Publications
GGSN:	Gateway GPRS Support Node
GPKI:	Governmental Public Key Infrastructure
GPRS:	General Packet Radio Service
GSM:	Global System for Mobile Communications
HCI:	Host Controller Interface
HLR:	Home Location Register
HMAC:	Hash Message Authentication Code
IEEE:	Institute of Electrical and Electronics Engineers
IETF:	Internet Engineering Task Force

IMEI:	International Mobile Equipment Identity
IMSI:	International Module Subscriber Identity
IrDa:	Infrared Data Association
ISO/IEC:	International Organization for Standardization
Kc:	Ciphering Key
Ki:	Individual subscriber authentication Key
LAI:	Location Area Identity
LLCP:	Logical Link Control Protocol
MD:	Message Digest
ME:	Mobile Equipment
MNO:	Mobile Network Operator
MS:	Mobile Station
MSC:	Mobile Switching Center
MSISDN:	Mobile Station ISDN
MSRN:	Mobile Station Roaming Number
NFC:	Near Field Communication
NDEF:	NFC Data Exchange Format
NIST:	National Institute of Standards and Technology
NPC:	Natural Person Certificate
NSS:	Network Switching Subsystem
OMC:	Operations and Maintenance Center
OSS:	Operation Support Subsystem
OTA:	Over The Air
PCB:	Printed Circuit Board
PCD:	Proximity Coupling Device
PIN:	Personal Identity Number
PKI:	Public Key Infrastructure
PS:	Packet-Switched
RFC:	Request for Comments
RSA:	Ron Rivest, Adi Shamir and Leonard Adleman public-key cryptography algorithm
RTD:	Record Type Definition
SE:	Secure Element
SGSN:	Serving GPRS Support Nodes
SHA:	Secure Hash Algorithm
SIM:	Subscriber Identity Module
SMS:	Short Messaging Service
SMSC:	SMS Switching Centre
SWP:	Single Wire Protocol
TDMA:	Time Division Multiple Access
UICC:	Universal Integrated Circuit Card
vCard:	Versitcard
VCD:	Vicinity Coupling Device
VLR:	Visitor Location Register

WEP:	Wired Equivalent Privacy
Wi-Fi:	Wireless Fidelity, a synonym for wireless local area network (WLAN)
WPA:	Wi-Fi Protected Access
WWW:	World Wide Web

Chapter 1

Introduction

Contents

This chapter gives an overview of the thesis. We provide the motivation and objectives for our research. In this chapter, we also present the overall structure of the thesis.

1.1 Motivation

Over the years many different kinds of wireless technologies have been developed in response to demands for diverse communication functionalities. One of the most prevalent areas where wireless technology and application development have skyrocketed is in mobile communication systems, where Internet connectivity and phone "app" have established important roles in our daily life. Whereas the emphasis on wireless solutions was once on maximising useful range, there is also interest in the localised, shorter-range, Personal Area

Network (PAN). PAN technologies include Bluetooth, 802.11(Wi-Fi), ZigBee, Ultra Wide Band (UWB), and Near Field Communications (NFC). Each has its own useful characteristics such as data transmission speed, range and power consumption.

In parallel to the development of wireless communications, the mobile phone has increasingly become a convenient platform for user services. The diversity of phone "apps" available for download is enormous, however to enable significant commercial services there needs to be a secure m-payments solution. There is no shortage of candidate solutions although most are proprietary and unpublished, which is of concern, especially as phone platforms are in general untrusted. The lack of a common solution, associated standardisation and commercial infrastructure support, arises in part because proposed schemes often require too many extensive and complicated changes to existing systems, platforms and processes. As a result, most legacy m-payment and money transfer schemes tend to be low-tech, using the most basic capabilities of mobile phones and without the ability to directly interact with Point of Sale Terminals (POS) in shops. However we are now beginning to see m-payment solutions based on more advanced capabilities of smart phones that have NFC capability. NFC offers customers a more intuitive and natural "touch-and-pay" experience yet providing attack resistant security protection via the standardised NFC Secure Element (SE).

There are many implementation options and how to make best use of mobile, Subscriber Identity Module (SIM) and NFC technologies to delivery an intuitive yet secure mobile payment scheme with respect to different types of payment methods (e.g. services in conjunction with e-cash and credit/debit cards) is becoming a fascinating research area.

A number of mobile payment related papers [172][139][140] put most emphasis on low-value transactions as a means to reduce the security requirements and necessary protections. Some researchers [161][163][164] have proposed more ambitious mobile payment architectures involving various entities e.g. mobile network operators (MNO), banks, service providers (SP) and certificate authorities (CA). However, these solutions can be limited to certain scenarios and to a closed set of commercial parties, narrowly restricting what you buy, where you buy it and how you pay for it. Furthermore they are often aimed at copying an existing payment solution rather than using the full capabilities of modern mobile devices, which can for example emulate payment cards, act as multi-media terminal devices and application platforms, have on-line and off-line communication capability, be location aware, and interrogate RFID tagged items including user IDs and passports.

The MNO is best placed to make best use of the advanced mobile capabilities, however there is strong and competing commercial interest from other parties, notably banks. The trusted entity that has control of the solutions and its se-

curity technology is in a powerful business position. Trusted Services Manager (TSM) was invented as a means of interfacing of financial institutions.

If the business conflicts are put aside then the MNO could in principle provide all the functionality and processes of mobile payment, satisfying the role of bank and TSM. For this to be practical, changes to the existing mobile implementation would need to be minimised, and in particular using the proven security capabilities of mobile networks. One of the criticisms of a MNO centric approach is that user registration for a SIM is weak compared to for example a bank card or a passport. An MNO has historically been focused on a communications payment associated with a unique user account rather than establishing a strong link to the user, and in the UK for example it is possible for pre-pay mobile customers to remain anonymous. For convenient low value transactions this anonymity could be attractive to users, however if the MNO is to be at the heart of future high value and sensitive transactions then an option is needed that provides stronger linkage with user identity.

1.2 Objectives

This thesis will present a set of secure mobile payment solutions, primarily for physical shop style purchases, which exploit existing infrastructures, technologies and security by reusing them for flexible payment, including customer self-service check-out. This is in contrast to m-payment system proposals that

require multiple complex changes and are not designed to make use of credentials that customers may already have. The set of solutions proposed in this research supports both GSM and 3G and can be linked to pre-existing citizen identity schemes, with the Chinese Citizen Digital Certificate (CDC) used as an example.

The solutions rely on NFC technology and also make use of temporary location indicators inherent in the mobile networks that can be used to counter potential fraud and security attacks.

In general, the objectives for the research were to create practical and secure m-payment solutions by reusing "legacy" security capabilities combined with NFC technology, location awareness and the customer's existing and strongly established identity "credentials".

1.3 Organisation of Thesis

The remainder of this thesis is organised as follows.

Background and Literature review: We present background material on NFC, GSM and 3G(UMTS), Citizen Digital Certificate (CDC), and mobile payment from Chapter 2 to Chapter 5 respectively. These are prerequisites for understanding our proposals for secure infrastructures suited to NFC-enabled mobile payment schemes. Chapters 2,3,and 4 provide

necessary knowledge of the technologies used in the proposed schemes. In Chapter 5, different types of m-payment schemes are discussed.

Binding of NFC with GSM and 3G network: Chapter 6 and 7 present our proposals for secure m-payment schemes in combination with NFC technology. In Chapter 6, we begin by explaining the possibility of using NFC for m-payment application, and indicating advantages from re-using existing technologies can leverage with combining the new technology, NFC. Chapter 7 is the extension work from Chapter 6, the evolution of the telecommunication network, 3G, inherits merits from the GSM as well as providing enhanced security features, this also reflects upon our proposed scheme. An overview of our proposals for both m-payment schemes is provided. Informal security analyses of the protocols are discussed as well as their advantages and disadvantages.

Binding of NFC with a PKI-based CDC card: In Chapter 8, a more advanced m-payment scheme is proposed compared to the previous two proposed schemes. A better user identity verification by binding the user's legitimate real world identity, a national ID card, with the user SIM signature in order to achieve a more secure m-payment service (with PKI system). Note that this chapter is rather independent of Chapters 6 and 7, and the reader should be able to understand most of the material presented in this chapter without reading Chapters 6 and 7. The aim of Chapter 8 is to make a handset capable of providing a similar legitimacy

for user identification like the real ID card, this allows the user to prove themselves without carrying a real ID card while the level of the public trust is still maintained. Informal security analyses of the protocols are discussed as well as advantages and disadvantages.

Practical work of the NFC CDC card m-payment scheme: Chapter 9 provides a proof-of-concept of a simplified protocol from Chapter 8, however the POS terminal is performed/replaced by an NFC handset. Runtime results and memory usage would be discussed.

Conclusions: In the final chapter of this thesis, Chapter 10, we give concluding remarks about our proposals in Chapters 6, 7, 8 and 9. These include the problems that we have studied, the importance of these problems, and a summary of our research findings. We also provide some suggestions for future work related to our proposals.

Chapter 2

Background: Near Field Communication

Contents

This chapter gives detailed background information about a core technology used within this thesis. Near Field Communication (NFC) is introduced here, as it is included in the protocols proposed later in the work.

2.1 NFC: Near Field Communication

Near Field Communication (NFC) – is a short-range and interactive contactless signal communication interface.

As mobile phones have become indispensable in our lives, both mobile network operators and manufactures have added more features on the handset other than just making phone calls. Based on a short-range wireless connectivity, NFC is designed for **intuitive**, **simple** and **safe** interaction between electronic devices. As NFC functionality is embedded in the mobile phone, this makes many day-to-day tasks more convenient for consumers.

The following line gives an essential description of the main NFC action: "NFC communication is enabled by bringing two NFC compatible devices within a few centimeters of one another or for the two devices to literally "touch" one another." [1]. **NFC provides 3 different operating modes: Card Mode, RFID Tag Read/Write mode, and Peer to Peer Mode** (more detailed description is shown in Section 2.3). NFC-based devices offer users easy access to different services without having to carry multiple cards in their wallets. For instance, a travel card, a contactless credit card or loyalty programs can be stored in an NFC device. NFC is in the news at the time of writing because of rumors that Apple will be including the technology in the next release of the iPhone. Google is including the technology in Android and Samsung has also included it in some of its handsets.

2.2 NFC: Basics

NFC is an open-platform technology and standardised as an ISO/IEC standard by the NFC Forum [2] in 2004. At that time the forum was dominated by the world leading companies: Nokia, Sony, and Phillips. The NFC Forum now has more than 200 members including manufacturers, developers, and financial services institutions today such as NXP, Infineon, Renesas, SONY, Mastercard, Visa, and JCB.

The NFC Forum is a non-profit industry association, which has the vision of enabling users to access or pay for content and services in a secure and intuitive way anywhere, at any time, using any device. Their missions and goals are defined in [2][12] and reproduced below:

- Developing standards-based specifications that ensure interoperability among devices and services
- Encouraging the development of products using NFC Forum specifications
- Educating the market globally about NFC technology
- Ensuring that products claiming NFC capabilities comply with NFC Forum specifications
- Promoting the NFC Forum N-Mark (shown below)

NFC N-Mark:

Figure 2.1: NFC N-Mark

NFC Forum has introduced the NFC technology trademark as shown in Figure 2.1. The goal is to help users identify objects and equipments with which their NFC-enabled devices can interact. The trademark has a free licence, and is available to use on smart posters, cards, labels, and device [2]. Allowing mobile devices to **"read"** information stored in tags on everyday objects is a fundamental property of NFC technology, as is the ability to **"emulate"** conventional contactless smart cards and RFIDs used in a variety of applications such as the London underground Oyster card or access control systems.

This is possible because NFC offers a short-range, zero-configuration wireless interface that has evolved from existing contactless identification and interconnection technologies,such as Radio-Frequency Identification (RFID), which allows a reader to send radio waves to a passive electronic tag for identification and tracking. NFC operates on **13.56MHz** frequency, with a communication range of up to **10cm in active mode** and **4cm in passive mode** (please see next paragraph for definition of active and passive modes), it also supports various data transmission rates including **106Kbps, 212Kbps and 424Kbp-**

s.

An NFC-enabled mobile phone can operate in the typical RFID system power modes i.e. passive or active. In passive mode it relies on the electromagnetic field of an"active" RFID/NFC reader device to both power it and to support communications. In active mode it could act as the RFID reader for accessing passive RFIDs. Alternatively, there is an active peer-to-peer mode in NFC, whereby each device acts as a self-powered RFID that is able to generate and control its own electromagnetic field.

Table 2.1: Basic use cases in relation to different operation modes of NFC mobile devices

Mobile phone	Target: Active	Target: Passive
Initiator: Active	**Peer-to-peer mode** Exchange pictures, videos and data	**Reader/Writer mode** Smart posters, contactless tags and smart card reading applications
Passive	**Card Emulation mode** Payment and transport cards features in handsets	no communication possible

Table 2.1 shows the correlation of different power states with NFC operation modes and use cases. A more detailed explanation of communication modes is described in Section 2.3 and Figure 2.4.

Key Benefits of NFC include:

Intuitive: NFC interactions may be triggered simply by bringing a mobile

close to another device or RFID.

Versatile: NFC has a wide range of uses and applications for the benefit of users, industry and government.

Open and standards-based: NFC is defined within international standards e.g. ISO, ECMA, and ETSI.

Technology-enabling: NFC can also provide fast and simple pairing, such as required by Bluetooth, Wi-Fi, etc.

Intended to be inherently secure: NFC transmissions are meant to be short range (up to 10cm), however this is not a property that should be heavily relied upon as there are known range extension attacks on RFID systems.

Interoperable: NFC is compatible with many existing contactless card and RFID technologies.

Security-ready: Standardised NFC Secure Element to provide secure features and applications.

2.3 NFC: Specifications

In this sub-section we will map NFC functionality to a range of applicable standards and RFID tag types.

- ISO/IEC 18092, NFCIP-1 and ECMA-340

As aforementioned, NFC offers an exchange data rate up to 424Kbps, operates in 13.56MHz, its communication range is up to 10cm in active mode and 4cm in passive mode, and the response time is less than 0.1 second [14][40]. To widely promote NFC technology, Sony and Philips developed the key communication interface and protocol called *NFCIP-1*, which is acknowledged by ECMA (European Computer Manufacturers Association), ISO/IEC (International Organization for Standardization) and ETSI (European Telecommunications Standards Institute) and standardised as *ECMA-340* [3], *ISO/IEC 18092* [4] and *ETSI TS 102.190* [5] respectively.

- ISO/IEC 21481, NFCIP-2 and ECMA-352

NFC has a later Interface-Protocol standard called *NFCIP-2*, also known as *ISO/IEC 21481* and *ECMA-352* [6], that specifies a mode switching mechanism for NFC-enabled devices to detect and select communication mode. These modes are covered by three standards: *ISO/IEC 18092 (NFCIP-1)*, *ISO/IEC 14443* [7] and *ISO/IEC 15693* [9] (please see Figure 2.2). They are defined as NFC, Proximity Coupling Device (PCD) and Vicinity Coupling Device (VCD) communication modes respectively. NFC devices therefore are compatible with the above three standards as they all have the same working frequency on 13.56MHz.

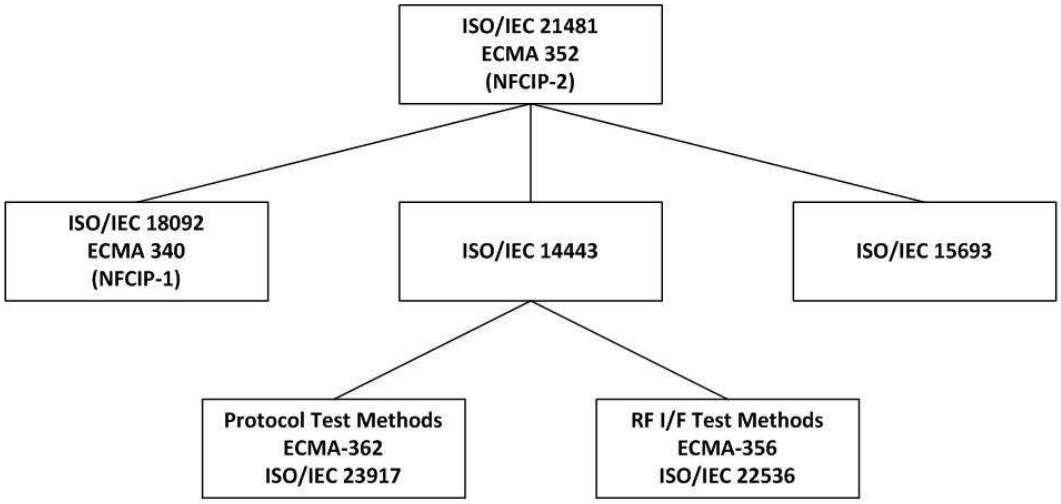


Figure 2.2: NFC related standards

The Stolpan Association (a member of the NFC Forum) stated that [11] "The NFC Forum, in addition, announced the initial set of four tag formats that all NFC Forum-compliant devices must support; these are based on ISO 18092, ISO 14443 Types A and B (the international standards for contactless smart-cards) and FeliCa [8](derived from the ISO 18092, passive communication mode, standard)". Figure 2.3 specifies procedures for NFCIP-2 devices to select/use NFC, PCD and VCD modes.

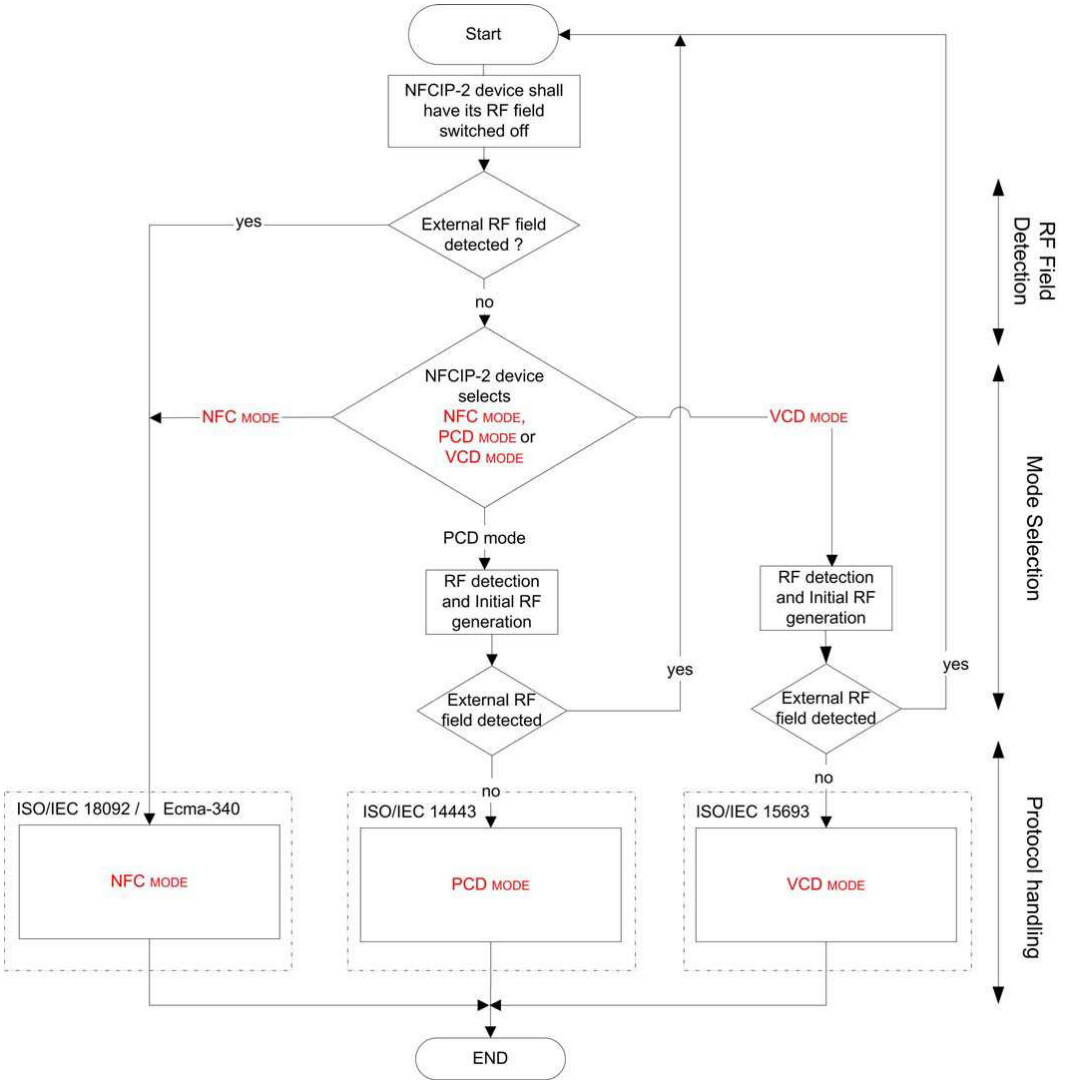


Figure 2.3: NFCIP2 mode selection [6]

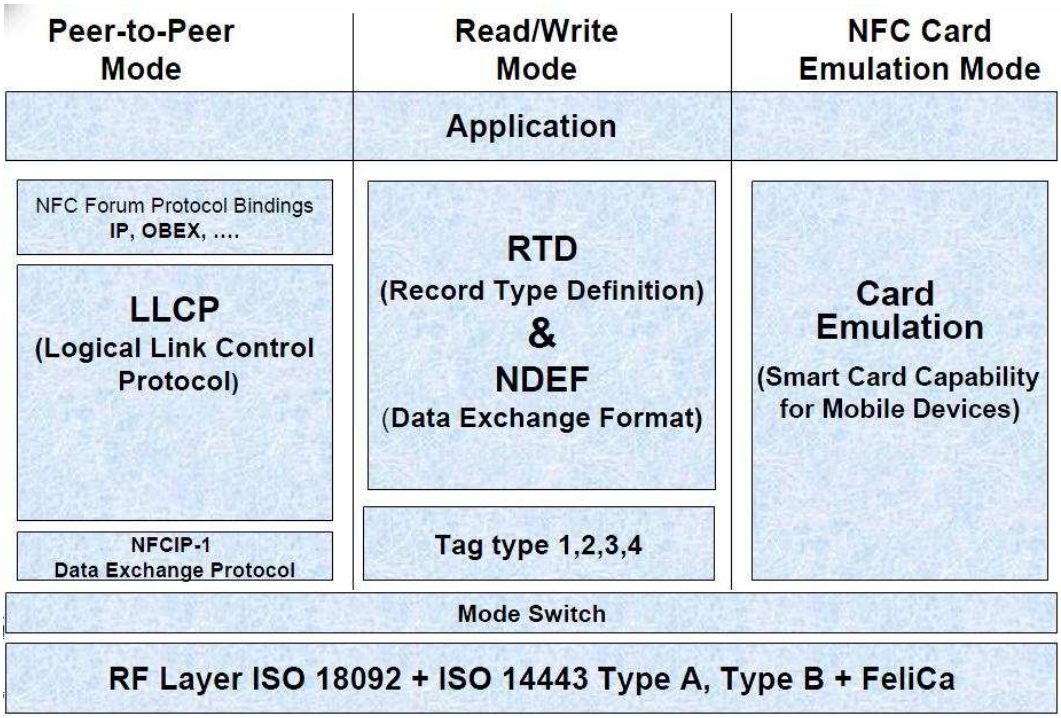


Figure 2.4: NFC communication modes [12]

NFC offers three main *Communication Modes* for various types of applications: peer-to-peer mode, card emulation mode, and reader/writer mode. Figure 2.4 shows the NFC Forum technology architecture, in which various RF layer standards are linked to the different NFC communication modes.

Peer-to-peer mode is standardised in the ISO/IEC 18092 and uses Logical Link Control Protocol (LLCP) for data exchange between two NFC devices. For example, you could use an NFC protocol to set-up the parameters for a Bluetooth or Wi-Fi link to set up parameters, and exchange data such as virtual business cards or digital photos.

A study of NFC published by Nokia Forum [13] has given a good explanation

of LLCP — "LLCP provides additional communication capabilities on top of the NFCIP-1/ ISO 18092. LLCP introduces a two-way link-level connection, allowing both peers to send and receive data, using the following methods of data exchange: Connection-oriented transfer, where the data exchanges are acknowledged. Connectionless transfer, where the data exchanges are unacknowledged."

Reader/writer mode is compliant with the ISO 14443 and FeliCa schemes. The NFC device is capable of reading NFC Forum mandated tag formats for NFC-compliant devices. The tag formats include NFC Data Exchange Format (NDEF) and NFC Record Type Definition (RTD) for smart posters [17], supporting text and Internet resource reading applications.

NDEF is a lightweight and compact binary format, which can carry URLs and vCard (Versitcard) and NFC-specific data types. RTD can vary from NFC Text RTD, NFC URI RTD, NFC Smart Poster RTD, NFC Generic Control RTD and NFC Signature RTD.[13]

(* vCard [19] is the abbreviation for Versitcard, it is an electronic business card format for the Internet. vCards are often attached to e-mail messages, but can be exchanged in other ways, such as via the World Wide Web or Instant Messaging. They can contain name and address information, phone numbers, e-mail addresses, URLs, logos, photographs, and audio clips.)

In **Card Emulation mode**, the NFC device itself acts as an NFC tag, ap-

pearing to an external reader exactly the same as a traditional contactless smart card or RFID. This enables contactless payments and e-ticketing [13] that are compatible with existing infrastructure.

	Type 1	Type 2	Type 3	Type 4
RF Interface	ISO 14443 A-2	ISO 14443 A-2	FeliCa (ISO 18092, passive communication mode at 212 kbits/sec)	ISO 14443-2
Initialization	ISO 14443 A-3	ISO 14443 A-3	FeliCa (ISO 18092, passive communication mode at 212 kbits/sec)	ISO 14443-3
Speed	106 kbits/sec	106 kbits/sec	212 kbits/sec	106-424 kbits/sec
Protocol	Specific Command set	Specific Command Set	FeliCa protocol	ISO 14443-4 ISO 7816-4 commands
Memory Size	Up to 1 KB	Up to 2 KB	Up to 1 MB	Up to 64KB
Cost (memory dependent)	Low	Low	Moderate	Moderate
Use cases	Tags with small memory for single application		Flexible tags with larger memory offering multi-application capabilities	

Figure 2.5: NFC tag specifications [12]

The NFC Forum specifies four types of compliant NFC tags (please see Figure 2.5): Types 1 and 2, based on ISO 14443A, have small memory capacity (1 and 2 kilobytes), which means they are low cost and intended for single-use applications. They operate at relatively low speed (106KB per second), and are driven by specific command sets. Type 3 is based on FeliCa, and has larger memory (up to 1MB) and higher transfer speed (212KB per second). This means it is suitable for more complex applications, but may be more costly. Type 4 is based on ISO 14443 and specifies memory of up to 64KB, with transfer speeds of between 106 and 424KB per second, making it suitable

for multiple applications. For more detailed NFC Forum tag type information please refer to [13]. Moreover, NFC technology is also compatible with MIFARE family tag types, which refers to NFC/RFID tag types developed by NXP semiconductors. MIFARE family tags are widely used and for example often deployed as electronic ticket cards in transportation applications. [13]

2.4 NFC: Mobile Architecture and Secure Element

An NFC device includes four necessary components: Host/Baseband Controller, NFC chip (modem), Secure Element (SE) and Antenna.

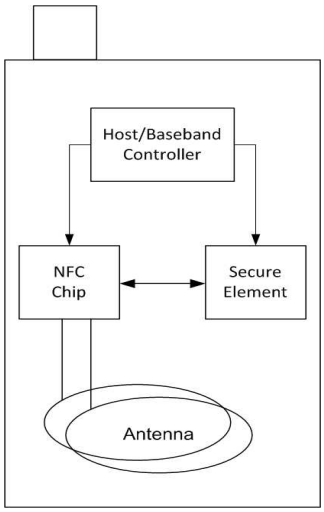


Figure 2.6: Secure element communication in NFC devices

The SE is there for a very specific and important purpose; to safeguard sensitive data and operations when the NFC phone is emulating contactless smart cards and RFIDs. For example if the phone was to emulate a bank card or identity

card it would need to safeguard cryptographic keys and personal data and resist attack in the same way as a normal bank card or identity card. Note that it does not have a direct role when using the NFC phone as a reader device in which case other means are required to secure phone application security.

2.4.1 The Secure Element

NFC technology is intended to be secure and reliable as it offers a special chip called the "Secure Element (SE)" for that purpose. A Secure Element is typically a tamper-resistant hardware platform (e.g. specialised chip with secured operating system etc) for the secure hosting of applications and sensitive data. It can be considered as an additional security-hardened computer for handling jobs like storing data credentials (such as cryptographic keys for payment applications, credit card transaction details, identity verification information etc.), running sophisticated cryptographic algorithms and being capable of hosting multiple applications.

The Secure Element has much in common with a smart card chip, and in some early NFC phones this was the "SmartMX" product from NXP Semiconductors [20][21]. It is important to note that the standards permit the use of a software based SE, however, due to the inferior attack/tamper-resistance inherent in software SEs, this report will only focus on the hardware SE options.

The following are requirements for a hardware SE: [15]

- High Security Smart Card IC platform (equivalent) required
- Crypto co-processors for fast symmetric and asymmetric crypto algorithm support e.g. Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES), RSA and Elliptic Curve Cryptography (ECC).
- Strongly tamper/attack resistant design.
- Sufficient non volatile memory for application code and data.
- Compliant to relevant international standards such as EMV96, EMV2000, EUROPAY CQM, ETSI TS 102 221, 3GPP TS 51.011, GSM 11.1x.
- Global Platform compliant to enable JavaCard operating system operations.
- Single Wire Protocol (SWP)/ Host Controller Interface (HCI) support for SIM-centric solutions.

Ever since NFC technology has been invented, mass deployment of mobile payment solutions has been hampered by the issue of where the SE should be stored (and indeed who controls it).

There are three proposed system formats for integrating the Secure Element in the mobile phone [15], as indicated in Figure 2.7:

1. Embedded in the phone (separate chip on the Printed Circuit Board (PCB)).

2. Included within the SIM card. Embedded

3. Embedded in the removable flash memory card (microSD card) that can be inserted in a phone.

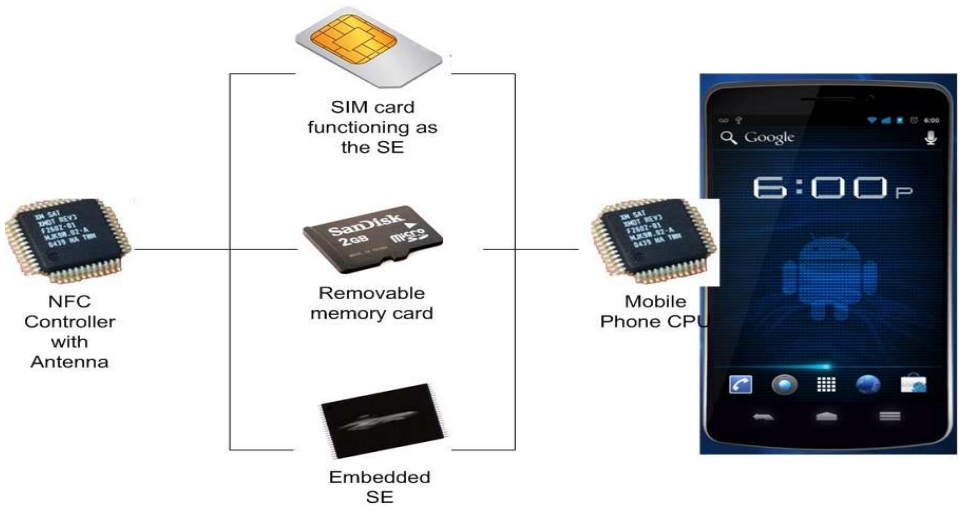


Figure 2.7: Different Secure Element (SE) solutions

There are supporters for each type of SE deployment, however it would be wrong to assume that this is because of security qualities. The different options could have enormous impact on business advantage and the general interests of a range of companies including Mobile Network Operators (MNO), phone manufacturers, operating system providers, search engine companies, content providers, developers, banks, transport companies and so on. In this report the focus is not on these business issues, but on the security and practical aspects that are likely to result in practical and usable systems for consumers

and providers.

SE:	Embedded in handset	in SIM	NFC SD card (contains NFC modem, smart card, SD controller)
Brief Summary:	SE embedded in handset, non-removable	SE & SIM features in one UICC	SE in SD Card, works on smart phones with SD card slot available so NFC feature is enabled when SD card is plugged
Location of NFC Modem:	In the phone	In the phone	In NFC SD card
Requirements:	Use phone battery	Have to use the new generation SIM	Need SD I/O....but tiny antenna, need non-metallic SD card slot and non-metallic phone back cover for better sensing ability.
Features:	NFC feasible without change to the new generation SIM	Removable SIM. Easy to swap between different phones	Removable SD card. Installing secure applications is feasible.
Existing Products:	Nokia 6131, Samsung Galaxy S2,S3	BenQ T80	Moneto SD card

Figure 2.8: Comparison of different SE placement in the phone

Figure 2.8 displays comparisons of the various hardware SE options, which will now be discussed in more detail.

Option 1: SE embedded in the phone

In this sub-section the option can be considered where a SE chip is pre-installed onto the phone PCB. This solution was one of the earliest to appear in mobile phones and to avoid confusion it is worth listing other names that have been used in the past for this approach:

- NFC-SE

- eSE (embedded SE)
- NFC-WI (Wired Interface) [10], WI is identical to S2C (SigIn-SigOut-Connection) [18]
- Basic NFC
- Or, NFC secure IC approach.

Since the SE is mounted into the phone by the handset manufacturer, this option is sometimes referred to as a "handset manufacturer - centric approach".

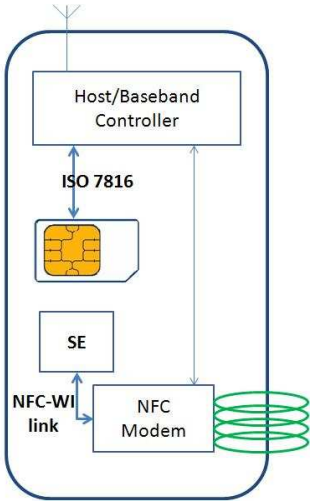


Figure 2.9: SE in the phone (handset manufacturer - centric)

The SE embedded in the phone approach was used on most of the initial trials with early handsets such as the Nokia6131. As Figure 2.9 shows, the SIM normally hosted on a Universal Integrated Circuit Card (UICC), has no direct connection to the SE. Such an architecture may be suited for devices that do not have SIMs such as PDAs or SIM-less Code Division Multiple Access

(CDMA) phones [11]. At first glance the approach has some merit as it is easy to implement, with no extra interface requirements for the UICC, however there are some disadvantages.

The ownership and management of the SE is not at all clear (which impacts key storage and management) and there are also concerns about personalisation and re-personalisation of the SE. If anyone can take ownership of the SE then it would not have the necessary security properties that are needed. If a single business entity owns the SE then there could be unnecessary restrictions that would not be advantageous to application providers and users. If a SE is eventually personalised (with very sensitive financial and identity credential) to an end-user, what happens if the phone is lost, replaced or sold to another user. The ownership issue may also be clouded by equivalent activity with Trusted Platform Modules (TPM), where it has been decided that the user owns the embedded security chip (the TPM) and has to "opt-in" to enable its use.

Based on some of these difficulties (and business interests of MNO) the SIM based option (described next) has attracted considerable support.

(2). SE embedded on the SIM card

It is also called:

- NFC-SIM or SIM-NFC
- SE-SIM

- NFC-SWP
- NFC-UICC
- Or, NFC secure UICC approach.

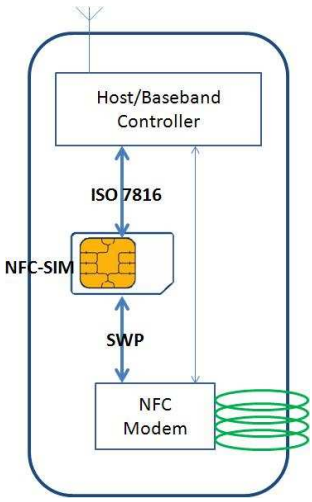


Figure 2.10: SE on the SIM (MNO-centric)

The SIM is the most widespread and successful of any security module deployment and over 6 billion are in use today (and it is expected the number of active mobile phones will reach 7.3 billion by 2014). Providing good quality tamper-resistant SIM chips are used, the SIM is a good candidate to include SE functionality as it was designed as a security processor, can be personalised and managed after deployment. These days the SIM (or the UMTS equivalent USIM) is actually an application hosted on a sophisticated multi-application UICC platform, however we will use the terms SIM and UICC interchangeably unless there is a need to highlight the difference.

Figure 2.10 represents a MNO-centric approach. As a UICC typically can

support several applications (historically it only contains a SIM), the SE functionality can be built into it as well, independently of the mobile phone, and bound to a user identity for secure and trusted transactions.

Of the various NFC SE, the SIM-SE (which represents a user-centric and/or MNO-centric approach) seems the most likely to result in a secure solution, without radically changing existing practices and roles. There are advantages such as:

- The SE can be securely personalised by the MNO either pre-issue or remotely.
- Existing and proven remote application management processes and protocols can be used. Credentials and applications can be downloaded and managed via the MNO existing Over The Air (OTA) mechanism [23], OTA is specified in 3GPP TS 23.048 "Security mechanisms for the (U)SIM application toolkit" [24].
- For users, there is a portability and control benefit as their important credentials, such as digital money, digital identity and keys, are saved in the **removable** UICC and can be easily transferred from one mobile device to another.
- The SIM/UICC has a proven track record as a tamper resistant security device.

- From the MNO perspective (bias) there is an advantage in retaining control of the customer relationship.

The main disadvantage is basically the opposite to the last advantage. Not all parties will be happy for the MNO to be in such a dominant controlling position and this may drive them towards the alternative solutions.

Whatever the perceived advantages or disadvantages, the SIM based SE will only work if the handset supports a protocol connection between the SIM and the NFC functionality; as described in Section 2.4.2.

(3). SE embedded on a removable flash card (SD card)

This option may also be referred to as:

- NFC-SD
- SD-SE
- Or, micro SD NFC chip approach.

In this architecture, the SD card hosts the applications. A single **micro SD card** could in theory be used in many different handsets. Some SD cards solutions would provide NFC functionality for phones that would otherwise not offer NFC support. There are various options for fitting an NFC-enabled SD card into a phone:

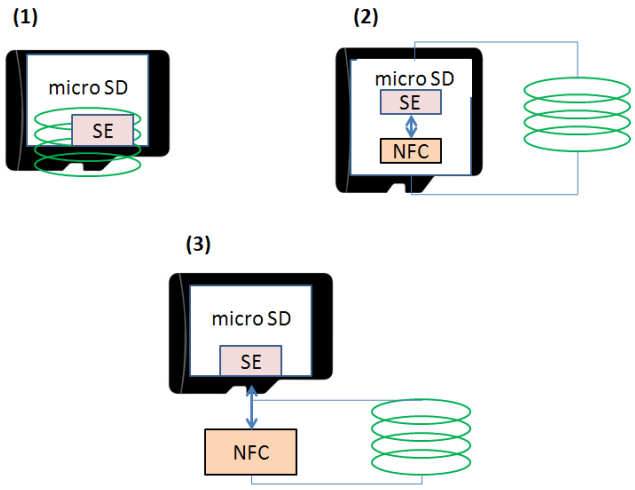


Figure 2.11: Various NFC-SD card architectures [16]

(1) (Antenna + NFC chip + SE) in SD card.

(2) Antenna attached directly to SD + (SE + NFC chip) in SD card.

(3) (Antenna + NFC chip) in phone + SE in SD card.

From the four various types of SE-SD card architecture, Type 1 is similar to existing contactless smart cards or RFIDs. For example a bank could issue SD cards to customers, which then emulate their contactless bank cards. Types 2 has the antenna attached externally to the SD card, which loses some of the advantage of independence from the phone NFC capability.

Figure 2.12: A SIM+antenna NFC solution by On Track Innovations (OTI) [31]

Type 2 has the combination of an NFC chip and antenna with a flash memory card. Moreover, a particular advantage of the Type 2 layout is that it can be an interim method to offer NFC features for non-NFC enabled handsets (this type is of similar concept as the NFC SIM+antenna solution in Figure 2.12), though the range of phones it can work with is limited. Those with a metallic SD card slot will not work; however, those with a non-metallic are compatible with the NFC SD card. A similar drawback relates to the handset: the handset's back cover cannot be built with metal either. Since the antenna is tiny, the scanning feature is difficult since the reader has a small sensing

area.

The long term and mass market viability of this approach is questionable, however there is currently significant commercial interest, for example, a type 3 like solution has been unveiled by an NFC microSD specialist company, DeviceFidelity [25], and a RFID writer/reader company, Spring Card Systems [26]. Together they released a mobile payment platform named Moneto [27] in 2012, the Moneto's microSD [28][29] provides the mobile payment solution that processes through MasterCard's PayPass system, and works on Android phones and iPhones [30] (if a microSD slot is available). This NFC on microSD product using the MasterCard PayPass may have some strategic more benefit for the banking industry, as transactions go directly into the banking/EMV system, without relying on the MNO system for transaction information.

Type 3 shows an embedded SE with NFC-WI connected to the NFC chip and antenna embedded in the phone. **Type 3** is more suitable at the stage when phones are upgraded to NFC enabled devices. Another example is Giesecke & Devrient Secure Flash Solutions has announced a trial launched in June 2012 in Taiwan by Cathay United Bank of mobile payment applications running on microSD cards in full NFC phones. A MasterCard PayPass credit application and a separate Mifare-based EasyCard e-purse are loaded onto microSDs that are inserted in a modified version of the HTC Incredible S NFC-enabled handset. The Android phone from Taiwan-based HTC is equipped with an NFC chip, antenna, and a single-wire protocol (SWP) connection to the microSD

card slot. [32]

The SWP connection between the NFC chip and microSD card slot is not yet standardised, but international standards organizations are drafting specifications to standardize a SWP link for microSDs. By using microSDs as a secure element, banks can generally bypass mobile operators to introduce NFC mobile payment on their own. [32]

Figure 2.13 displays a large layout of the likely optimum form for the embedded SE in SD card approach.

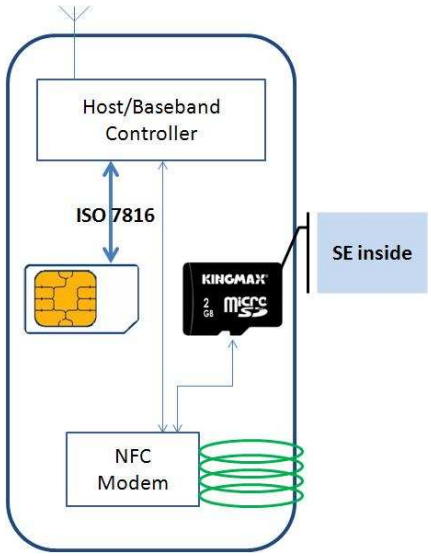


Figure 2.13: NFC-SD

2.4.2 Single Wire Protocol (SWP)

A connection interface called the Single Wire Protocol (SWP)[155] has been developed for the *NFC-SIM centric* solution, running between the UICC (SE embedded SIM) and an NFC chip (i.e. the Contactless Frontend (CLF) in the NFC modem) [11][41]. The CLF acts as the master and the UICC acts as the slave, and both of them should remain compliant with ETSI TS 102 221 "Smart Cards; UICC - Terminal interface, Physical and logical characteristics" [34]. In terms of the phone architecture, Figure 2.10, shows the SE built in the SIM is controlled by the NFC chip/modem via SWP. Lower layer protocols that support the Host Controller Interface (HCI) like the SWP are specified in TS 102 613 [33]. The SWP requires an extra physical connection with the mobile phone and Figure 2.14 and Table 2.2 show how this was arrived at.

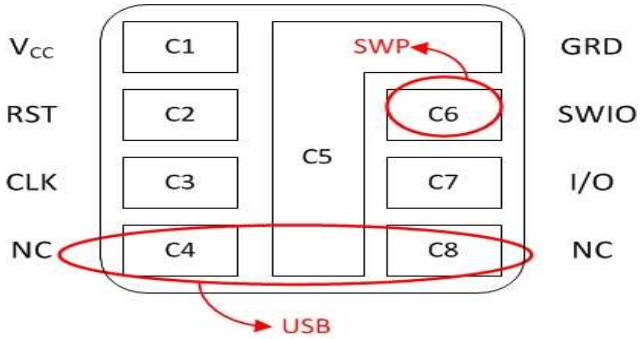


Figure 2.14: Pin contacts for the SIM

Table 2.2: The pin description for SIM card

Vcc	5V power supply
RST	Signal reset
CLK	Clock for timing signal
GND	Ground signal
SWIO	Single wire protocol input/output (former Vpp - programming voltage)
I/O	Input/output data
NC	Not connected

Table 2.2 shows description of each abbreviation of pin contacts from Figure 2.14.

Since USB [38] was adopted for high speed interface connections, using pin c4 and c8 of the SIM (and C1,C2,C3,C5,C7 are already used by SIM), the SWP was initially proposed by Gemalto [35][36] using a single wire connection via pin C6, aka SWIO [33], for the signal input and output [11][37].

2.5 NFC: Applications

This section illustrates some of the applications which are beginning to use NFC. Four basic application concepts are briefly described to highlight the versatility of NFC: Touch & Go, Touch & Confirm, Touch & Connect, and Touch & Explore [40].

Touch & Go:

This type is mainly used for access control, ticketing applications and logistics management. Users only need to carry a mobile device that saved IDs or ticket

credentials and hold it close to the corresponding reading devices. In future mobile phones may have electronic keys to open the doors of your home and office.

Touch & Confirm:

Applications falling into this category mainly cover the mobile payment mechanisms, where password input is usually required to confirm transaction actions; however, on occasion, a micro-payment transaction can be processed directly without user confirmation.

Touch & Connect:

Connect two NFC enabled devices via a peer-to-peer connection, e.g. for downloading music, exchanging data between devices.

Touch & Explore:

NFC can also be used for discovering information and the user's handset can read data out of a document or a poster. For instance, a handset can read website addresses from a smart (RFID tag embedded) poster. There is a lot of interest in this area and for further technical specifications about NFC smart posters please refer to an NFC Forum report: "Smart Poster Record Type Definition, Technical Specification" [39].

Figure 2.15: Three NFC core applications [42]

Three core applications are shown in Figure 2.15 [42][43] corresponding to the three main NFC operating modes:

- Card Emulation Mode –> Mobile payment transaction.
- Peer-to-Peer Mode –> Data transfer between devices.
- Reader Mode –> Access info on-the-move.

Table 2.3: Further classified NFC applications

Mobile Payment	Credit card
	Micro payment
	Internet m-payment
Identification	e-Ticket
	Access control
	Account Log-in
	e-Official Document
Data Exchange	Data transfer between NFC devices
	Wi-Fi/Bluetooth pairing
Information Collection	Smart Poster

Further examples for the three core applications of Figure 2.15 are listed in Table 2.3. These applications areas can be further subdivided into payment/transaction, ticketing, access control, connectivity, information download and loyalty and coupons [11]. NFC basically supports most of RFID-based applications as it is compatible to ISO1443, Felica and ISO15693. [6]

2.5.1 Use Cases

Some use cases scenarios are listed below:

- Two NFC cell phones can exchange data by just tapping them or bringing them close together. (see special case of Bluetooth pairing below).
- An NFC camera device could transfer photos to an NFC equipped computer or TV.
- An NFC equipped computer could transfer data to a mobile device.
- An NFC mobile device could be used to check out and pay at a shop cash register using a virtual wallet.
- An NFC mobile device may be used to make purchases from vending machines.
- An NFC mobile device could pay at a parking meter.
- An NFC mobile device could obtain cash from an ATM.
- An NFC mobile device could be used for a range of ticketing applications.

2.5.2 Bluetooth pairing

Figure 2.16: NFC Bluetooth pairing. [47]

A special use-case is of interest for NFC, and is referred to as Bluetooth pairing. Bluetooth is a useful means of connecting devices and peripherals without the need for wires, however there have been security problems associated with pairing devices so that they can work together.

Fortunately, NFC is based on a communication standard that specifies how two devices establish a peer to peer network in order to exchange data. NFC-enabled devices also allow the user to establish a Bluetooth [46][154] connection without the overhead of entering passkeys (shortcomings in its transport layer protocol), which greatly enhances the speed of initial set-up of links between devices. NFC and Bluetooth therefore are complimentary to each other, Bluetooth offers a medium distance connection capability (from 10m to 100m) whereas NFC offers improved security and ease of connection. Together, they support unidirectional wireless pairing for Bluetooth devices such as mice, keyboards, headphones, car dashboards and push content from your phone to

your TV. For details of how the NFC to Bluetooth connection handover is done please refer to the NFC Forum reports "Connection Handover 1.2, Technical Specification" [48] and "Bluetooth Secure Simple Pairing Using NFC, Application Document" [49].

Other application areas include: Hands-free connections (e.g. headsets) , desktop/Handheld synchronization, gaming, image printing (e.g. between printer and handset) and image sharing (e.g. between TV and handset). For further explanations of each application please see [50].

Some real life NFC Bluetooth pairing products are available commercially. Nokia released an NFC-enabled Bluetooth speaker called Nokia360 in 2011 [51]. Nintendo included NFC into their Wii U controller in 2012 [52]; the Wii U controller is set to be compatible with both FeliCa for its home audience and MIFARE for the rest of the world.

2.5.3 NFC with respect to Other Technologies

	Bluetooth	IrDA	Contactless Smartcard	NFC	WiFi	Zigbee
Data Rate:	100~480 Mbps	9.6K ~ 16Mbps	106,212, 424Kbps	106,212, 424Kbps	<600Mbps	10K ~ 250Kbps
Connection Distance:	10~100m	< 1 m	3~10cm	3~10cm	100m	10~75m
Frequency:	2.4 GHz	36 KHz	13.56 GHz	13.56 GHz	2.4 GHz	2.4 GHz
Network Type:	P-P/star, ad-hoc (Allows 8 devices share with one Piconet. Max Piconet x 10 work at the same time.)	Peer-to-Peer	Master/Slave	Master/Slave or Peer-to-Peer	One-to-Muti	One-to-Muti
International Standard:	IEEE 802.15.1X	DSRC	ISO/IEC 14443, 10536, 15693	ISO/IEC 18092, 21481	IEEE 802.11 b/g/n	IEEE 802.15.4
Security Protocol:	-	-	ISO/IEC 7816, EMV	ISO/IEC 7816, EMV	WEP, WPA, 802.11i	RFC 3610

Figure 2.17: WPAN functionalities list [12][53]

This section considers how NFC compares with other Wireless Personal Access Network (WPAN) technologies. From Figure 2.17, there are six WPAN technologies which are frequently used in our daily life. Though some of technologies may work at the same frequency or have similar data transmission distance, they are not replacements for each other. For example, Wi-Fi currently has the fastest data rate; Zigbee aims for a low power consumption and has a one-to-multi communication network. In [12][53], an NFC Forum published article indicates that individual setup times for NFC, RFID, IrDA and Bluetooth are <0.1ms, <0.1ms, ∼0.5s and ∼6s respectively. The setup time may be another good reason why NFC and Bluetooth are good partners to complement each other's innate limitations as mentioned in Section 2.5.2

2.6 NFC: Security

NFC technology should provide users with convenient access to a wide range of services and applications, however security is certainly one of the important factors which cannot be neglected, especially for mobile payment applications. For example, NFC handset users can touch and download information from a smart poster (with an NFC-enabled tag), and then they are able to access relevant websites by mobile wireless Internet connection to obtain further information or to purchase products. Products such as e-tickets can be purchased by credit card payment type over the internet, and the purchased products are then available for downloading to the user's handset after a successful payment transaction.

Confidential personal information and security credentials (e.g. cryptographic keys) are critical during mobile payment transactions, so a complete and secure system is required to prevent information and money loss during actions. *Authentication, authorisation, integrity, confidentiality, non-repudiation, and availability* - are fundamental security requirements in many NFC applications.

Common attacks and threats against RFID systems (which will be relevant to NFC) include **eavesdropping, data corruption, data modification, cloning, phishing, and man-in-the-middle attacks**. Although the short time/range over which communications is possible reduces the possibility of effective attacks, it does not ensure adequate NFC security. As a result each

NFC security issue must be addressed to ensure that it is not possible to breach it.

In the literature, E. Haselsteiner and K. Breitfuss of Philips Semiconductors [54], provides a good explanation about fundamental security and threats in NFC. Some major attacks are summarised as follow:

– **Eavesdropping:**

Though NFC works over a really short distance, as its name "near field" implies, it is not immune from security attacks. Since NFC devices communicate through "radio frequency waves", information is sent omnidirectionally in the air. An attacker can pick up and decode the transmitted signals with an antenna and radio receiver.

NFC works up to 4cm in passive mode, however, an attacker might use a large sophisticated antenna to pick up transaction signals at extended range. It is quite possible for an attacker to retrieve usable signals up to distances of up to about 1 metre away for passive signals, and about 10m for active mode signals. Further extension cannot be ruled out, but it becomes "difficult" and provides diminishing returns for the attacker.

"The only real solution to prevent eavesdropping is to use a secure channel." [55][56]. An NFC device that emulates a contactless smartcard will have similar eavesdropping risks to the conventional card. The literature [57] presents discussion of practical eavesdropping and skimming attacks against ISO 14443

tokens.

– **Data Corruption:**

This attack can be expressed as a "Denial of Service" (DoS) attack. The attacker may try to disturb the communications by sending data that blocking the channel so that the legitimate data is corrupted. For example, the fraudster could prevent a genuine card transaction feature from working. C. Mulliner [58] has stated some good points which are "DoS attacks can be used for destroying the trust between the user and the service provider". Corruption may be easily detected, although service disruption will continue if the attacker is persistent.

– **Data Modification:**

This kind of attack is when an attacker tries to send a valid-manipulated message in the correct format to the receiving phone. One solution is to establish a secure channel or at least make use of cryptographic integrity checks. [54][55]

– **Man-in-the-middle:**

The man-in-the-middle attack is when two parties need a connection but there is a malicious 3rd party in between, intercepting and able to modify messages as they pass through to the legitimate parties. The 3rd party modifications must are achieved without the two original parties being aware of them. The solution to prevent this attack is for the legitimate parties to use a mutual

authentication protocol. [54][55][56]

– **Smart Poster URL Spoofing Attacks:**

Tokens and tags that are interactive with NFC phones also can have important security issue, C. Mulliner [58] has stated malicious smart poster with false URL (Uniform Resource Locator), in corresponse with a correct title of the service provider, can mislead users to the wrong URL. A NFC tag is placed on the smart poster, its content can be read by an NFC-enabled handset. A low tamper-resistance tags can be spoofed and replaced to the attacker's URL address. For example [58],

Title: XYZ V Bank.

https://www.XYXbank.com

URL: http://www.attackersite.com

On most occasions users only check the correctness of the title, not the URL, therefore, phishing attack can be easily triggered if the browser is misdirected to the attacker's website.[58]

Chapter 3

Background: GSM and 3G

Contents

This chapter gives background information on the mobile technologies used within this thesis. In particular the Global System for Mobile Communications (GSM) and Third Generation Mobile Communications (3G) are introduced here, as they are used within the protocols proposed later in the work. The focus and depth of description is only intended for understanding of the later chapters and so for a more detailed review of GSM the reader is referred to [64]

3.1 Global System for Mobile Communications: GSM

The Global System for Mobile Communications (GSM) is one of the legacy technologies re-used for the proposed m-payment scheme in Chapter 6. The inherited security features help to protect sensitive information and functionality.

GSM was developed by the Group Special Mobile (GSM), which was founded in 1982 to develop a European standard for digital voice telephony, and the associated specifications were standardised by the European Telecommunication Standards Institute (ETSI). Phase 1 standard was first released in 1990 and the first GSM phone call was made in 1991 on the Radiolinja network in Finland. GSM was primarily designed as a circuit-switched system for voice call, however the standards have evolved to include the Short Messaging Service (SMS), FAX, data calls and packet data transmission e.g. General Packet

Radio Service (GPRS) [65]. GSM works flexibly in many spectra because it is a combination of Frequency Division Multiple Access (FDMA) and Time Division Multiple Access (TDMA). The FDMA part divides 25 MHz of spectrum into 124 carrier frequencies spaced 200 kHz apart. Each 200 kHz channel is then divided into eight time slots using TDMA procedures. The systems success is based on each user being able to be synchronized into its frequency/time slot. GSM operates in the 900MHz and 1.8GHz bands in Europe and the 1.9GHz and 850MHz bands in the US.[59][64]

3.1.1 GSM Architecture

A GSM network consists of several functional entities that can be grouped into four broad parts:
`Mobile Station(MS), Base Station Subsystem (BSS), Network Switching Subsystem (NSS) and Operation Support Subsystem (OSS)` [60][64].

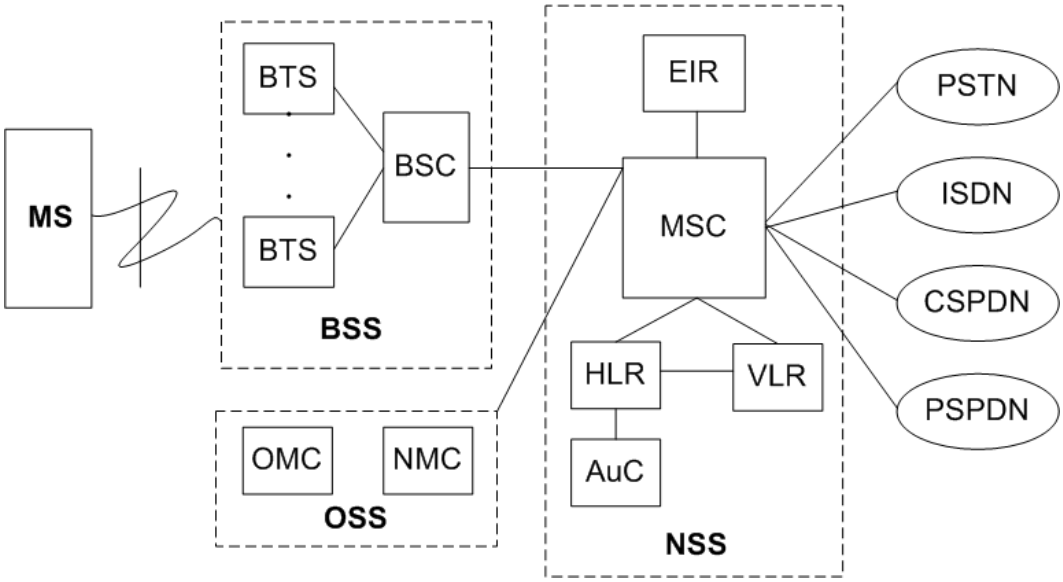


Figure 3.1: GSM Architecture

MS :– This consists of the Subscriber Identity Module (SIM) and the Mobile Equipment (ME).

BSS :– This is usually composed of a large number of Base Transceiver Stations (BTS), connected via a smaller number of Base Station Controllers (BSC).

NSS :– This includes Mobile Switching Centre (MSC), the Authentication Centre (AuC), the Home Location Register (HLR), Visitor Location Registers (VLR) and the Equipment Identity Register (EIR).

OSS :– This represents the Operations and Maintenance Center (OMC).

To summarise, in a GSM system the user's mobile phone with the plugged in SIM is called the Mobile Station (MS). A cell is formed by the coverage area

of a Base Transceiver Station (BTS) which serves the MS in its coverage area. Several BTS together are controlled by one Base Station Controller (BSC). The BTS and BSC together form Base Station Subsystem (BSS). The combined call traffic of the mobile stations in their respective cells is routed through a switch called the Mobile Switching Center (MSC). Connections originating or terminating from external telephone (PSTN) are handled by a dedicated gateway Gateway Mobile Switching Center (GMSC) [64]. Packet data is routed via Serving GPRS Support Nodes (SGSN) and connected to the Internet (or other networks) via a Gateway GPRS Support Node (GGSN). SMS traffic is also handled differently, being routed via an SMS Switching Centre (SMSC).

In addition to the above entities several databases/servers are used for the purpose of MS authentication, call control and network management. These databases include the HLR, VLRs, the AuC, and the EIR.

The HLR holds an entry for each SIM that is permitted to access the MNO's network and it keeps track of the mobile's location with respect to VLRs. A VLR handles the mobiles within its geographic area of responsibility. It communicates with the HLR for the purposes of authenticating mobiles (actually the SIMs) and advising the HLR of the mobile location. The AuC (which may actually be implemented within the HLR) typically stores the authentication credentials of the legitimate users (such as cryptographic keys, PINs IDs etc.) and computes cryptographic results used for the authentication process. The users are identified by the International Module Subscriber Identity ($IMSI$)

which is stored in the Subscriber Identity Module (SIM) of the user.[60][64]

The EIR stores data (e.g. phone serial numbers) about MEs and can be used to prevent calls from stolen equipment [60][64]. This is feasible because all the mobile equipments in GSM system should be assigned a unique ID called the International Mobile Equipment Identity ($IMEI$)), a copy of which is stored in the EIR. Unfortunately the IMEI is not always correctly programmed or may sometimes be modified by a third party, and so it is not such a strong identifier as the IMSI.

3.1.2 GSM Security

GSM security is primarily based around authentication of the SIM card associated with a registered IMSI, in a manner which does not rely on the security of the ME. The latter point is very important as historically the security attack resistance of ME devices has been very poor. A by-product of the authentication is the establishment of session keys for the encryption/decryption of transmission data between the ME and the serving BTS. As authentication is a fairly regular and localised activity, the location area identity (LAI) gives a very rough idea of where the SIM was when it authenticated.

The IMSI is the primary subscriber identity within the GSM system and a copy is stored in the SIM. For privacy/eavesdropping reasons the IMSI is rarely transmitted, but rather a temporary version (TMSI) is used instead. The MNO keeps a mapping of IMSI/TMSI to the users normal telephone number

(MSISDN) so calls can be routed via other networks such as the PSTN.

A brief explanation of the authentication and ciphering in the GSM system will be given here and for a more detailed explanation please see [153][156][157][71][158]. In GSM the Authentication Centre (AuC) holds the authentication algorithm ($A3$) and the cipher key generation algorithm ($A8$) as well as a copy of all the subscribers' International Subscriber Mobile Identities ($IMSI$) and associated secret keys (K_i). The SIM of a subscriber contains the same algorithms and one $IMSI/K_i$ pair. Therefore, given a random challenge ($RAND$) the AuC and a particular SIM can both generate an authentication result ($SRES$) and a session/cipher key (K_c). Network authentication is normally a test that the AuC and SIM results are the same and thereafter the cipher key is used for encryption/decryption via the A5 algorithm that exists in the handset (not SIM) and in the network. An overview of the GSM security process is shown in Figure 3.2. [62][64]

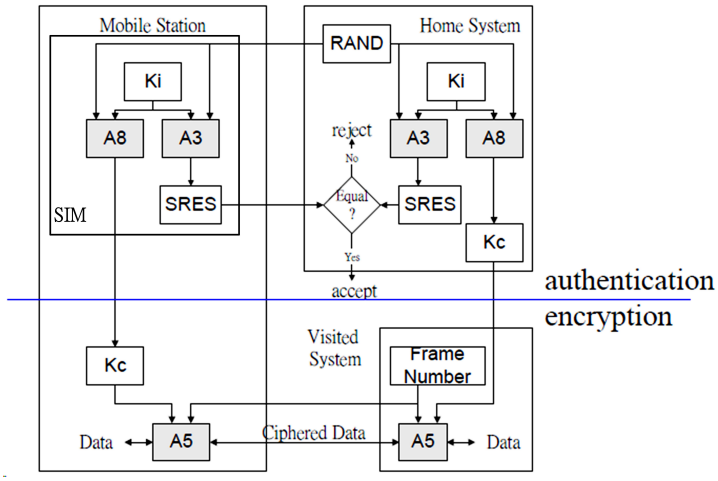


Figure 3.2: GSM Authentication and Encryption

Note that a MS is challenged via the local VLR and not the HLR, so in practice the VLR obtains authentication triplets (RAND, RES, Kc) from the HLR/AuC in order to authenticate the SIM. Note that the actual algorithms A3, A8 are not standardised (only their interface), but of course the AuC and SIM must use the same algorithms. [60]

3.1.3 GSM Security Weakness

The AuC and SIM in GSM have done a pretty good job of securing the numerous communications networks over many years, however the system does have some well known security limitations, as discussed below.

Information securiy best practice suggest that two parties in a security protocol should mutually authenticate each other, however in GSM only the SIM is authenticated to the network and not vice versa. This creates a vulnerability that may be exploited by a false BTS attack (man-in-the-middle attack)

[69][70]. Such an attack may be exploited to eavesdrop transmissions, insert false messages or to seize radio resources.

A related problem is the lack of integrity protection and replay detection for the authentication challenges. It is sometimes mistakenly reported that the GSM authentication algorithm (A3) is weak, due to successful attacks on the algorithm known as COMP128-1 [66]. However ETSI did not standardise an algorithm and COMP128-1 was just an example, so many networks opted for their own designs, Whether the network algorithms are better is hard to tell as it was quite normal to keep them secret rather than adopt publicly evaluated designs as would be expected nowadays. We do know that the secret keysize of 128 bits is still acceptable via today's best practice recommendations. Ciphering could present more of a problem as Kc is a maximum of only 64 bits [73][63] and the phone based algorithm (A5) has been subject to attacks [67][68]. The value of such attacks may be questionable as Kc is only a session key which is changed regularly.

3.2 Third Generation Mobile Communications: 3G

The ideas developed and presented within this thesis cannot be restricted to GSM as mobile technology is evolving and GSM exists alongside solutions known as Third Generation Communications (3G). In fact this wireless t-elecommunication technology is the basis of one of the proposed NFC mobile payment systems in Chapter 7, in which the security improvements of 3G (over GSM), benefit the proposed solution. Brief explanations of 3G, and its standardisation and security are given in this chapter.

3.2.1 3G Introduction

The market driver for 3G was really to provide a faster and more flexible mobile communications solution than GSM could offer and it used new bandwidth allocations and "spread spectrum" technology called Code Division Multiple Access (CDMA) to achieve this. CDMA allows many users to occupy the same time and frequency allocations in a given bandwidth and there are three major 3G systems currently in use: W-CDMA, CDMA-2000, and TD-SCDMA.

W-CDMA: Wideband Code Division Multiple Access

CDMA-2000: Code Division Multiple Access - 2000

TD-SCDMA: Time Division Synchronous Code Division Multiple Access

3.2.1.1 W-CDMA

The W-CDMA specification has been created in 3GPP (the 3rd Generation Partnership Project) [75], although some of the original work was completed by ETSI. Within 3GPP, W-CDMA is called the Universal Terrestrial Radio Access (UTRA) and there are both Frequency Division Duplex (FDD) and Time Division Duplex (TDD) modes in 3GPP Technical Specifications 25.101 [76] and 25.102 [77] respectively [78].

W-CDMA was originally designed to support (at least theoretically) a data rate of up to 2 Mbps. The input signals are digitized and transmitted in coded, spread-spectrum mode over abroad range of frequencies using 5 MHz-wide spaced carriers.

In Europe, the European Telecommunications Standard Institute (ETSI) defined W-CDMA as part of the **Universal Mobile Telecommunications System (UMTS)** in 1998 [102], which was intended as the compatible successor to GSM. This offered an easy upgrade from the GSM systems and less costs for replacing the infrastructure [79]. In this thesis we focus on the UMTS/W-CDMA evolution of GSM as our target 3G solution, however the other solutions are mentioned briefly as compatibility in other major areas such as China and the USA may be of relevance to future work.

3.2.1.2 CDMA-2000

CDMA technology transmits streams of bits in channels which are divided using codes. CDMA-2000 is a code-division multiple access (CDMA) version of the IMT-2000 standard developed by the International Telecommunication Union (ITU) based on the evolution of the second-generation (2G) IS-95, (CDMA-One), standard, which was a regional competitor/alternative to GSM. The CDMA2000 radio interface has much in common with W-CDMA and also had a target data rate of up to 2Mbps. However its specification was developed by a different body i.e. the Third Generation Partnership Project 2 (3GPP2) [82], a partnership consisting of five telecommunications standards bodies: ARIB[1] and TTC[2] (Japan), CWTS[3] (China), TTA[4] (Korea) and TIA[5] (USA). [80][81]

3.2.1.3 TD-SCDMA

Time Division Synchronous CDMA (TD-SCDMA) was developed by the Chinese Academy of Telecommunications Technology (CATT) and Siemens, originally proposed by the China Wireless Telecommunication Standards group (CWTS), approved by the ITU in May 2000, commercialised in 2009 and is only offered in China [83]. A similar technology was presented to ETSI

[1]ARIB: Association of Radio Industries and Businesses
[2]TTC: Telecommunication Technology Committee
[3]CWTS: China Wireless Telecommunication Standard group
[4]TTA: Telecommunications Technology Association
[5]TIA: Telecommunications Industry Association

as a candidate wireless technology, for UMTS although it was effectively rejected in favour of W-CDMA for main stream (FDD) use. However usage in TDD modes was standardised.

"TD-SCDMA combines an advanced TDMA (Time Domain Multiple Access) / TDD (Time Domain Duplex) system with an adaptive CDMA component operating in a synchronous mode" is quoted from [85].

The word "*synchronous*" means that uplink signals are synchronized at the base station receiver, achieved by continuous timing adjustments. Interference is reduced between users of the same timeslot using different codes, therefore increasing system capacity, at the cost of some hardware complexity in achieving uplink synchronization. [84]

At the technical level, TD-SCDMA transmits uplink traffic (traffic from the mobile terminal to the base station) and downlink traffic (traffic from the base station to the terminal) in the same frame in different time slots. That means that the uplink and downlink spectrum is assigned flexibly, dependent on the type of information being transmitted. When asymmetrical data like e-mail and internet are transmitted from the base station, more time slots are used for downlink than for uplink. A symmetrical split in the uplink and downlink takes place with symmetrical services like telephony.

In real time applications, such as voice, the system uses Circuit-Switched (C-S) transmission, whereas non real-time applications, such as email, require

Packet-Switched (PS) transmission, both CS and PS transmissions provide data rates up to 2Mbps. [83][85]

3.2.2 3G(UMTS) System Architecture

As the 3G system architcture model for use in this report we will focus on UMTS which includes the following components:

Base Station (Node B), Radio Network Controller (RNC), Home Location Register (HLR), Visitor Location Register (VLR), Mobile Services Switching Centre (MSC), Gateway MSC (GMSC), Serving GPRS Support Node (SGSN), Gateway GPRS Support Node (GGSN), Authentication Centre (AuC), Mobile Station (MS), Universal SIM (USIM), Mobile Equipment (ME) [78]. Many of the nodes sound similar to those in GSM and indeed evolution and compatibility with GSM were important considerations for standardisation.

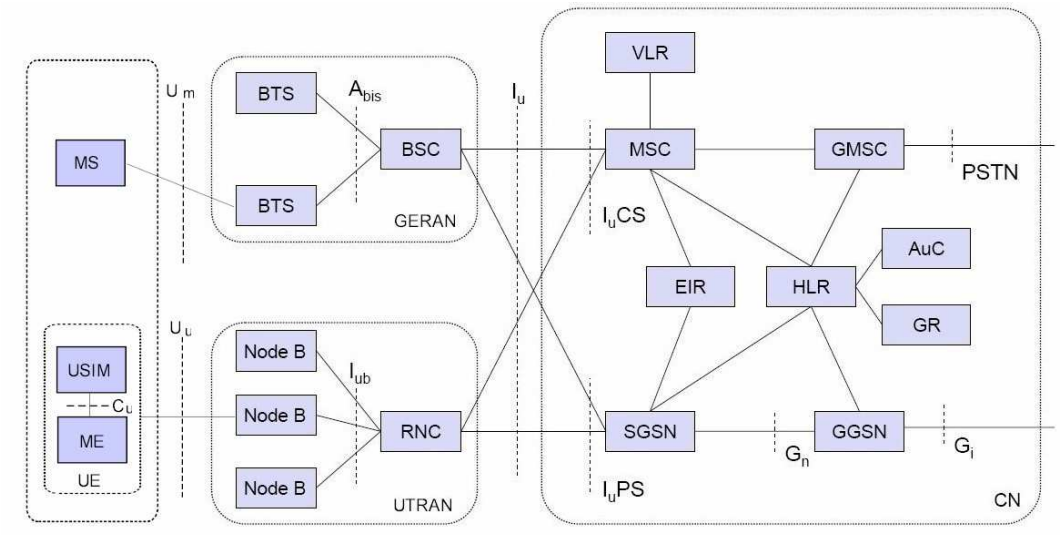


Figure 3.3: UMTS Architecture [103]

3.2.3 3G Security

In this section we will give a brief description 3G system security and for more detail treatment please refer to [87][89][74]. In general, 3G authentication and encryption security follows a similar methodology to GSM, however with enhanced security properties. This evolutionary approach helps to ensure compatibility with GSM in order to ease inter-working and handover, yet ensures that 3G systems do not suffer from the most significant security weaknesses of GSM.

There are several potential *security weaknesses* that have been identified within GSM networks, such as: Active Attacks, Key Transmission, Limited Encryption Scope, Channel Hijack, Implicit Data Integrity, Unilateral Authentication, Weak Encryption Algorithms, Unsecured Terminal, Lawful Interception and Fraud, Lack of Visibility, and Inflexibility. For further explanation please refer to [87][88][89][90][91].

In general,the main security improvements of the 3G standards compared to GSM are: Mutual authentication of SIM and Network. Longer cipher key (128 bit) [95]. Authentication replay protection.

In providing these improvements a new example authentication algorithm was developed known as MILENAGE. A very important shift from GSM practices was that the algorithm was published and subject to open expert review before it was proposed for use. This means that many networks adopt MILENAGE

rather than using proprietary algorithms. Another related improvement arises from the use of the KASUMI algorithn [97][98] for data ciphering (and integrity protection) instead of the aging GSM A5/1 algorithm.

3.2.3.1 KASUMI

KASUMI is one of 3GPP confidentiality and integrity algorithms, which applies a 64-bit block with an 128-bit key. The process of KASUMI has eight rounds of Feistel ciphers. Each round requires 32-bit input corresponding with 32-bit output. KASUMI is not utilised in the proposed system architectures within this thesis, therefore for detailed explanation please refer to 3GPP T-S35.202 [98].

3.2.3.2 Authentication and Key Arrangement (AKA) and MILENAGE

- An overview of the 3G authentication process in AuC is shown in Figure 3.4

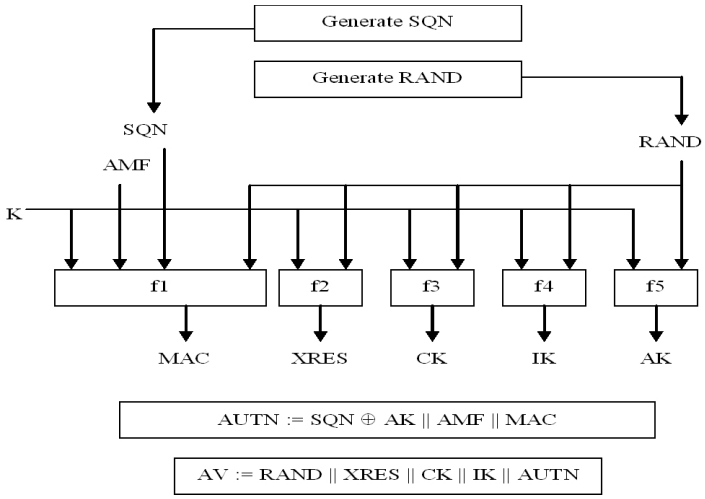


Figure 3.4: 3G generation of authentication data at AuC/HLR [97]

- An overview of the 3G authentication process in USIM is shown in Figure 3.5

In this section the Authentication and Key Arrangement (AKA) is given detailed explanation, because AKA has an important role in the proposed system protocols in chapter 7.

An overview of 3G authentication and key arrangement process is shown in Figure 3.6.

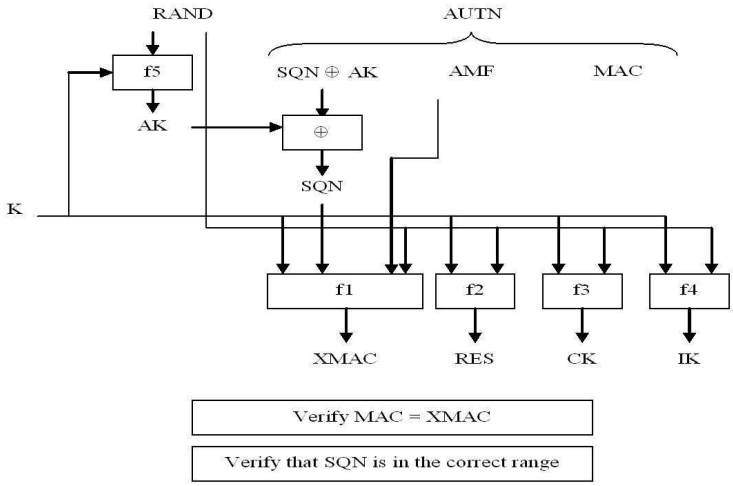


Figure 3.5: 3G generation of authentication data at USIM [97]

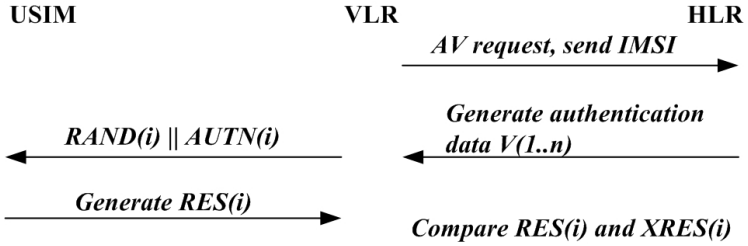


Figure 3.6: 3G Authentication and Key Arrangement (AKA) Process

The 3G system uses a challenge-response authentication mechanism for mutual authentication, referred to as "Authentication and Key Agreement (AKA)", during which the user and network authenticate each other. The **Authentication Vectors (AV)** is similar in concept to the security triplets in the GSM system [72] in that these can be retrieved early by the VLR (several can be retrieved at the same time) and they are used in the agreement of the cipher and integrity keys (CK, IK). Note that CK and IK are temporal so equivalent to session keys.

– UMTS uses the following AKA variables and functions [102]:

K = is the long-term 128-bit shared secret key between the USIM and AuC

RAND = random challenge generated by AuC

SQN = sequence number

XRES = $f2_k(RAND)$ = Expected user response computed by AuC

CK = $f3_k(RAND)$ = Cipher Key

IK = $f4_k(RAND)$ = Integrity key

AK = $f5_k(RAND)$ = Anonymity Key

AMF = Authentication Management Field

MAC = $f1_k(SQN||RAND||AMF)$ = Message Authentication Code

AUTN= $SQN \bigoplus AK||AMF||MAC$ = Network Authentication Token

AV = $RAND||XRES||CK||IK||AUTN$ = Authentication Vector

f1 = Message Authentication Function used to calculate Message Authentication Code (MAC).

f2 = Message Authentication Function used to calculate RES and $XRES$.

f3 = Key generating function used to compute CK.

f4 = Key generating function used to compute IK.

f5 = Key generating function used to compute AK.

Parameters in AKA process such as $K, RAND, CK, IK, AUTN$ are in 128 bits; RES is usually in between 32-128 bits. Other parameters within $AUTN$

like $SQN, AMF, and MAC$ have data block as 48 bits, 16 bits, and 64 bits respectively.

During the AKA, the mobile phone starts by sending $IMSI$ or $TMSI$ to the VLR for subscriber identification. From the received $IMSI/\ TMSI$, the HLR/AuC finds the associated subscriber's permanent secret key (K). The AuC generates the appropriate SQN [90], $RAND$ and AMF [94]. All these three parameters along with K are used with MILENAGE: f1-f5 to generate the MAC, the $XRES$, CK, IK and AK for use by the VLR. The VLR sends $RAND$ and $AUTN$ to the USIM via the ME, which uses them to go through the same MILENAGE functions to generate $XMAC$, RES, CK, IK, AK.

The USIM compares both the generated and received MAC to check the validity of the message sent from the MNO to authenticate the network challenge. If the MAC is valid then it is checked that the SQN is within the allowed range, in order to prevent replay attacks. If both checks pass the USIM sends RES back to the VLR where it is compared with $XRES$ in order to complete the subscriber authentication. After all the above steps are completed both the MS and the network have copies of CK and IK so can support ciphering and integrity protection.

Chapter 4

Background: The Citizen Digital Certificate

Contents

This chapter provides some basic background information about the Citizen Digital Certificate (CDC) system and the related technology, including Public Key Infrastructure (PKI), which is used later on in the thesis in Chapter 8. The CDC is of interest because it provides a strong binding to user identity, in contrast to some mobile transactions that are based on a strong binding to an account or ID, but not necessarily the real and legitimate user.

4.1 Introduction

Public Key Infrastructure (PKI) is known for offering good authentication, authorisation, integrity, privacy and non-repudiation, with practical key management. The Taiwanese governmental PKI (GPKI) system effectively supports and provides the Citizen Digital Certificate (CDC) card; equivalent to, Natural Person Certificate (NPC) card [104]. This is a national card (government endorsed) designed for representing the citizen digitally on the Internet by presenting the citizen's digital certificate, offering a digital signature signing feature for transactions with governmental PKI-enabled applications and websites. The system is intended to be secure and efficient to realise a paperless environment. The background to PKI and CDC are presented in the following sections.

4.2 Public Key Infrastructure

There are two fundamental categories for encryption algorithms:

- **Symmetric algorithm**: the same secret-key is used for both encryption and decryption, e.g the Data Encryption Standard (DES) and Advanced Encryption Standard (AES)
- **Asymmetric algorithm**: different keys are used for encryption (public key) and decryption (private key) e.g. Rivest, Shamir, and Adelman

Signatures (RSA) [105].

Symmetric algorithms are fast simple and widespread, however as the same secret key is used for encryption and decryption, there is a significant key distribution problem, especially for systems with many users.

One of the most popular public key cryptographic (or key generation) algorithms is called RSA. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described it in 1977. The algorithm is based on the fact that it is extremely difficult to factorise the product of two prime numbers. A secret key can be generated by two selected large prime numbers. The product of the two large prime numbers are used as the public key, moreover, knowledge of the public key does not allow one to easily derive the associated private key.

RSA performs the generation of a public/private key pair as follows: [117]

> Two large primes, p and q are used to compute their product n = pq, where n is called the modulus. A number is chosen, e, which is less than n and relatively prime to (p-1)(q-1), which means e and (p-1)(q-1) have no common factors except 1. Another number is chosen, d, such that (ed - 1) is divisible by (p-1)(q-1). This is the inverse of e and means that ed = 1 mod (p-1)(q-1). The values e and d are called the public and private exponents, respectively. The public key is the pair (n, e) and the private key is (d). [117]

RSA encipherment is performed as follows: [117]

$$c = m^e \, mod \, n$$

> Where m is the message to be enciphered and c is the resultant ciphertext. The specific operation performed is the exponentiation of $c = m^e \, mod \, n$, where e and n are the public key of the recipient of the ciphertext. The recovery of the ciphertext by the recipient occurs as follows:
>
> $$m = c^d \, mod \, n$$
>
> The specific operation performed is the exponentiation of $m = c^d \, mod \, n$, where d and n are the recipients private key. [117]

Distribution of public keys is therefore much easier than for symmetric secret keys, however the public keys need to be certified so they can be verified as genuine. Although asymmetric algorithms can be used for encryption/decryption they are often used to provide digital signatures, as described next.

4.2.1 Digital signatures

It is not very practical to carry out a complex cryptographic process on a large input message or data file and so the first stage in a digital signature

process is to create a smaller data field with special properties that make it representative of the original input.

A one-way cryptographic hash function takes an arbitrary length input message and produces a fixed-length, pseudo random output called a hash. It is computationally difficult to find a message that produced that hash *(pre-image resistance)*, or to find different messages that will generate the same hash (collision resistance).

Hash functions can be divided into unkeyed and keyed types. In the former case there is no secret key shared between the communicating parties, and legacy examples include, the *Message Digest 5* (MD5) and the *Secure Hash Algorithm* (SHA-1). An example of a keyed hash is the Hash Message Authentication Code (HMAC) [106][107].

For digital signatures we are interested in the unkeyed hash type which computes a fixed output (message digest) size regardless of the size of the input message/file. The actual message digest size is algorithm dependent. For example, *Message Digest 5* (MD5) [108][109], SHA-1 [110][111] and SHA-256 [113] produce message digest sizes of 128, 160 and 256 bits respectively.

The sender sends the original message and the message digest together to the destination, and any changes to the original message will result in a different message digest.

*Note that *MD5* is today considered compromised and *SHA-1* is no longer

recommended for new systems. The *SHA-256* algorithm is compliant with current best-practice guidelines.

Digital signatures are used for *authentication* and *non-repudiation* as well as *data integrity* checking. By comparing the digital signature with the original message it should be possible to see that the message has not been changed and that it has been signed using a particular private key that can be verified as belonging to the legitimate signatory.

Messages digests (hashed data) alone are useful for integrity checks, but do not provide all the security features of a digital signature. By using public-key cryptography and having the message digest signed, we have a signature that can be verified by the corresponding public key (providing it can be verified as authentic).

Note that this is a simplistic treatment of digital signatures and the reader may wish to refer to the Digital Signature Standard (DSS) that specifies a Digital Signature Algorithm (DSA) for computing digital signatures. This was proposed in Federal Information Processing Standards Publications (FIPS PUB) 186 by the National Institute of Standards and Technology (NIST) in August 1991. DSS uses SHA-1 with the standard DSA [115], but the stronger SHA-2 hash functions are approved for use in the current DSS [112].

4.2.2 PKI Framework

The purpose of a PKI framework is to enable and support the secured exchange of data, credentials, and value (such as monetary instruments) in various environments that are typically insecure, such as the Internet [117]. PKI uses certificates to bind a user identity to a public key. The certificates are documents containing the public key and some identification, such as a name of the user it belongs to, or the domain name in case of a server certificate, and a digital signature. The signature is made by a trusted third party is known as a Certificate Authority (CA) that should have done some checking to see that the claimed user identity is genuine. This way if you trust the CA who signed the certificate and you verify the certificate you also have trust that the public key belongs to the user identified in the certificate. Because the certificate is signed you dont need to have it in advance to be sure it has not been tampered with, and so you can access it when you need to, for instance from a key-server or even via an insecure connection with the user that you wish to communicate with. [116][117][118][119]

A PKI is commonly based on the establishment of the *Certification Authority Hierarchy*, this hierarchy system is a chain of trust, consisted of different layers of CAs. The highest level authority is called the root authority and is at the top of the PKI pyramid. The root CA needs unquestionable acceptance as there is no higher authority capable of confirming its certificate, which is therefore normally self-signed.

4.2 Public Key Infrastructure

A CA is a trusted entity that issues digital certificates and optionally public-private key pairs. The role of the CA is linked to that of the Registration Authority (RA). The RA should operate a rigorous registration process so that the captured identity information (relied on by the CA) is strongly bound to the legitimate user. To simplify description we will assumes that the RA duties are combined with those of the CA.

The main operational functions of the CA are: To verifies the identity of certificate requestors, to issue signed digital certificates, to maintain a Certificate Revocation List (CRL) [117]. Please see Figure 4.1 for clear layout of the CA hierarchy (note "E" stands for Entity in Figure 4.1).

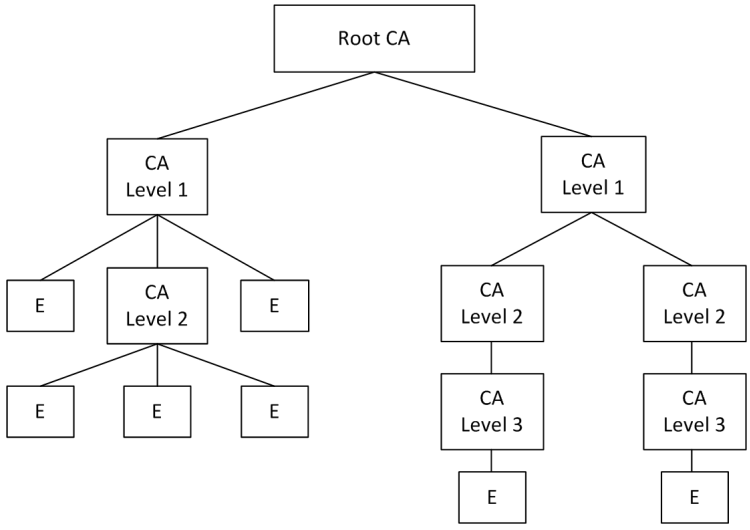


Figure 4.1: PKI Hierarchy

4.2.2.1 X.509 Public Key Certificates

In short, a certificate binds an identity to a public key. Digital certificates allow a message recipient to verify the sender's signature using the public key in the sender's certificate. A digital certificate needs some way to get the public-key of the correspondent in a trusted manner, either by directly swapping public keys, or using a trusted 3rd party the CA. The certificate requires authentication and integrity check before issuing, however it may alter expire or be revoked and so the certificate validity should be checked before use.

The most widely used format for digital certificates is the Internet Engineering Task Force (IETF) X.509. A detailed semantic profile of X.509 based public key certificates can be found in the IETF RFC[1] 3280 [117]. X.509 certificates contain several required and optional attributes that enable the identification of the subject.

Some of the attributes required in an X.509 certificate are listed in Table 4.1 and the layout of general X.509 certificate is shown in Figure 4.2 : [123]

[1]Request for Comments

Table 4.1: X.509 certificate attributes [120]

Version number	The certificate version
Serial number	A unique identifier for the certificate.
Signature algorithm ID	The algorithm used to create the digital signature.
Issuer name	The name of the certificate issuer.
Validity	The period during which the certificate is valid. (e.g. one year.)
Subject name	The name of the subject represented by the certificate. (e.g. a person, an organization, or a Web/application server.)
Subject public key information	The public key algorithm.
Issuer unique identifier	The identifier for the issuer.
Subject unique identifier	The identifier for the subject.
Extensions	Extensions that can be used to store additional information. Such as KeyUsage or AlternativeNames.
Signature: Signed hash of the certificate data	The hash of the preceding fields encrypted using the issuer's private key, which results in a digital signature.

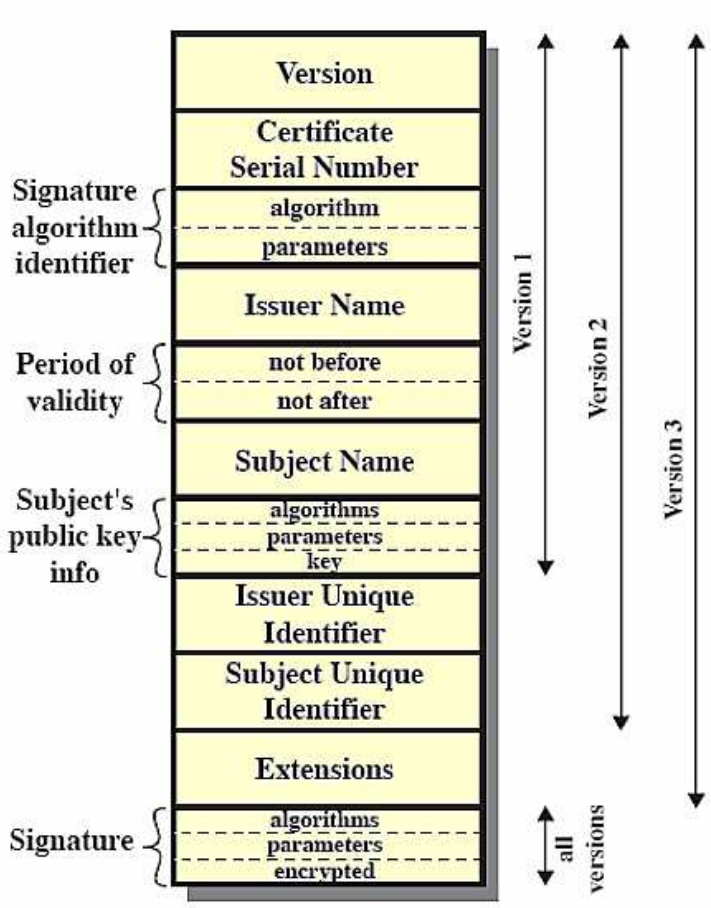


Figure 4.2: X.509 Certificate [120]

An example of a test Taiwan MOICA certificate with a RSA 1024Bits public key is displayed in Figure 4.34.4. And the complete value description of each field are listed in Table 4.2.

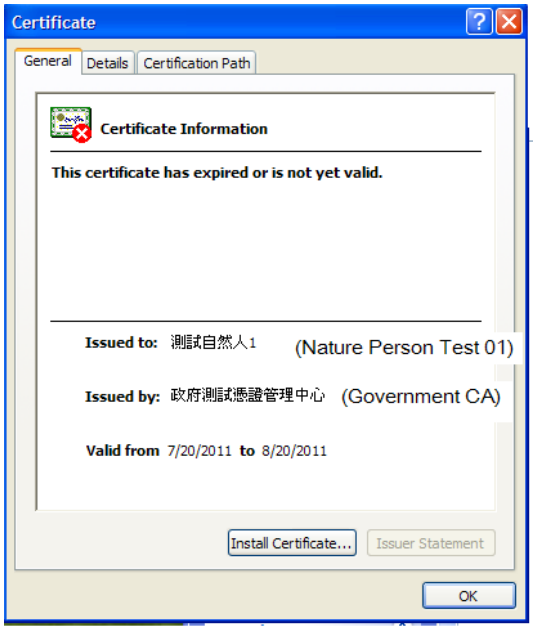


Figure 4.3: A Taiwan MOICA test certificate on a PC display 01

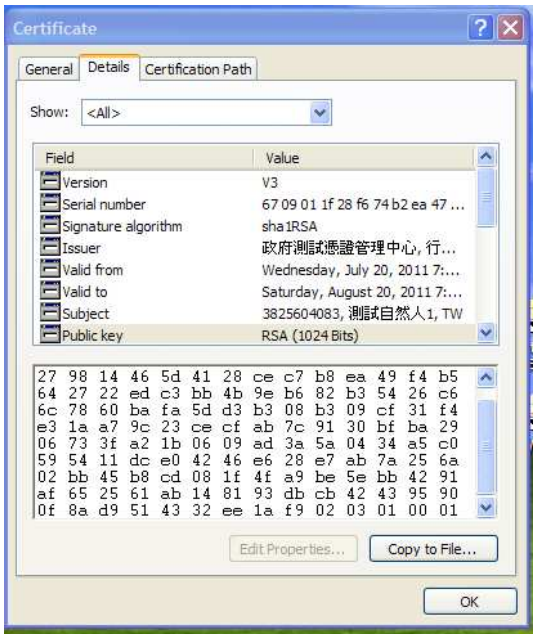


Figure 4.4: A Taiwan MOICA test certificate on a PC display 02

Table 4.2: An example of a test Taiwan MOICA certificate

Version number	V3
Serial number	67 09 01 1f 28 f6 74 b2 ea 47 68 1e 23 48 13 50
Signature algorithm	sha1RSA
Issuer	OU = Test GCA centre, O = Executive Yuan, C = TW
Validity from Validity to	Wednesday, July 20, 2011 7:52:26 AM Saturday, August 20, 2011 7:52:26 AM
Subject name	SERIALNUMBER = 3825604083, CN = Nature person test 01, C = TW
public key	RSA (1024Bits)
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://gtestca.nat.gov.tw/certs/IssuedToThisCA.p7b [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://gtestca.nat.gov.tw/OCSP/ocsp
Certificate Policies	[1]Certificate Policy: Policy Identifier=2.16.886.101.0.3.0
Extensions	Extensions that can be used to store additional information. Such as KeyUsage or AlternativeNames.
Authority Key Identifier	KeyID=4b f6 4a 77 68 d3 94 c4 e3 b5 60 dc 0e 1b ef a9 ba 7b f6 53
Subject Key Identifier	1f 2a 55 a6 87 85 8e cc 97 70 e8 ba ff 15 ef 77 69 c2 10 66
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://gtestca.nat.gov.tw/crl/GTestCA/ completedelta.crl
Subject Alternative Name	RFC822 Name=test@cht.com.tw
Key Usage	Digital Signature (80)

4.3 Citizen Digital Certificate: CDC

The Citizen Digital Certificate is a natural person certificate based on Public Key Infrastructure (PKI), mainly for assisting the Taiwan government in solving problems associated with offering electronic services on the Internet. These problems include the difficulty of verifying online user identity and ensuring the security of online data transmission. The main purposes for having this government PKI (GPKI) are offering good government information security on the Internet, providing integrity and non-repudiation features on each transaction, simplifying government administrative processes (physically and electronically), and upgrading services to be more efficient for both the government agencies and citizens. A CDC card uses RSA 2048 bits key size on a X.509 Public Key Certificate.

Main functions of the CDC include:

(1) *Identification Verification*: During any kind of online process when identity verification is needed, the CDC IC card can be used instead of providing user name and password.

(2) *Encryption*: Information is encrypted; the information being transmitted is protected from the danger of interception and disclosure.

(3) *Signature*: According to E-Signature law[2] [121][122], and with the agree-

[2]E-Signature Law: Legislation passed in the U.S., Canada, U.K., E.U., Australia, New

ment of the signer, his/her signature can be transformed into an E-Signature. When an electronic file is combined with an electronic signature, it is viewed as a legal document and has the same authority as a paper document with governmental seal. Therefore, the original paper document can be legally replaced by the electronic document.

(4) *Electronic Certificate*: Paper certificates from different agencies can be changed into electronic form by using the Citizen Digital Certificate.

Some use cases of CDC include:

- Internet tax return filing
- Health insurance personal data and fine inquiry
- Personal travel restriction inquiry
- Electronic motor vehicle and driver licence information system
- Digital household registration copies
- ID loss reporting

For more detailed explanation please refer to [133][129][136].

Zealand, and most nations around the world establishes the legality of e-signatures. Documents signed online with legally compliant e-signature software are as valid and binding as traditional pen-and-paper documents.

4.4 Government PKI: GPKI

The Government PKI uses the same hierarchy CA structure mentioned in Section 4.2.2 to build a certificate interoperability mechanism between domestic and international domains, and to offer Electronic signature on application documents e.g. Tax application, passport issuance. Several countries have set up their GPKI such as Japan[127], Taiwan[133][130][131][132], Switzerland[128], Australia[125], Denmark[126]...etc.

Government Root Certification Authority (GRCA) is a government credentials management centre and situated at the top of the PKI hierarchy, as government agencies must possess the highest level of public confidence [130]. The GRCA is a trust anchor for GPKI. Other CAs within the GPKI are established by individual government sectors. They issue certificates to be used in applications of electronic government in order to provide more convenient Internet service for citizens and business; this improves governmental administration efficiency and promotes applications development of electronic commerce. According to the e-Government Program (2001-2004) in Taiwan [131][132], the GRCA started issuing certificates to designated CAs in 2002 and providing certification services to government agencies, industry, business organizations, and citizens. Those subordinate CAs are GCA[3], MOICA[4], MOEACA[5], X-

[3]Government CA
[4]Ministry of the Interior CA
[5]Ministry of Economic Affairs CA

CA and GTestCA[6]. For more information about the corresponding CAs please refer to [130][131][132].

The goals of setting up the GPKI are listed below [133]:

1. Building the foundation for the basic security of a governmental Internet certification authority.

2. Simplifying government operations, upgrading service levels to be more efficient and effective for both the government agencies and citizens.

3. Sharing the benefits of the Citizen Digital Certificate plan with industry.

In 2003, the Taiwan Ministry of the Interior (MOI) optimized their administrative processes and began offering online services to citizens who are above 18 years of age [136]. The new concept was intended to speed up processes, increase efficiency and provide a higher service level. The CDC card is called MOICA in Taiwan, which was named by simply adding the two words MOI and CA together, and it was established by the Ministry of Interior in 2003 [131]. Each MOICA is valid for five years from the time it is used [134]. The MOI issues certificates to Taiwanese citizens and as of 18/11/2012 "3,088,711" have been issued [135]. The CDC card (MOICA) is effectively an online identity card, its benefits include having secure and unique verification of a person's identity on the Internet, faster and more efficient administrative processes, more convenience for the citizens from the 24-hour online service, reduction of

[6]GPKI applications Test CA

fraud, and high security for online transactions [136][133].

The CDC card was of interest to the research described in this thesis as it offered a strong and government backed binding of user identity to on-line credentials, whereas strong proof of identity is often a weak area for mobile phone based transaction systems. In Chapter 8 we will describe a protocol that attempts to combine the best features of the CDC and mobile technologies.

Chapter 5

Overview of Mobile Payment

Contents

This chapter provides an overview of related research concerning mobile payment. It covers technologies, platforms, and protocols described in a variety of literatures, which have been proposed in order to facilitate mobile payment services/solutions.

5.1 Introduction

Ever since mobile phone became widely prevalent, people have been thinking of how to easily carry out a payment transaction through the mobile handset. The potential sophistication and practicality of mobile payment has practically evolved in parallel with the evolution of the mobile telecommunications networks and devices. The industry has been making efforts to stimulate mobile payment market by basically offering people greater ease and efficiency during the purchasing process than the traditional payment method, i.e. by cash. Moreover, the trend tends towards providing contactless credit card payment functionality and the increasing availability of NFC technology (and the RFID-SIM) will see this payment method combined with the mobile phone. This is considered a more convenient approach than just carrying wallet full of cards, and these days people always remember to bring their mobile phones with them, whereas wallets and keys may be mislaid.

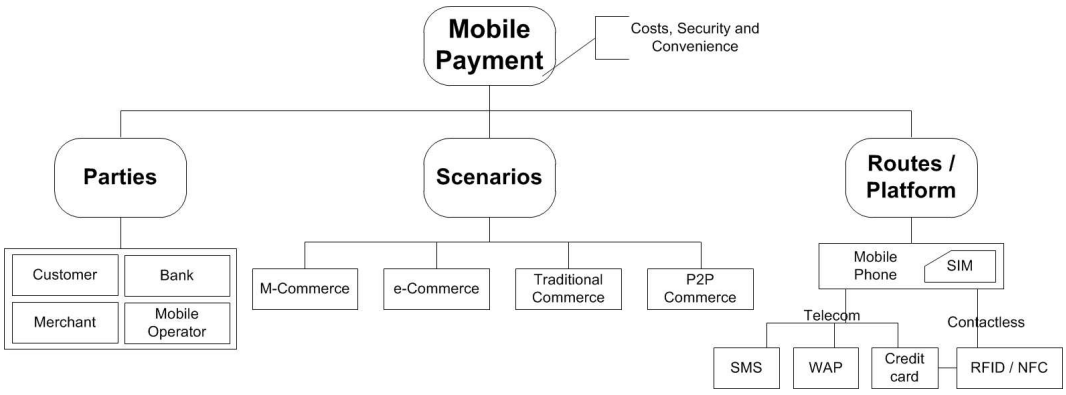


Figure 5.1: M-payment scope.

5.1 Introduction

Figure 5.1 provides a general scope of m-payment, which includes three major divisions such as: **parties**, **scenarios**, and **routes/platforms**.

M-commerce is defined as any transaction with monetary value that is conducted via a mobile telecommunications network [150]. Guo [151], mentions the importance of different methods, timing and medium for the payment in the m-payment business. **Payment methods** differ and can be *account-based* or *token-based*, while the **timing** of the payment can be made in *real-time*, *pre-paid* or *post-paid*. For the **medium**, the payment can be charged to a *bank account*, *credit card* or the *phone bill*.

Mobile payment has seen rapid growth in recent years, and many papers related to m-payment have been published. Papers with technological aspects that use various wireless protocols and technologies as a bearer to carry out the m-payment include:

Table 5.1: Literatures relate to different wireless technologies

1) General Packet Radio Service	[139]
2) Bluetooth	[159][141][142]
3) Near-Field Communication	[160]
4) Interactive Voice Response (IVR)	[146]
5) Short Message Service (SMS)	[140][148]
6) Unstructured Supplementary Service Data (USSD)	[146]
7) Wireless Application Protocol 2.0 (WAP)	[161][143][144]

However, most of the aforementioned approaches are designed for online web payment transaction [166], and have security and ease-of-use restrictions that limit user acceptance. Other weaknesses relate to Internet connection speed or

SMS latency, which result in lengthy set-up and transaction times. There is less literature related to conventional (shop based) payment transaction scenarios [173][174], which will be the focus for all the proposed schemes in this thesis. A good comparison of these proposals along with NFC-based solutions can be found in [166].

Kadhiwal and Zulfiquar have provided an analysis of m-payment security measures and different standards [137], in which various architectural security levels for m-payment are clearly classified. The levels defined by these authors are listed in table 5.2:

Table 5.2: M-payment security measures and standards

Platforms/Application	STK, Browser, Java, BREW
Services/Protocols	voice, WAP, SMS, USSD
Network/Radio Interface	GSM, CDMA, TDMA, 3G, GPRS
On Device	WPKI/WIM, SIM, Device OS

The important analysis factors usually reported are *security strength, transaction efficiency, user cases*, and *scalability*. In Massaoth and Bingel's paper [162] they discussed different mobile payment services compared with an NFC based solution. They showed that NFC is a growing trend for mobile payment solutions, however, there was no focus on the security or how NFC improves and benefits the overall mobile payment system, and not much practical detail on the proposed protocol and architecture.

In general there are several factors that are considered as essential for m-payment to be successful [147][148][149]:

1. Ease-of-use
2. Security
3. Comprehensiveness
4. Cost
5. Technical acceptability [151]
6. Technical feasibility
7. Efficiency
8. Feeling of safety
9. Cognitive automation [145]
10. Compatibility
11. Scalability
12. Complexity [151]

From a security viewpoint, having a secure transaction environment that includes the security of mobile devices and the communication network, is essential in earning the customer's trust in the service. Most of the existing proposals only give high level descriptions of the transaction and business processes and little detail of the actual security mechanisms or data flows. Previous papers also do not take into account the possibility of leveraging existing security

mechanisms from the telecommunication system, e.g. GSM, 3G/UMTS and PKI.

Zhang [152] has raised an interesting point about the main problem of m-commerce at present; the insufficient choice of payment methods. In his paper, he compares the differences between online payments and mobile payments and concluded that mobile payments should make transactions available anytime and anywhere, but that it has not yet matured in terms of new technology and modes. He also commented on the advantages and disadvantages of mobile bankcard payments when compared to the usual mobile billing payment through the Mobile Network Operator (MNO).

It appears that even though the bankcard has a high security, it still requires further identity authentication (for significant transactions), which makes the systems more complex. In terms of contactless card usage for low value payments, it could be argued that the MNO billing method is more convenient mobile alternative, as long as the MNO billing system has a suitable business model and the technology to ensure the security of the transaction. The latter approach could be secured via the SIM card, however the solution might not be compatible or practical to use in a traditional shop. In face many m-payment schemes are not suitable for use within the traditional payment environment, e.g. transferring funds via SMS is not quick or intuitive enough for making a payment at a store and both the customer and merchant would need to reveal their phone number.

To overcome these problems a payment system is required that integrates the SIM's authentication/identity features within the payment system, while stil-l fitting into traditional purchasing procedures via merchants' Point-Of-Sale (POS) terminals, and using the existing telecommunication infrastructure. Therefore a main goal of this thesis is to try and realise such m-payment schemes, exploiting the latest secure proximity NFC technology while leverag-ing and re-using exiting mobile security technologies and solutions.

Chapter 6

NFC Mobile Payment with GSM Network

Contents

This chapter describes a mobile payment system for merchant micropayments, which can be built on existing GSM and NFC architecture components. Many mobile payment methods have been proposed, although most are not intended for a conventional merchant payment environment. Our proposal leverages the SIM's authentication and identification capabilities and uses GSM crypto-

graphic primitives, which simplifies integration into the current mobile infrastructure. The use of NFC for short range communication allows for possible integration with existing Point-of-Sale (POS) equipment and the payment process from the customer and merchant perspectives remains unchanged. The system offers acceptable security for low value payments, customer anonymity and ubiquitous implementation using available technical components.

6.1 Introduction

Mobile phones have become indispensable items in our daily life. As wireless telecommunication and hardware technology become more advanced the mobile phone/handset is evolving into a powerful computing and communication platform. The handset functionality has increased enormously and not only for making phone calls, but also for applications like surfing the internet, watching videos, taking photos, etc. The main benefits of a mobile phone are that it is a "mobile", light and small computing platform with reasonable processing power which makes the handset an attractive alternative to other platforms, such as desktop or laptop computers.

Near Field Communication (NFC), is a relatively new technology that allows the handset to emulate both a contactless card and/or a contactless reader. Its ease of use when conducting short range communication, and compatibility with existing contactless payment systems are major reasons why it is seen as a key enabling technology for mobile payment services.

This proposed scheme focuses on combining NFC functionality with GSM system components to create a new solution for m-payment. It uses existing security algorithms from the GSM system to derive dynamic passwords from signed responses ($SRES$) [153], which are used to secure transactions between different entities communicating via NFC.

The random challenge (R) result ($SRES$) and cipher key (K_c) vary with each

authentication to the mobile network. The same parameters and algorithm used in our scheme can be treated as a plug-in service that is easy to integrate onto the current GSM system. In common with credit card systems, the ordering information (OI) will not be known by the Mobile Network Operator (MNO) and the shop will not know the customer's confidential payment details.

T.S. Fun et al. [163] proposed a symmetric key centric mobile payment system that was constructed upon the MNO protocols. Pointing out the symmetric mobile payment system had performance advantages on the limited computation platform compared to PKI based system. Their symmetric system proposal reduced the communications steps between engaging parties without compromising the security.

The ideas in [162] and [163] can be extended by reusing GSM's existing core cryptographic functionality for authentication and additional encryption key generation, providing a reasonable level of security yet with less computational overhead compared to PKI based solutions. To explore this idea further within this scheme I focus on mobile payment-transactions, although the proposed concept is also applicable to other applications such as identity authentication services.

6.2 NFC M-PAYMENT SYSTEM BASED ON GSM

This section details the design of our proposed mobile payments protocol. The assumptions and requirements for this symmetric cryptographic approach for a mobile payments system are first discussed followed by a stepwise explanation of the payment protocol.

There are number of requirements that must be met for this initial proposed system to work:

1. All the entities must be under the same MNO, as we rely on the MNO and the subscriber SIM sharing secret keys.

   In principle the shared key could be the one used for GSM authentication (Ki), although re-using the key for m-commerce would compromise information security best practice. A better approach would be to have a new key Ki' for the m-commerce aspects although the SIM functionality would remain the same except for the key choice, which could for example be indicated by a new authentication command, or an additional paramter in the existing command. For simplicity of description we will just refer to a Ki in the following text, as representing Ki or Ki'.

2. Both of the shop POS and customer phone are NFC enabled. The SIM used must be a new version that has the secure element functionality.

3. The customer has to trust the MNO (sufficiently for the low value trans-

actions) and follow the SIM should support the existing GSM security mechanisms [153][71][158], with possible minor modification for key choice.

4. we assume that the communication between the Payment Gateway (PG) and the shop POS is over a secure channel, recalling that the purpose of this design is to achieve the m-payment in a "physical" store environment.

   The PG [164] here should be part of the MNO system, acting in a similar fashion to a VLR, which handles authentication triplets in GSM. The PG's job is mainly centered on the related payment and user authentication actions. Note that the random number (R), used in the m-commerce authentication should be will different to the one for the GSM authentication, however it will be of the same size and format.

Implementation Assumptions:

- The phone can support custom applications in the form of Java MidLets
- The Midlets have access to a basic Crypto API (we use the phone for, DES encryption/decryption, DES CBC-MAC and SHA-1 hash)
- The phone can only be temporarily trusted with session keys for encryption/decryption and integrity checking.
- Existing SIM application crypto functions are used for authentication

and key generation; the functions can be slightly modified, but no extra crypto functions added. (We use the SIM for authentication, and key generation)

- Normal communications should be disabled during a transaction

Our goal is to design a payment system that can reuse existing GSM security mechanisms and take advantage of the identity/authentication services provide by the MNO and SIM to build an NFC payment service.

The proposed Symmetric GSM payment data flows and the detailed explanation of the system are shown in Figure 6.1. The proposed system contains the following five entities: HLR/Billing Centre, VLR, Payment Gateway, Shop NFC POS and Customer NFC phone/SIM as defined in [151][164]. A list of variables/entities are provided in Table 6.1.

Table 6.1: ABBREVIATIONS AND NOTATIONS

AuC	Authentication Centre
$D()$	Decryption (DES CBC mode)
$E()$	Encryption (DES CBC mode)
$H()$	Hash Function (SHA-1)
HLR	Home Location Register
$IMSI$	International Mobile Subscriber Identity
K_c	GSM data transmission encryption key generated by algorithm A8, max 64 bits [153][71]
K_i	Ki is the 128-bit Individual Subscriber Authentication Key
K_p	Shop Key shared between MNO and Shop (minimum of 56 bit DES key, but operator specific)
LAI	Local Area Identity
$MAC_{K_c}(R)$	Message Authentication Code, use key K_c to generate MAC on R. (DES CBC-MAC)
MDS	Mobile Digital Signature
MNC	Mobile Network Code
MNO	Mobile Network Operator
NFC	Near Field Communication
OI	Ordering Information
P	Shop
PI	Payment Information
PG	Payment Gateway
POS	Point of Sale
R	$RAND$, Random Number (128 bits) (generated to best practices)
S	$SRES$, GSM Signed Response (32 bits) [153]
SE	Secure Element
SIM	Subscriber Identity Module
TC	Transaction Counter
$TMSI$	Temporary Mobile Subscriber Identity
TP	Total Price
TS	Time Stamp
TSN	Transaction Number
U	User (Customer)
VLR	Visitor Location Register

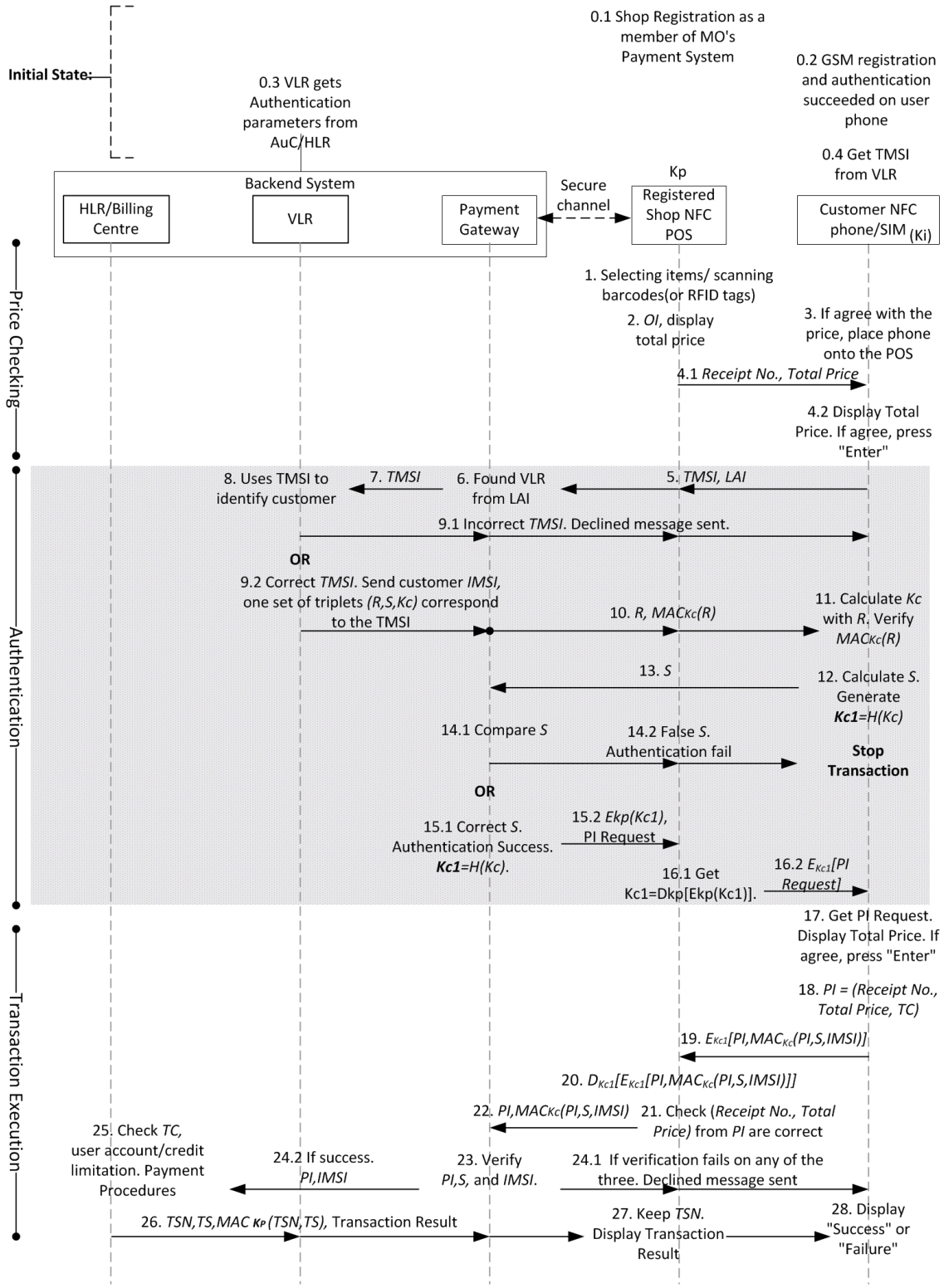


Figure 6.1: NFC m-payment GSM based scheme

6.2.1 Initial Setup

There are some prerequisites to meet before entering the main payment procedures (please look at the "initial state" in Figure 6.1), which are:

Step 0.1: All shops wishing to adopt this m-payment mechanism must register with the corresponding MNO who offers this service. Each shop will be issued with a unique shop key, K_p, by the MNO after shop registration, this shared key would later be used for distributing another secure parameter with the PG.

Step 0.2: The SIM in the user's handset must have successfully gone through the regular GSM registration, activation and authentication processes, and be ready to receive calls.

Step 0.3: As per the existing GSM system structure, authentication will have been conducted via a VLR that can retrieve the authentication parameters, triplets, from AuC/HLR [71].

Step 0.4: The user's handset should get a TMSI allocated by the local VLR.

6.2.2 Price Visual Checking

The first 4 steps contain the initial goods scanning, the price displaying and the visual confirmation at both the shop POS and the customer phone.

Steps 1 – 2: At the beginning of the whole process, the shop POS scans bar-

codes (or RFID tags) from each selected product, calculates the Total Price (TP) of this purchase, and generates a receipt. The receipt is also the Ordering Information (OI) in which the Receipt Number and the Total Price are included. The OI is kept by the shop as a record and a proof of transaction if any dispute happened in the future.

Steps 3 – 4: If the customer agrees with the TP showed on the POS, the customer may place the NFC phone onto the shop POS to continue the payment process. The customer phone gets the receipt number and the total price from the POS.

6.2.3 Authentication

The triple authentication will be executed after the customer agrees to the payment information (PI) in step 4 transferred to the NFC phone. This part encloses processes whereby the backend system, shop POS and the customer handset authenticate the other two entities to guard the safety of the transaction processes that follow.

Steps 5 – 8: The customer phone returns its current "$TMSI$" and "LAI" to the PG via the shop POS. In step 6, as the LAI contains 1-2 digits indicating the Mobile Network Code (MNC), that the customer claims to be using. After the PG recognizes the LAI code, it proves that the user is under the same MNO network as this service (Network correspondence check). The PG then identifies the corresponding VLR by using LAI, and then sends it the customer

$TMSI$. The VLR then attempts to identify the customer from the TMSI.

Steps 9 – 11: If the TMSI is not known to the VLR the transaction is aborted/declines; step 9.1. Alternatively, if the VLR can identify the customer,provides an authentication triplet (R,S,K_c) for this particular customer to the PG. Note that the VLR may automatically have prestored triplets for Ki, however if we use a secondary m-commerce key Ki' then the VLR would need to request associated triplets from the HLR as part of some new non-standard functionality.

Since we assume there is a secure channel between PG and the shop POS, the POS can be treated as transparent in the communication between the PG and the customer handset. From step 10, the PG initializes a "challenge-response" authentication protocol by sending R and $MAC_{K_c}(R)$. As the K_c is generated from the K_i shared between the MNO and the SIM, the SIM can use its K_i to generate K_c with the algorithm A8. Hence the new NFC enabled SIM can use the calculated K_c to recalculate the MAC on the given R, compare this to the MAC sent in step10 to check the correctness of R.

In addition, by verifying R, we determine that the message content of step 10 was sourced by a legitimate PG of the MNO (although at this stage the SIM cannot tell if it is a recorded message, replayed by a rogue POS).

Steps 12 – 14.2: The SIM uses K_i and the verified R to go through an A3 algorithm to calculate a signed response, S, and cipher key, Kc. The Kc

is used to generate K_c1 (as a secret key between the customer phone and the shop POS) taking the Least Significant Bits (LSBs) of the output of the SHA-1 hash. The customer phone sends an encrypted R with key $S1$ to PG.

If the returned S, from step 13, does not match, the PG would return a message showing authentication failed and the transaction is ended.

Steps 15.1 – 16: If S is correct, this also implies that the SIM has a valid K_i. and so the subscriber authentication is successfully completed. The PG verifies the user if successful then continues to step 15.1 and generates K_c1. The PG sends K_c1 encrypted with the known K_p to the POS; step 15.2. Recall that K_p was issued to the shop when it first registered with the MNO. Since the POS can compute K_c1 (step 16.1) using $D_{K_p}[E_{K_p}(K_c1)]$, both the customer phone and the POS now have a shared key to setup a secure communications link to transmit sensitive information. The shop POS sends the Payment Information (PI) back from the customer phone; step 16.2.

6.2.4 Transaction Execution

After successful authentication, the transaction information can be used into the process for further transaction checking.

Step 17: After the completion of the user authentication from previous steps and the TP is sent from step 4, the handset displays the total price, and an "Enter" button to be pressed after the customer has confirmed and agreed

with the price.

Step 18: After the Enter button is pressed, a PI is produced by the customer's handset using the information sent from step 4, which results as $PI = (ReceiptNo., TP, TC)$. A Transaction Counter (TC) is also used here for the purpose of preventing replay attack, otherwise, a copy of step 19 from a 3rd party might go through as long as the shop POS found the value of the total price to be the same as expected. Thus adding a TC here allows the billing centre to update and check the TC value in its system.

Step 19: The SIM computed a MAC of $(PI, S, IMSI)$ with key K_C, which means the user has approved and agreed the PI. MAC was used to provide integrity protection so that PI is finalised and cannot be modified by the shop. The S actually bounds the authentication part (part 2), and the K_c1 bounds the transaction part (part 3).

The IMSI added here allows the billing centre to identify the subscriber, as it is a long term ID for identifying the user to debit the charge and deal with other transaction related information.

For preventing dispute between the customer and the shop. The shop POS shall receive the message $PI, MAC_{K_C}(PI, S, IMSI)$ that is encrypted/protected by the key K_C1 to let it know the Total Price remains unchanged. Furthermore, only the legitimate Backend System has K_c to verify the inner MAC message and authenticate the user by checking S and $IMSI$, and so to process the PI.

Steps 20 – 21: the shop POS decrypts the message from step 19, gets and checks the correctness of the *ReceiptNo.* and TP against the original value from step 4.1. If not correct then the transaction is aborted.

Steps 22 – 23: The shop POS forwards $PI, MAC_{K_c}(PI, S, IMSI)$ to the PG for subsequent payment verification. In step 23, as the PG already knew S and $IMSI$, it can uses K_c to verify the MAC (for user authentication) and PI. The PG hereby confirmed it is still the same user who is using the service. The transaction is based on the user's long term MNO-ID; the $IMSI$, which is associated to the triplet and TMSI used earlier to authenticate the user/SIM. Thus the billing centre can have a clear idea of which account should be charged and by how much.

Step 24.1: If any of the three (PI, S and $IMSI$) fail verification, a declined message is sent back to the shop POS and the user handset.

Step 24.2 – 26: In this system the PG is under the same MNO as the HLR/Billing Centre, to ensure the secure connection for transferring the sensitive data like $TMSI$ and triplets. The PG sends the PI and $IMSI$ to the billing centre, which can then check the user account(and credit limitation) associated with the $IMSI$. A Transaction Counter, TC, is a continuous increment of a series number that increases every time after a payment has been confirmed. The payment process only starts if the TC check shows a positive result. A Time Stamp (TS) of the payment is also included in step 26 that is

important to indicate the specific transaction time for future check and dispute reference.

Once the user has passed the credit check, the billing centre would initiate the following payment procedures and update the billing related information. After the billing centre has confirmed the payment deduction, it sends a message with the Transaction Number, TSN, the TS and a MAC of the two with key K_P to the shop POS.

Step 27 – 28: If the shop POS successfully verified the MAC of (TSN, TS), it then keeps a copy that can be used as a proof when querying the charge in a dispute, and display the result on the POS. Meanwhile, the customer handset shall will also display the result, which allows the customer to confirm and feel more assured with the correctness of the transaction.

6.3 PROTOCOL ANALYSIS

The whole system is basically based on the GSM network and uses its triplets authentication process [71] as the foundation to produce other keys for use in the transaction processes. A main goal was to try and use as much legacy capability as possible (in association with the new NFC capabilities) to provide a practical solution with an acceptable (rather than high) level of security for low value transactions, whilst exploiting some temporary identity and rough location dependence through the TMSI. In this section we give the top-down

security analysis of the protocol.

6.3.1 Detailed Risk Scenario Descriptions

Here we describe some risk scenarios and analyze (step-by-step) the potential security vulnerabilities.

Scenario 1: We assume a customer is dishonest, has a modified handset, and is trying to breach the protocol for personal gain e.g. customer account impersonation and/or credit modification. Thus all messages sent out from the customer handset have to be regarded with suspicion and a number of issues are apparent.

1. Unprotected messages in step 4 and step 5.

   In step 4, the attacker may take advantage of the unencrypted message, $ReceiptNo$ and TP, by manipulating the content to cause a denial of service attack. Alternatively, an attacker could possibly copy stored messages from step 4 and 5, e.g. from the previous customer for an account impersonation, as there are not secret parameters that can be used for setting up a secure channel.

   Normally, each handset on a given network within a specific (but possibly large) local area is allocated a unique $TMSI$.

   As $TMSI$ is unlikely to be renewed as soon as a transaction is completed, there is a chance for attackers to intervene and copy the $TMSI$ informa-

tion. The attacker's modified handset transmits a copied $TMSI$, step 6 to step 10 can still be performed without any problem. The attacker's handset does not have the correct K_c, so cannot verify $MAC_{K_c}(R)$, but the attacker does not care. However, as long as the core K_i inside the SIM is not compromised, the genuine S cannot be calculated by the attacker's handset, the attacker cannot proceed after step 12.

It should be noted that S is a very weak key as it is a 32-bit field and so it is advisable for the PG to operate a retry count on $TMSI$, LAI combinations to prevent brute-forcing of the matching S.

Only the correct match of the "$TMSI, LAI$ combination" with the availability of calculating the correct S and K_c can communicate with the POS successfully at the transaction stage. Therefore, it appears that via this route, attackers cannot illegally extract money from the system.

2. Skipping authentication.

   The financial transaction actually starts at step 16, so an attacker could try and skip the previous authentication steps. So if the request message of 16.2 could be faked, the attacker could get the subsequent information about PI. However, to prevent the whole message from step 16 being copied and replayed, an encryption with the shared key between the POS and the handset, E_{Kc1}, is used to protect the "PI request".

   It is reasonable to state that customers tend to trust what they can see and especially when the display is via their own devices, therefore,

having the handset display (in step 17) re-confirmation of the Total Price (as in step 4 to 5) is a valuable step for the user. For a similar reason, displaying the result of the overall transaction is also crucial for customer trust and confidence.

Scenario 2: In this scenario we assume that the shop owner is dishonest and has access to a modified POS device, and he is trying to manipulate the transaction information in order to deceive the backend system or customer to extract money. Although it is considered that the success of such a shop owner would be short-lived as the owner has to register with the MNO in order to join this mobile payment system. If the shop transactions are reported as suspicious, the shop could be eliminated from the registered list.

1. Unprotected messages in step 4 and step 5.

   The merchant would ask the customer to place the phone onto the POS, and then display the total price on the screen of the customer's NFC phone. However, as we cannot trust the merchant or the POS, it is not guaranteed that the actual price sent to the phone is correct, therefore we added one more step (4.2) in between step 4 and step 5 in which displaying the TP on the phone is necessary to inform the customer that the handset has indeed received the correct price.

   If there was no check and transactions with incorrect TP the PG, it could become overloaded, leading to longer times for legitimate transaction

processing and potential for Denial of Service. Therefore, to protect the customer and the PG the extra step of displaying TP and seeking confirmation from the user is well justified.

2. Most messages need to go through the shop POS, so could be vulnerable to unauthorized access and/or modification.

   The POS does not know key (K_c) used between the backend system and the customer, thus cannot retrieve the core authentication data, S and $IMSI$, from step 19 in order to impersonate the customer phone/SIM. Similar to a typical credit card POS system, the merchant POS network has to have a secure channel connection with the backend system. Normal POS terminals also have to be security certified and protect sensitive data and functionality from unauthorized access, use and modification.

6.3.2 Advantages and Disadvantages of the Mobile Payment System

In this section we weigh up some of the more general advantages and disadvantages of our proposed payment system.

6.3.2.1 Advantages

Re-using existing GSM security mechanisms and taking advantage of intuitive operation and compatibility of NFC with existing payment infrastructure is at the foundation of our scheme. Therefore, the proposed system can easily

inherit the same scalability capability as a GSM system, along with the authentication and encryption parameters. This eases the effort of implementation and integrating the proposed system. The service can also be used anywhere where GSM and contactless payment infrastructure are available.

The dynamically derived session keys are generated from $SRES$ and K_c that are found universally in GSM systems. These can be used to ensure authentication of all three parties involved in our protocol, i.e. (1) Steps 5 – 6, (2) Steps 10 – 11, (3) Steps 12 – 15.1.

Significantly, the shopping list is not revealed to the MNO who then does not know the items that the customer purchased. The shop does not know the customer's long term ID and general purchasing habits, thus supporting good privacy and anonymity for the customer.

The scheme predominantly uses technical aspects of GSM but executing the protocol using NFC has a distinct advantage in that the system could feasibly be deployed using current payment infrastructure, i.e. the protocol can be run between a mobile phone and POS terminals; albeit with some significant changes to the terminals. From the customers' point of view the payment may be similar to paying with a credit or debit card.

6.3.2.2 Disadvantages

A major weakness of this scheme is the short length of the $SRES$ and K_c fields in GSM. Furthermore, customers have to trust the MNO with their involvement in shopping transactions, albeit with some privacy protection. Merchants must also establish a relationship with the MOs, where more typically they are used to relationships with banks. The protocol overhead is relatively complex compared to the m-payment via SMS and WAP, although it has the capability to fit into the existing merchant/customer relationship and use existing POS infrastructure.

The appearance of contactless payment POS devices suggest that the NFC communications will be supported, however the POS terminals would need to be upgraded to support the proposed protocol.

6.4 Conclusion

In this chapter we proposed a hybrid m-payment scheme that combines the technological capabilities of GSM and NFC systems. The scheme should be relatively easy to integrate into existing GSM networks and deployed POS systems. However, the standard GSM cipher key length is a maximum of 64 bits [158], which is insufficient for providing long term security. The scheme could be extended to 3G systems that use a longer cipher key length (128 bits) in order to provide stronger security. Even so, the protocol is not aimed at

security levels associated with high value credit card transactions. The aim is to provide reasonable protection for low value transactions in a convenient way that maximizes benefits from the re-use of legacy systems.

Chapter 7

NFC Mobile Payment with 3G Network

Contents

The increasing technical capabilities of mobile phones have resulted in improvements (with respect to GSM)in wireless communications (referred to as 3G) and security, and several m-payment methods have been proposed. M-payment applications are being developed for both online and in-store purchases. Near Field Communication (NFC) technology has the potential to greatly impact the way mobile devices are used. Recall that NFC is a short range wireless communication interface that allows for the integration of a mobile device in existing

contactless application infrastructure, such as using a mobile phone to pay at Point-of-Sale(POS).

It is important to provide a simple method for implementing m-payment systems that offer both security protection (against anticipated attacks) as well as ease of use for the customer. We propose a system that combines existing 3G cryptographic primitives and algorithms, the identification and authentication capabilities of the USIM, with NFC technology to implement a m-payment system. Such a system could readily be integrated into current 3G infrastructure and provide a practical solution for scalability and ubiquity in m-payment services.

Our proposed scheme focuses on a "conventional in-store payment environment", with mutual authentication between entities and a subsequent trustworthy transaction being achieved through 3G and USIM security services.

7.1 Introduction

Mobile phones, with their ever increasing processing speed and functionality, can offer sophisticated applications and strong security. User requirements for a "good" mobile application generally include ease-of-use, processing speed, practicality and security. Near Field Communication (NFC), a wireless short-range communication technology, has the potential to satisfy all four of these requirements. NFC is especially easy to use and allows the handset to activate applications or initiate transactions through simply being brought into close proximity with another compliant device.

Standards like GSM and 3G already have mature authentication mechanisms, so we take advantage of these and the benefits of NFC technology to construct a new m-payment framework. 3G is prevalent as the leading telecommunication network technology because of its faster data transmission speed and stronger security mechanisms, than in GSM. Recall that GSM has a short ciphering key length (64-bits) [73] and no authentication of the network. In contrast 3G systems use a 128-bit ciphering key[95] in addition to enhanced entity authentication (MILENAGE: $f1 - f5$) [99][100], data ciphering and integrity algorithms (KASUMI: f8-f9) [97][98] for stronger security protection.

We proposed an enhanced version of the GSM m-payment solution with NFC that uses 3G technology in this chapter. This new solution benefits from the 3G authentication mechanisms and stronger data transmission protection

between entities while carrying out the payment transactions process.

Both GSM and 3G telecommunication systems use challenge-response authentication and encryption/decryption schemes for user identification and data confidentiality. Using 3G security mechanisms results in a significant improvement of the GSM system [173]. Notably, the user authentication/identification and payment information (PI) authentication are significantly changed when compared to the original GSM scheme.

The new design objectives of the proposed scheme are as follows:

(I) Improve ordering information authentication and integrity checking to prevent data modification.

(II) User PIN verification is required for confirming the price and to proceed to the subsequent authentication/payment processes; to support higher value transactions.

(III) The security mechanisms in the GSM scheme are replaced by 3G cryptographic primitives, and a real 3G re-authentication is executed for mutual authentication between entities.

(IV) Effectively deliver reasonable confidentiality, integrity and freshness protections of the protocol by "reusing" the cryptographic primitives and functions (i.e. MILENAGE) in the 3G network.

(V) The transaction result is protected when delivered to the customer phone via the shop POS and is verifiable by the customer phone through the use of associated secret keys and algorithms, which prevents the POS terminal from

generating a fraudulent result.

This proposed system is an evolution of the GSM design described in [173], rather than a completely new one. The scheme leverages from the 3G/UMTS environment and security mechanisms. A new version of the USIM (SE-SIM for NFC use) provides a secure environment for data confidentiality (stronger encryption key length), client authentication and authorisation functionality as well as mutual authentication between the terminal(POS) and the NFC phone. In addition, the attributes of NFC wireless technology offer a simple "touch" human-machine interaction that significantly enhances ease-of-use, technical acceptability, cognitive automation and incorporates compatibility with existing RFID/contactless infrastructure. 3G networks are widely used, thus scalability is achieved, and due to re-use of the 3G functions/mechanisms the proposed scheme has good compatibility to existing infrastructure.

7.2 NFC M-PAYMENT SYSTEM BASED ON 3G

In this section We describe the design of our proposed mobile payments protocol. The envisaged *application scenario* is a customer conducting an m-payment in a "physical" store environment with the customer's phone being authenticated onto a 3G network. Our design goal is an m-payment system that can reuse/leverage existing 3G security mechanisms and take advantage of the identity/authentication services provide by the MNO and USIM to build an NFC m-payment service.

A detailed explanation of the system and data flows are shown in Figure 7.1. The proposed system contains the following five entities: AuC/HLR/Billing Centre, VLR, Payment Gateway (PG), Shop NFC POS and Customer NFC phone/USIM as defined in [164]. A list of variables/entities are provided in Table 7.1.

There are number of **requirements** that must be met for this proposed system to work:

1. First of all, in this version of the protocol entities must be under the same MNO, which means both the customer USIM and shop POS have to register with the MNO.

2. Both the customer phone and the shop POS are NFC enabled.

3. The customer's phone must be switched on and authenticated to the 3G network and the customer USIM and the MNO share a secret key, K, because authentication parameters used later in the process are originally generated from the user K.

Implementation Assumptions

- The phone can support custom applications in the form of Java MidLets.
- The Midlets have access to a basic Crypto API (we use the phone for AES block encryption/decryption).

- The phone can only be temporarily trusted with session keys for encryption/decryption.
- Existing SIM application crypto functions are used for authentication, key generation and integrity checks; the functions can be slightly modified, but no extra crypto functions added (we use the SIM for authentication, key generation and MAC calculation).
- Normal communications should not be blocked during a transaction

Note that it is not best practice to use a key for multiple purposes and so if this was considered a problem the USIM and MNO could share another key K', and the key to use would simply be indicated in a command parameter or via modified commands. For simplicity of explanation we will just refer to K in the description although this can imply either K or K'.

Note that in order to satisfy the implementation assumptions it is necessary to introduce a new SIM command (CRYP) described below. Note that this command does not introduce any new cryptographic functions, but rather modifies the input and output of the existing functions, and so represents a minor modification.

CRYP COMMAND

COMMAND	CLASS	INS	P1	P2	P3
CRYP	0x00	0x8F	FSELECT	FMode	FLENGTH

Valid Parameter Combinations

FSELECT	FMODE	FLENGTH	DATA (all fields 16 bytes)	Comment
0x01	0x00	0x20	Key||Input1	f1 e.g. = f1(Key, Input) Note AMF and SQN = 0
0x01	0x01	0x10	Input	f1 e.g. = f1(K, Input) Note AMF and SQN = 0
0x04	0x00	0x20	Key||Input	f4 e.g. = f4(Key, Input)
0x04	0x01	0x10	Input	f4 e.g. = f4(K, Input)

Response data

FSELECT	Bytes(s)	Description	Length
0x01	0x00 - 0x07	Output (normally MAC)	0x08
0x04	0x00 - 0x0F	Output (normally key)	0x10

Mode Usage: Mode 0x00 used at step 12 and 21 of Fig 7.1; Mode 0x01 used at step 29.2

The shop POS has a secure access module (SAM) that contains a shop POS registration/certified key (K_{CER}) shared between the PG and shop POS for encryption of the session key (i.e. $IK1$) for use between the shop POS and customer phone. The user has to trust the MNO and that the secret K is kept safe.

We assume that a secure channel is available for communications between the PG and the shop POS and that all parties in the MNO backend system are in a secure environment. Furthermore, the USIM used must have secure element functionality to execute all cryptographic calculations, i.e SE-SIM, adhere to the existing 3G security mechanisms [89], and allow our proposed m-payment application to utilise the 3G security algorithm as the application security

mechanisms. Moreover, when a payment transaction is in progress receiving and making phone calls are not allowed.

The PG [164] should be part of the MNO system, orientated as a sub-VLR. Its job is finding the correct VLR (step 6), dealing with all communications of the m-payments application from the shop POS, and lightening the workload of the VLR by doing most of the payment and user authentication actions as seen in step 9 of Figure 7.1.

Table 7.1: ABBREVIATIONS AND NOTATIONS

AK	Anonymity Key
AMF	Authentication management field (indicates the algorithm and key in use)
AuC	Authentication Centre
$AUTN$	Authentication Token
AV	Authentication Vector
B	Billing Centre
CK	3G data transmission cipher key generated by algorithm A8, max 128 bits [72][71]
$D()$	Decryption (AES CBC mode 128 bit key)
DT	Date and Time
$E()$	Encryption (AES CBC mode 128 bit key)
f4()	Milenage f4 function used for key generation
f1()	Milenage f1 function used for MAC calculation
HLR	Home Location Register
IK	Integrity Key (128 bits)
$IK1$	A session ciphering key (128 bits) for the shop POS and customer phone generated from f4(IK,CK)
$IMSI$	International Mobile Subscriber Identity
K	Permanent secret key (128 bits)
K_{CER}	Shop POS certified Key shared between MNO and Shop (AES 128 bit)
$KASUMI$	f8-f9 Integrity and cipher algorithms in the handset
LAI	Local Area Identity
$(X)MAC$	(Expected) Message Authentication Code (64 bits)
$MILENAGE$	f1-f5 Authentication algorithms in USIM
MNO	Mobile Network Operator
MP	Mobile Payment
NFC	Near Field Communication
OI	Ordering Information
ON	Order Number
P	Shop
PI	Payment Information
PI_{REQ}	Payment Information Request
PI_{RES}	Payment Information Response
PG	Payment Gateway
POS	Point of Sale

$RAND$	Random Challenge (128 bits)
$(X)RES$	(Expected) Response
SAM	Secure Access Module
SE	Secure Element
SQN	Sequence Number
TC	Transaction Counter
$TMSI$	Temporary Mobile Subscriber Identity
TP	Total Price
TS	Time Stamp
TSN	Transaction Number
U	User (Customer)
$USIM$	Universal Subscriber Identity Module
VLR	Visitor Location Register

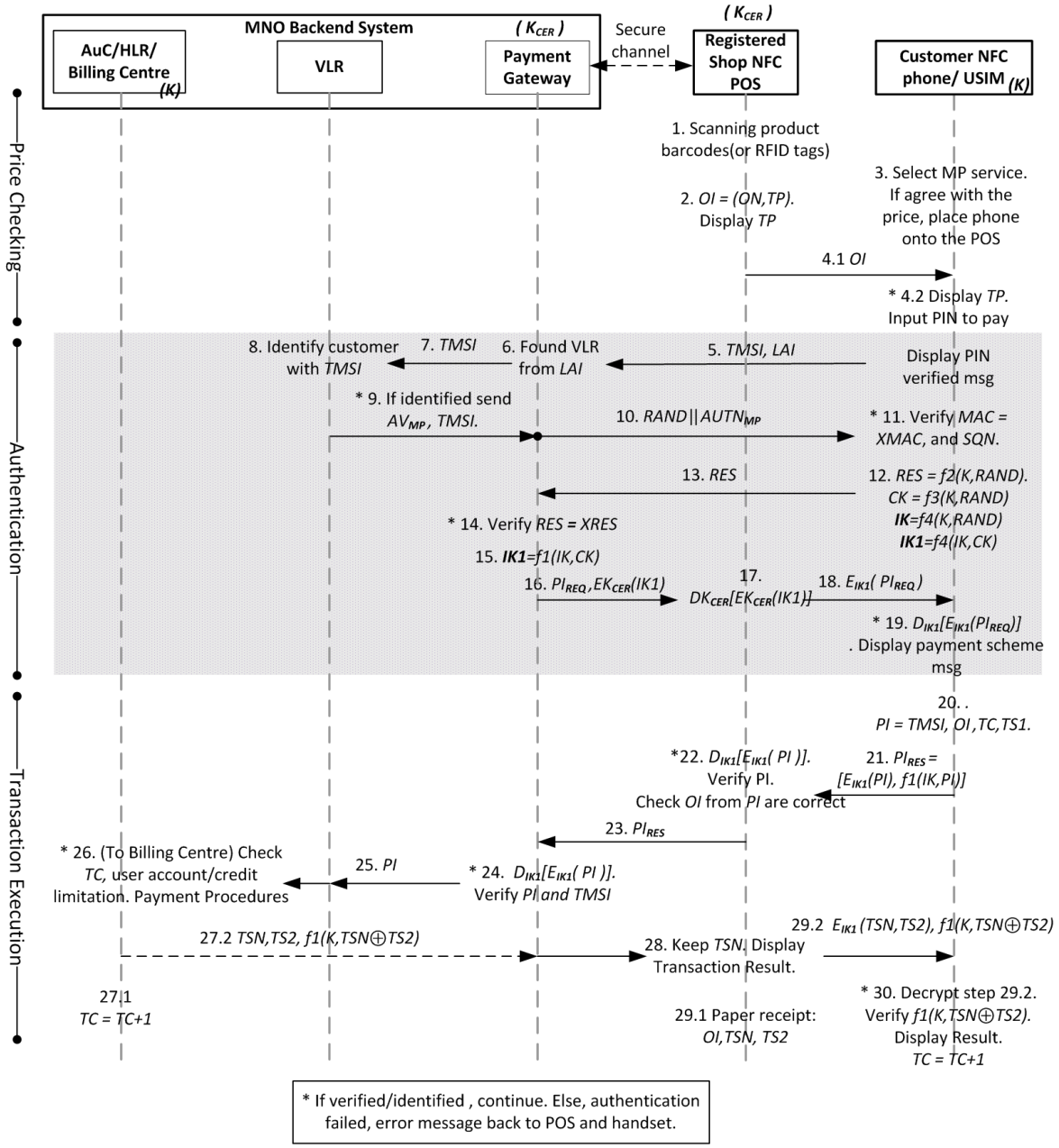


Figure 7.1: NFC m-Payment with 3G Authentication and Encryption

7.2.1 Price Visual Checking

The first 4 steps involve the initial item scanning, displaying the price and the visual confirmation at both the shop POS and the customer phone.

Steps 1 – 2: The shop POS starts with scanning barcodes (or RFID tags) from each selected product, and calculates the total price of this purchase. The order number (ON) and the total price (TP) are kept by the shop as a record and a proof of transaction if any dispute happens in the future. The customer needs to enter the m-payment application (midlet) to start using the payment service. The order information (OI) is comprised of (ON), (TP) and the OI date/time (DT_{OI}).

A DT_{OI} is just a record of the payment start time, it is not strictly necessary, but it is useful to have it as an easily readable reference for distinguishing the freshness of the OI, since using a formal time stamp require further synchronisation and verification between both sender and receiver. The total price (TP) shall be displayed on both of the shop POS and customer phone.

Steps 3 – 4: In these steps the customer visually checks the TP showed on the POS. The customer may place the NFC phone onto the shop POS if he agrees with the price. The customer phone displays the TP once more to ensure the correctness of charge sent to the phone as part of the OI from the POS. Inputting the PIN verifies ownership of the phone and also confirms the TP received. The phone displays the PIN verified message before going onto the next step.

The PIN entry could be skipped for low value purchases, however it is very easy for general shopping to exceed the payment limits associated with PIN-

less contactless card transactions.

7.2.2 Mutual Authentication between Entities

The authentications are carried out after the customer agrees to the displayed TP. This part encloses processes whereby the backend system, the shop POS and the customer phone authenticate each other to safe guard the transaction processes that follow. The POS authenticates the customer phone from the result obtained from the MNO. The customer phone checks that the POS is genuine from the secret information sent originally from the MNO. The process is based on the similar steps in the GSM scheme [173]. In our 3G approach the authentication vector (AV) is used instead of the triplet (used in the GSM approach) for generating the temporary secret key shared between the shop POS and customer phone.

Steps 5 – 8: The $TMSI$, assigned by the Visitor Location Register (VLR), is the most appropriate parameter (as K must, and the $IMSI$ should be kept private) that can temporarily represent the customer at this particular time before setting up a secure channel between the POS and phone. A restriction of this scheme is that m-payments can only be executed at the fixed state within one network sub-area as we need the "$TMSI$ and LAI" to stay unchanged to check the owner of the "$TMSI$" for ID authentication.

* An added advantage of using the $TMSI$ is that there is a binding of the

transaction to location. In step 6, the LAI contains a Location Area Code (LAC), which means that the MNO can use this location information as a crude check that the customer is in the shop. The identity of this $TMSI$ user can be recognised by the VLR, where the associated AV to the customer can be loaded and distributed for later processes.

Step 9: The VLR knows which customer USIM is involved, thus one subset of a group of AVs that belongs to this particular customer is delivered to the PG (note that if K' is used, the VLR may need to request alternative AVs from the HLR/AuC).

Step 9 allows the PG to send an authentication to the customer. Note that AV_{MP} is used to discriminate the vector from the conventional AV used when authenticating the phone to the bearer network. We assume that there is a secure channel between the PG and the shop POS, so the POS can be treated as transparent in the communications between the PG and the customer handset/USIM.

Steps 10 – 14: $AUTN_{MP}$ is one of the 3G authentication parameters from AV_{MP}. In step 10, the PG initiates a "challenge-response" authentication protocol by sending $RAND$ and $AUTN_{MP}$.

In the previous GSM scheme $MAC_{K_c}(R)$ is used for further protection against R (= RAND) being tampered with. However, the "integrity check" functionality is already built into the 3G authentication mechanism, thus we simply

reuse the whole 3G mechanism without modification. If all the authentication criteria are satisfied, the customer infers that the shop POS is legitimate as it is registered and authorised by the same MNO. Once $AUTN_{MP}$ has been verified by the customer phone/USIM and the PG/MNO knows the customer USIM from step 14 is genuine. A secret session key can be distributed to the POS and phone/USIM to set-up a secure channel.

Steps 15 – 19: The session key ($IK1$)is generated using the MILENAGE $f4$ algorithm plus the existing secrets, IK and CK. In step 16, $IK1$ is distributed to the shop POS, along with the Payment Info request, PI_{REQ}. Note that in Figure 7.1 it shows $IK1$ encrypted by the shop registration key ($E_{K_{CER}}()$) in order to emphasis the key usage. However, ($E_{K_{CER}}()$) is actually used to establish the secure channel between the PG and the POS, and so step 16 could have been shown just as "$PI_{REQ}, IK1$" and the decryption in step 17 would then be unnecessary.

PI_{REQ} is needed here to tell the customer phone that network authentication has successfully completed. In steps 19/20 the PI_{REQ} can be decrypted via $IK1$ and if valid a message can be displayed on the phone, e.g. "payment scheme connected please wait". Note that $IK1$ is used as the POS/phone session key so that CK is not revealed to the POS and therefore can still be used for securing network/backoffice communications with the handset.

7.2.3 Transaction Execution

After successful authentication, the transaction information can be used for further transaction checking.

Steps 20 – 21: PI is produced in the customer phone using OI, $TMSI$, transaction counter TC and time stamp TS, as $PI = (TMSI, OI, TC, TS1)$. Both TS and TC are used to prevent replay attacks and ensure freshness of the transaction. The $TS1$ field help the MNO/Billing Centre to make sure the received transaction messages and related logs are valid and happened in the expected duration.

The payment information response ($PI_{RES} = [E_{IK1}(PI), f1(IK, PI)]$) is sent back to the shop POS, which transfers the requested payment information back to the MNO. $IK1$ is used to encrypt PI while a different key IK is used with the MILENAGE: $f1$ function to ensure the integrity of PI. The integrity check prevents PI from malicious modification. As only the MNO and the customer phone/USIM know IK, the MNO is able to verify the validity of $f1(IK, PI)$.

Please note that the $f1$ function accepts a 128-bit input block size (K & $RAND$ in the original 3G system), thus the input PI is constrained to 128 bits. Therefore the field size are specified as: $TMSI$: 32-bits, TC: 10-bits, $TS1$: 10-bits; $OI = (ON, TP, DT_{OI})$, ON: 10-bits, TP: 10-bits (e.g. max 1,023 pounds per transaction), DT: 56-bits (sec/min/hr/day/month/year).

Steps 22 – 23: The POS can recover PI after decryption with IK. If the received OI/TP is different to the original from step 2, the POS has the right to stop this transaction; otherwise, the POS forwards PI_{RES} to the backend system for further transaction authentication and verification.

Step 24: The first MNO entity that receives PI_{RES} is the PG. The PG acts as the entry to the MNO for purpose of the m-payment scheme, collects/verifies PI and the customer identification information, $TMSI$; and for $TMSI$ that is still equivalent to the USIM which requested this service in steps 5 & 6. The PG is used to provide similar checks as in step 22, but is also able to check the integrity of, PI (due to knowledge of IK), as well as the correctness of the $TMSI$. In this mobile system it is crucial to have the PG under the same MNO with the HLR/Billing Centre, to ensure the safe connection for transferring sensitive data like PI_{RES} [173].

Steps 25 – 26: Here the PG sends PI to the billing centre, and not the AuC/HLR. The billing centre first checks if the TC is synchronized with the user record associated with the $TMSI$ and then checks the account/credit limitation. The Transaction Counter (TC) is incremented every time a payment is confirmed. The payment process only starts if the TC check shows a positive result[173].

Steps 27 – 28: If the credit check of the customer is valid, the TC would be incremented by one. The Transaction Number, TSN, includes information

of the transaction result and any other information that the MNO wants to enclose [173]. The TSN is integrity protected using the MILENAGE function $f1(K, TSN \bigoplus TS2)$.

The 3G authentication key, K (or K'), is the only relevant long-term shared secret between the home MNO and USIM, which means only these two entities can verify "$f1(K, TSN \bigoplus TS2)$". It is crucial to deliver the correct transaction back to the customer to prevent an untrustworthy shop from tampering with the TSN.

In step 27.2 an "exclusive or" is used to mix TSN and $TS2$ and compress the data to fit into the field size in order to satisfy the key size limitation (maximum 128 bits) of the MILENAGE: $f1$ function. The size and format of the TSN and the method of $TS2$ combination and filed size mapping can be MNO decisions..

Steps 29 – 30: In step 29.1, the paper receipt should contain at least OI, TSN and $TS2$. In step 29.2, $(TSN, TS2)$ are encrypted under $IK1$ to avoid modification by an attacker. In step 30, the customer phone can retrieve $(TSN, TS2)$ and also verify the integrity of the TSN passed from the shop POS, which can be helpful if a merchant/customer dispute occurs. Finally, displaying the transaction result on the phone gives the customer confidence in the correctness of the transaction [173].

7.3 PROTOCOL ANALYSIS

7.3.1 Detailed Risk Scenario Descriptions

Risk scenarios are concerned with the physical merchant POS and customer phone/USIM in a payment token environment. A selection of potential security vulnerabilities are discussed in this section.

Scenario 1:

An untrustworthy customer with a modified handset is trying to get illegal benefits from potential loopholes in our proposed system, e.g. customer account impersonation or credit modification. Messages received and sent must have strong security protection, otherwise confidential price and personal information may be stolen/modified by a malicious 3rd party or fraudulent customer.

1. Unprotected messages in step 5.

   As mentioned in [173] a $TMSI$ is unlikely to get renewed as soon as the transaction is completed, so it could be possible for attackers to copy the $TMSI$ information. An attacker using a forged handset can bypass the PIN entry protection step (step 4.2) and continue the processes until step 10 (receive $RAND$ & $AUTN_{MP}$).

   However, the forged handset can not authenticate the received information and generate the correct RES to send to the MNO in order to prove

that the response came from the real subscriber's handset. As long as the permanent secret key between the MNO and the customer USIM is not compromised, the customer identity can be kept safe without being cloned and/or re-used fraudulently.

2. Replayed messages of step 21.

   Here it is assumed that the attacker bypasses the authentication section, and attempts to exploit the subsequent transaction stages. In step 21, PI is encrypted with the key $IK1$ for confidentiality, and IK is used with $f1$ to provide integrity protection and prevent modification attacks. Ensuring freshness is required to prevent replay attacks. Thus in order to ensure the uniqueness of each message, the transaction counter value TC, that is included in PI, is incremented after each successful transaction and synchronised with the MNO.

   Note that IK is changed after each transaction. Only the genuine USIM is able to generate the correct IK and $f1(IK, PI)$ in step 21 for authentication by the MNO. The protocol design also prevents the situation when the merchant is untrustworthy and using a modified/forged POS.

Scenario 2:

A dishonest merchant with a modified POS tries to manipulate the transaction

information in order to deceive the backend system (e.g. ask for fake/gratuitous payments from the MNO with no item sold), or to deceive the customer (e.g. charge the customer a larger amount) to fraudulently extract money. This scenario must be considered in the design of the system even though our proposed architecture requires merchants to register with the MNO, which means that any merchants acting fraudulently should be swiftly disqualified from the registered list [173].

1. Unprotected messages in step 5.

   An unprotected $TMSI$ and LAI can be obtained and stored fairly easily. However, this information is temporary and the customer's identification may change when the customer handset moves to a different 3G network cell/local area. On the other hand, if the customer is still shopping within the same area then further security mechanisms are required.

   The protocol makes use of the 3G authentication mechanism to prevent the customer identity being spoofed. This means that despite the $TMSI$ remaining unchanged over a shopping area or period of time spent shopping, a forged POS cannot impersonate customer's identity to the backend system.

2. Displaying the payment result to the customer.

   The transaction result has to be known to both the shop POS and cus-

tomer phone. For example, the merchant could deny the successful payment transaction and not give the purchased item to the customer, when the payment actually completed and debited the customer's account. The protocol provides that the message can be read by the Shop POS as well as delivering the genuine result to the customer phone, taking into account that all MNO messages are returned to the phone via the shop POS.

The function $f1(K, TSN \bigoplus TS2)$ in step 27.2 works as a keyed hash function that provide integrity protection. This prevents transmitted information, $TSN \bigoplus TS2$, being modified by a dishonest shop POS. Alternatively, the payment result can be sent via SMS direct to the phone, but a drawback is that the SMS process requires additional overhead and could add to the total transaction time and cost.

7.3.2 Advantages and Disadvantages of the 3G Mobile Payment Scheme

Advantages: The benefits of the proposed protocol/system are listed below.

1. The protocol reuses the existing and well proven secure algorithm/functionality of the 3G network and the availability of a long-term shared secret key between the MNO and USIM. This reduces the technical changes that are to be implemented and requires less integration effort within deployed 3G systems.

2. The proposed system offers broad scalability, ease of use as well as good user authentication/identification and data confidentiality. The service can be used anywhere where 3G and contactless payment infrastructure are available. The MNO gets the advantage of being involved in payment transactions as well as collecting customer location and transaction records for business strategy purposes.

3. From a privacy perspective, no more information is disclosed than for normal credit/debit card transactions.

4. The mutual authentication mechanism of 3G, AKA, is used by the MNO, shop POS, and customer phone to authenticate each other (steps 5 – 14). The customer's shopping list is not revealed to the MNO, and the customer's long term ID and personal MNO associated payment information cannot be retrieved at the shop POS, thus good privacy and reasonable anonymity are provided to the customer.

Disadvantages: As well as the advantages mentioned above, there are also weaknesses that need further discussion.

1. A major drawback is that due to the utilization of the $TMSI$ for initial user identification the system is restricted if used in a changing $TMSI$ environment like a moving vehicle, e.g. trains.

2. The whole m-payment process is online and reliant on communication

connections, while some merchants would prefer an off-line payment method as this increases speed of the transaction and minimises the merchant's data cost.

3. In the description of step 20, a bit-breakdown is suggested for PI. A problem may occur if the input data, in step 21, to the $f1$ function is larger than the maximum size of 128-bits. Possible solutions are either to perform a hash function before $f1$ for each of the sub PI parameters or to use $ExclusiveOR(XOR)$, thereby maintaining simplicity and efficiency while adhering to the maximum input data length.

4. 3G re-authentication is performed in the mutual authentication section and so if we use the key K without some functional changes in the phone we risk the phone's radio cipher and integrity keys, thus the m-payment could disrupt normal communications. Furthermore, and as mentioned previously, it is not a good idea to use a key for more than one purpose and so it may be better to use a second K', shared between the MNO and the USIM although this would require some additional functional changes in the phone/USIM and back office.

7.4 Conclusion

The core of this scheme is based on a simple challenge-response authentication process that reuses the 3G security functions and parameters to provide a prac-

tical NFC m-payment system. Unlike in the previously proposed GSM-based schemes, where repeated hash functions are used for generating new cipher and integrity keys, the 3G scheme uses existing keys. The authentication process is shortened and less effort is needed for generating new cryptographic keys for ciphering and protection compared to the GSM based scheme. The security of the entire system is strengthened by the enhanced 3G authentications mechanisms. Future investigations include off-line transactions and self-service check-out.

Chapter 8

NFC M-Payment with Citizen Digital Certificate

Contents

In this chapter a Citizen Digital Certificate (CDC) m-payment scheme in conjunction with NFC is proposed. Detailed system architectures, protocols, steps and analysis are given to show the feasibility of this scheme.

With the increasing availability of smart handsets, the mobile phone is likely to become the device of choice for accessing sophisticated services and applications in a convenient yet secure manner. This is especially true with the introduction of Near Field Communication (NFC), which provides the phone with an

interface allowing it to act as a smart card reader or to emulate smart cards. However the user registration process is relatively weak for access to mobile communication services and some third party application providers have concerns when security certification is totally reliant on the trust and processes of the mobile network operator. In contrast, the Citizen Digital Certificate (CDC) is a PKI based citizen identification card issued to a user by the government, following a rigorous user registration process. In our investigation we explore the combined use of NFC phones and the CDC card, by using the government card to endorse the security of credentials held within the NFC Security Element that is hosted within the phone's Subscriber Identity Module (SIM). In this chapter, we propose and describe a secure mobile payment system solution for use in a traditional in-store environment, which combines the CDC PKI, the NFC secure element within the SIM and a 3G mobile network. Moreover, the solution provides a convenient user experience, which leverages from the wide-scale 3G network and the short-range contactless communication of NFC, and could replace the use of payment or service specific smart cards.

8.1 Introduction

A very common way of allowing users to make non-cash payments is to issue them with a smart card. The number of issued physical cards has been steadily increasing in recent years and many people have multiple debit, credit and transport cards. To address this, some bank cards are already issuing

multi-purpose cards, e.g. the Oyster card and payWave variant of credit cards issued by Barclay in the UK. Combining banking and transport functionality in a secure manner has some notable advantages, e.g. a user can have the e-cash functionality of a transport card and use the bank credentials for top-up whenever the credit runs low. [165]

The above example serves to illustrate that an alternative to simply issuing more and more smart cards is desirable and that a solution may benefit from combination of multiple technologies and legacy systems. In this chapter the combination of the multiple technologies: Near Field Communication (NFC), Secure Element-SIM (SE-SIM) and Public Key Infrastructure (PKI), are used with mobile communication and CDC legacy systems to construct an m-payment system.

NFC in addition with SE-SIM provides strong cryptographic calculation power and proximity communication between compatible devices. It offers good security, yet an easy intuitive user experience and ubiquitous mobile access to users' payment accounts and credit. The functionality may also be securely managed via the mature and well standardised telecommunication infrastructure of the mobile network operator (MNO). PKI, apart from its slow speed of calculation on limited resource devices, offers strong security and verifiable digital signatures without the key distribution problems of symmetric solutions. How to combine the best features of these existing technologies (and associated legacy systems) and construct a secure and easy to use in-store

payment system, is the main goal of this work.

Two phases are defined in the proposed payment transaction; the user registration (endorsed registration) phase and the actual payment execution phase. Registration is only performed once and relies on a prior trust relationship of both the MNO and the user with a third party Certification Authority (CA). In particular, the CA is the government entity that issued the user's CDC card. The MNO trust relationship with the CA permits a mobile enabled transaction to be associated with the strong user identity registration of the CDC card. Note that some changes to CDC functionality would be required to adopt this solution, although they are well within the capabilities of the CDC card devices.

8.2 NFC M-PAYMENT SYSTEM WITH CDC

We assume that a customer wishes to perform a mobile payment transaction while shopping within a conventional in-store environment (with a fixed line POS) and that the customer is already registered for CDC i.e. CDC is a government issued certificate that works as a digital ID card. The uniqueness of the CDC card, the private-key and public-key secure functionality, and the nation-wide acceptance and validation are complimentary features for NFC phone (SE-SIM) enabled mobile payment services. Please note that all phone-based cryptographic calculations and confidential data in the proposed solution are carried out and stored in the SE-SIM.

8.2 NFC M-PAYMENT SYSTEM WITH CDC

In this section, a step-by-step description is given of the combined CDC and NFC mobile payment system solution. The m-payment transaction service is separated into two phases: **Endorsed Registration phase** and the **Payment Transaction phase**. Assumptions and requirements are presented before each phase description. All the notations and abbreviations used within the descriptions are provided in Table 8.1.

Table 8.1: ABBREVIATIONS AND NOTATIONS

AuC	Authentication Centre
CDC	Citizen Digital Certificate
Cer	Certificate (X.509)
$D()$	Decryption (RSA 2048 bits)
DT	Date and Time
$E()$	Encryption (RSA 2048 bits)
EC	Endorsed Credential
ED	Expiry Date
GEN	Self Key Generation Command from MNO
GCA	Government Certificate Authority
ID	Identity/serial number of the smart card
$IMSI$	International Mobile Subscriber Identity
K_{APP}	Application Key between SE-SIM and CDC
MAC	Message Authentication Code
MNO	Mobile Network Operator
MP	Mobile Payment
$MSISDN$	Mobile Subscriber ISDN Number (phone number)
MSK	Shared key between MNO and SE-SIM (AES 128 bits)
NFC	Near Field Communication
OI	Ordering Information
ON	Ordering Number
PI	Payment Information
PI_{REQ}	Payment Information Request
PK	Public Key
POS	Point of Sale
PR	Payment Result
R	Random Number
SE	Secure Element
$Sig_A(B)$	Signature of B which is signed by key A
SK	Private Key
SN	Serial Number
TC	Transaction Counter
TL	Transaction Limit
$TMSI$	Temporary Mobile Subscriber Identity
TP	Total Price
TN	Transaction Number
$USIM$	Universal Subscriber Identity Module

8.2.1 Phase 1: Endorsed Registration

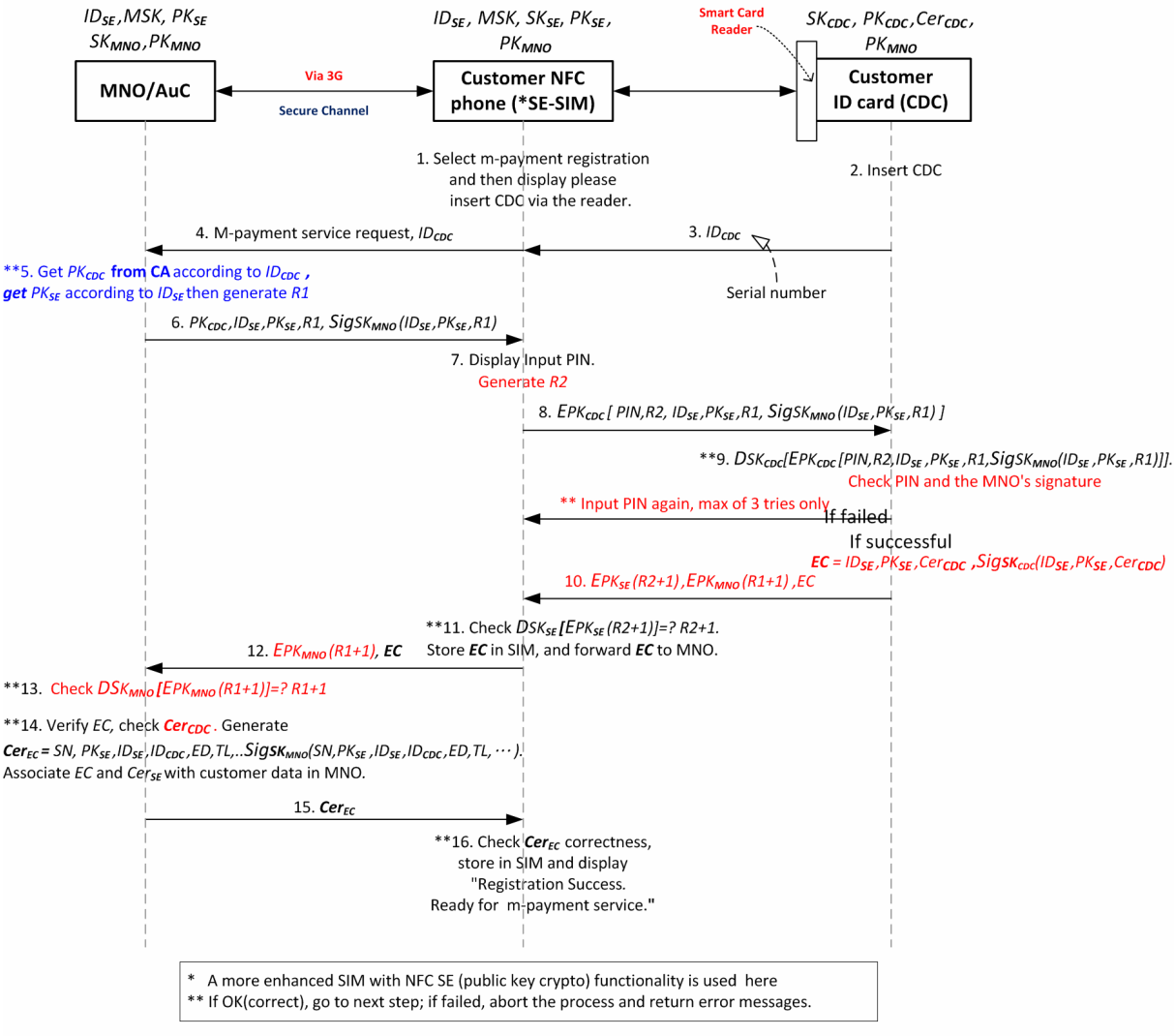


Figure 8.1: NFC m-Payment with CDC – Endorsed Registration Phase

Endorsed registration is the process of binding the mobile transactional credentials with customer credentials certified by a trusted third party. As Figure 8.1 depicts, three entities are used in this phase: **MNO/AuC**, the **customer's NFC phone/SE-SIM** and the **customer's ID card**, e.g. CDC.

8.2 NFC M-PAYMENT SYSTEM WITH CDC

Here we use CDC as an example in the system and assume both MNO and customer's CDC are under the same CA, i.e. the Government CA (GCA). Please see Figure 8.2.

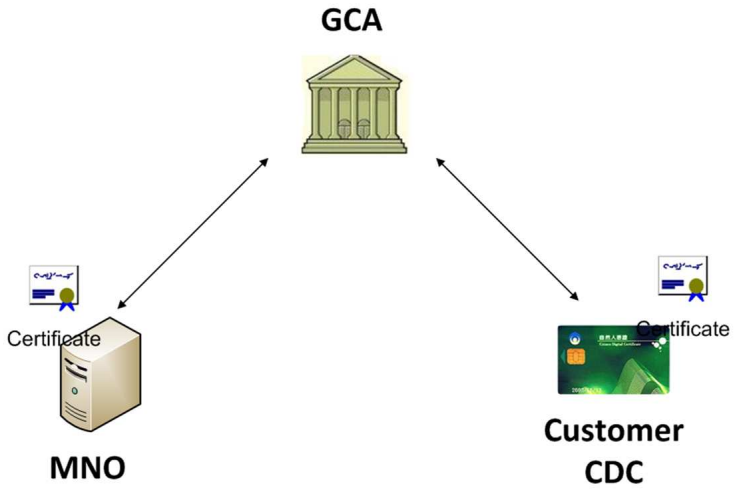


Figure 8.2: Hierarchy of MNO and CDC under the GCA

The GCA (which represents the trusted third party) is used to verify the customer's CDC, so that it can be used to endorse the customer's SE-SIM. The MNO works as a domain entity to verify the mobile user's phone and associated CDC. Because it recognises the GCA it can check the authenticity of the CDC provided by the customer and verify the Endorsed Credential (EC) to generate a certificate for the SE-SIM (Cer_{SE}) for later use in mobile payment transactions.

The customer NFC phone is a bridge for the MNO to authenticate the CDC ID card and prove that transaction information is backed by the CDC. The main job of the CDC here is to generate the EC as a valid endorsement for

the customer phone when performing subsequent m-payment transactions.

Some additional *assumptions* are necessary:

(1) The MNO has already cooperated with the GCA, which means the CDC card would contain the public key of the MNO (PK_{MNO}) when it is issued to the user.

(2) The MNO has pre-stored its public key (PK_{MNO}) and a "personalised" shared key (MSK) on the SE-SIM.

(3) The SE-SIM already has a personalised secret key (SK_{SE}) and public key (PK_{SE}) stored securely in non-volatile memory.

(4) The mobile communication channel between the MNO/AuC and the customer NFC phone is secure.

(5) The customer NFC phone has an external smart card reader (or cradle) connected in order to communicate with the customer's ID card (CDC).

(6) The MNO can obtain the public key of the CDC via a channel to the GCA.

Note that assumption (5) is only required for registration and would become unnecessary if future CDC cards follow the market trend and also offer a contactless interface.

The first step of endorsed registration is to forge a strong legal binding between the "customer's CDC" and "SE-SIM" cards. In order to achieve this we use the customers's CDC private key (SK_{CDC}) to sign the public key of the SE

(PK_{SE}). An Endorsed Credential (EC) and a certificate of the SE (Cer_{SE}) will be generated and utilised in the payment transaction phase. For further detail on the binding generation processes between the CDC and the SE-SIM please see the protocol step descriptions.

Steps 1 – 2: The customer first selects "registration" feature from the m-payment application on his mobile phone, which prompts the user to insert the CDC card into the reader (or bring in NFC range if contactless CDC).

Step 3: Here the ID number of the CDC card (ID_{CDC}) is sent to the customer's phone.

Steps 4 – 5: The customer's NFC phone makes an m-payment service request to the MNO.

We assume there is a secure channel between the MNO and the customer phone, using the identity and security credentials that are pre-stored in the SIM and known by the MNO. Furthermore, the MNO has records of the phone's ID_{SE} and associated PK_{SE}. By sending the ID_{CDC} to the MNO it is possible for the MNO to check the validity of the CDC via the GCA and obtain the associated public key (PK_{CDC}).

Step 6: A random number, $R1$, is generated when the check of step 5 is successful. The MNO produces a packet of information including PK_{CDC}, ID_{SE}, PK_{SE}, $R1$. A signature is added using the MNO's private key (SK_{MNO}). For

the efficiency purpose, PK_{CDC} is excluded from the signature so it can be used as an encryption key by the user phone and the rest of the parameters can also be put into use right away in step 8.

Steps 7 –8: After the pack of information is received, the NFC phone prompts the user to enter a PIN for the purpose of user identification of the CDC card. The SE-SIM then forwards a new pack of information to the CDC including the original information ID_{SE}, PK_{SE}, $R1$, MNO's signature in addition with the PIN and another random number, $R2$, using the public key of CDC sent from MNO and encrypted under it.

Step 9: The government issued ID card, CDC, decrypts the received packet of information $(PIN, R2, ID_{SE}, PK_{SE}, R1)$ from the MNO and SE-SIM. If the PIN check fails then the phone may repeat step 8 allowing the customer to try again. If the PIN try limit is reached (typically three attempts) then the transaction terminates with an error message and customer guidance is displayed via the phone. The significance is that the CDC card may no longer be in possession of the legitimate holder.

If the PIN and signature are valid the CDC card increments both $R1$ and $R2$, to reduce the risk of replay attack when the values are used again. An Endorsed Credential (EC) is generated here, which is a binding of NFC phone and CDC information (ID_{SE}, Cer_{CDC}, PK_{SE}), that is signed by the CDC.

ID_{SE} and PK_{SE} are the two critical components for identifying the SE-SIM.

Cer_{CDC} and the signature of the CDC provide a proof that these components are backed and guaranteed by a legitimate government issued ID card. $EC = ID_{SE}, PK_{SE}, Cer_{CDC}, SigSK_{CDC}(ID_{SE}, PK_{SE}, Cer_{CDC})$.

Steps 10 − 11: The random numbers $R1 + 1$ and $R2 + 1$ are used by the MNO and SE-SIM respectively as tests of **freshness**. $R1 + 1$ and $R2 + 1$ are encrypted by PK_{MNO} and PK_{SE} respectively to provide **confidentiality**. The encrypted random values and the EC are sent to the NFC phone. Providing $R2 + 1$, is correct, the EC is stored in the SE-SIM.

Steps 12 − 14: The encryption of $R1 + 1$ by PK_{MNO} and the EC are forwarded to the MNO for further authentication. The MNO can decrypt $R1+1$. If the check on the returned $R1 + 1$ is correct, it implies that the correct CDC card is being used for registration this is still true as the value of R1 is correct. Furthermore, by checking the certificate of the CDC (Cer_{CDC}) via the GCA's Certificate Revocation List (CRL) the MNO can determine if the CDC is still valid. After the check of Cer_{CDC} and EC, a new certificate is created for subsequent use in m-payment transactions.

This certificate is called the certificate of EC i.e. (Cer_{EC}) and it includes extra customer account information and payment details associated to this service, such as the certificate's serial number (SN), expiry date (ED), transaction limits (TL) as well as PK_{SE}, ID_{SE} and ID_{CDC}. All this information is signed by the MNO's private key (SK_{MNO}).

Step 15 – 16: Finally the certificate of EC is sent back to the NFC phone. If the signature is correct the information is stored in the SE-SIM for use in the m-payment transactions.

8.2.2 Phase 2: NFC m-Payment Transaction

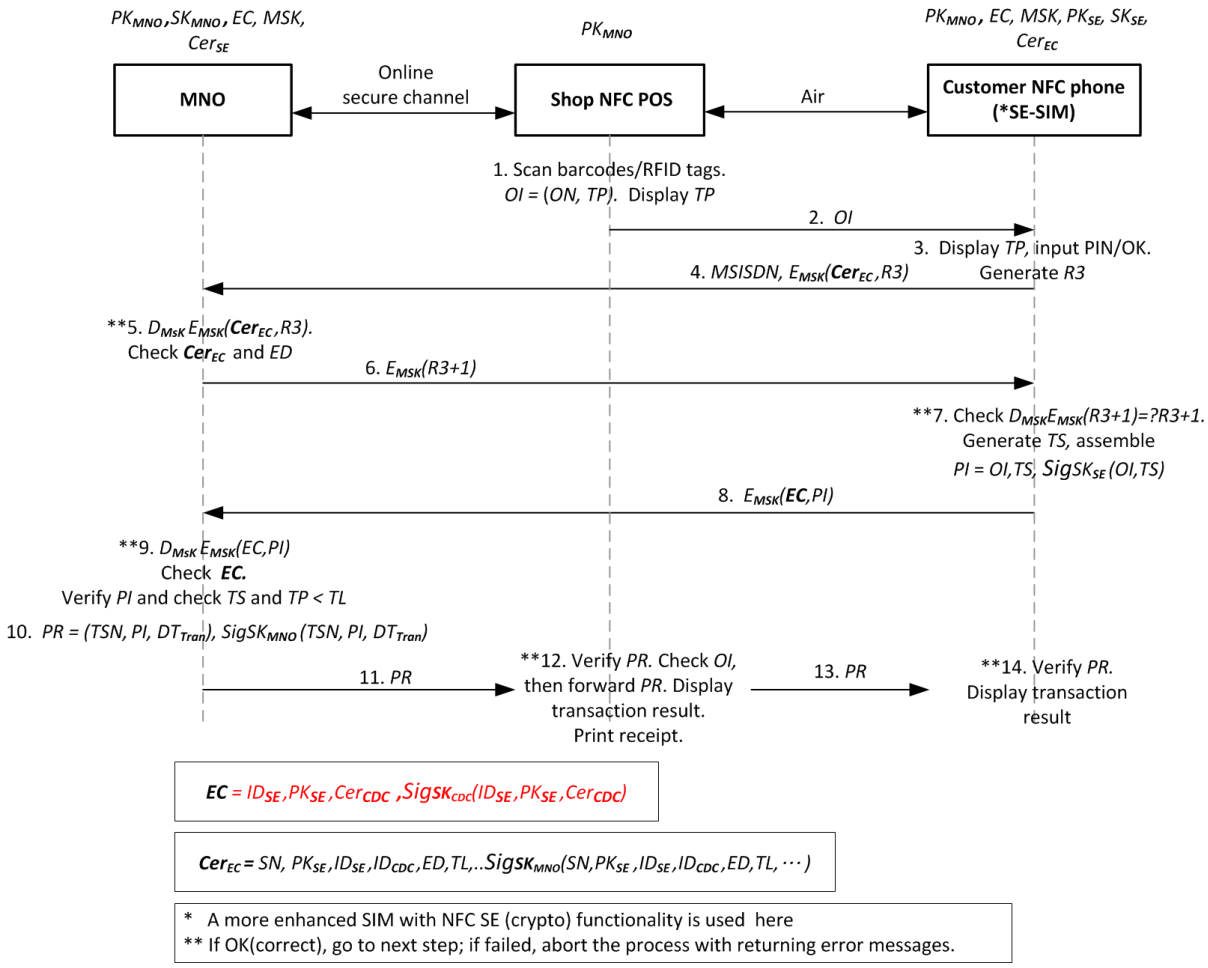


Figure 8.3: NFC m-Payment with CDC – Payment Transaction Phase

Given a successful endorsed registration from the previous phase, the customer phone/SIM is now ready to perform in-store m-payment transactions, in which a customer tries to perform an in-store m-payment through the authentica-

tion/verification of the MNO (that is endorsed by the CDC). On first entering the payment application, the phone shall automatically display the expiry date of certificate EC to the user, and payment actions will be restricted if Cer_{EC} is out of date. The general payment process is that a customer presents his phone close to the shop NFC POS, so the phone can present Cer_{EC} for an ID authentication of its SE-SIM, and if the check passes then EC is sent in addition with the payment information.

The MNO should already have EC and Cer_{EC} from the registration phase, and a personalised/unique secret key (MSK) for the customer SE-SIM. There is no secret key shared between the shop POS terminal and the customer SE-SIM, thus the shop POS relies on the MNO to verify the authenticity of the customer SE-SIM. The shop POS is able to verify the MNO signatures as it has access to the public key of the MNO (PK_{MNO}).

Steps 1 − 2: The shop NFC POS first scans barcodes/RFID tags of the items to be purchased. The shop POS has a display of the total price of this purchase. The customer holds his phone close to the shop POS as the preferred method of payment and receives ordering information (OI) from the POS. The information includes the order number (ON) and total price (TP). A given date/time of purchase is essential in any kind of payment transaction record.

Step 3: In this step there is a design option, as the user can be prompted for

manual input e.g. a PIN, or alternatively the process could continue automatically for a faster/smoother transaction. The manual check prevents misuse of lost or stolen phones; whereas an automatic process can be faster and more convenient for customers. By displaying total price, the customer can be sure that the amount of money he would pay is correct. The SE-SIM then generates a random number ($R3$) that is used in subsequent authentication.

Steps 4 – 5: The Cer_{EC} and $R3$ are encrypted under the personalised key (MSK) between the MNO and the SE-SIM and sent along with the Mobile Subscriber ISDN Number ($MSISDN$) (phone number) to the MNO, using the POS as a simple pipe. Using $IMSI$ instead of $MSISDN$ for added privacy is an option, however $MSISDN$ is perhaps more relevant to customers i.e. clearly indicates purchases made with the phone.

In any case, the account details can be linked to the $IMSI$ or $MSISDN$ by the MNO, which means the MNO should know the SE-SIM's identity and the associated certificate created during endorsed registration. The MNO compares the received Cer_{EC} with the registration version and checks for expiry before continuing with the process.

Step 6: The incremented $R3$ is encrypted under MSK and sent back to the customer SE-SIM, using the POS and phone as a simple pipe.

Steps 7 – 8: If the check of the incremented random number is correct, the SE-SIM can confirm that it is dealing with messages from the genuine MNO. The

SE-SIM then generates payment information, $PI = OI, TS, SigSK_{SE}(OI, TS)$. The time stamp ($TS$) is embedded here to keep the **freshness** of the system. The customer SE-SIM signs OI and TS, to prove that this binding data is authorised and legally issued from the SE-SIM. In step 8, the PI and EC are encrypted under MSK (to preserve privacy) and sent to the MNO.

Step 9: EC is checked first after the decryption of the binding data from step 8. The MNO uses PK_{SE} from within EC for verifying the signature of the SE-SIM on the payment information. At this stage, the MNO has confirmed the identity of the customer and its signed PI. A check of time stamp (TS) is necessary to ensure payment messages are sent within an expected time, and a further check is made to ensure that the total price (TP) does not exceed the transaction limit (TL).

Steps 10 – 11: After the verification of PI, the money is deducted from the customer's account. The MNO creates a payment result PR for this transaction. The PR includes the transaction number (TN), payment information and date/time of completed transaction, plus the MNO signature.

Steps 12 – 14: The shop POS verifies the signature on PR using its pre-stored MNO public key (PK_{MNO}). It then checks for the correct payment amount within OI. The POS then displays the transaction result on its screen and prints an itemised billing receipt (on paper). The customer phone also receives PR and then independently verifies and displays the transaction result. The

same PR are expected to be shown on the shop POS and the customer phone as the final step in the transaction.

8.3 PRELIMINARY ANALYSIS

8.3.1 Attack Scenarios

The protocol has been considered with respect to a number of attack scenarios which are outlined in this section. Note that **RP** and **PP** are used to indicate **registration phase** and **payment phase** respectively.

1. (RP) The customer could present a stolen CDC card during registration however the user PIN challenge would prevent this from being useful. An invalidated or expired CDC would also be detected by the MNO.

2. (RP) The use of the phone as a PIN entry device could create a vulnerability if the code could be tampered with, however the integrity of the phone application could be secured via the cryptographic functionality of the SIM card.

3. (RP) If the CDC to phone link could be eavesdropped during a normal registration then an attacker may attempt to discover the CDC PIN from the exchanged messages. Registration is intended to happen in a trusted environment although this cannot be completely guaranteed and the likelihood of attack increases if the CDC evolves to a contactless interface.

Therefore, the protocol protects the transmitted PIN via encryption with (PK_{CDC}).

4. (RP) A dishonest customer could take a copy of the legitimate EC and Cer_{EC} and store in a second phone, however this should be of limited use as the original phone's SE (rather than that of the second phone) is bound within the credentials.

5. (PP) A dishonest customer or shop-keeper might attempt to send captured transaction credentials to try and charge purchases to another account, however the signature on new payment information will not be correct and the timestamp will be invalid on an old payment signature.

6. (PP) During an m-payment transaction a customer or shop-keeper might attempt to change the order information and correct payment, however this information is checked visually as well as within the transaction protocol.

7. (PP) It is unlikely that the MNO would attempt fraud due to the existing trust relationship with its customers; however customers would have some protection as legitimate transactions are required to be associated with signed payment information. This assumes that the SK_{SE} only exists within the SIM-SE.

8.3.2 Advantages and Disadvantages of the CDC Mobile Payment Scheme

In this section We weigh up some of the more general advantages and disadvantages of our proposed payment system.

Advantages: The benefits of the proposed protocol/system are listed below.

1. The customer NFC phone has an endorsed transaction credential (i.e. EC) stored in the SE-SIM, which is backed by the strong registration processes of the government ID card that has national recognition.

2. It is unnecessary for shops to be fitted with multiple proprietary MNO systems as the proposed solution offers flexible multi-MNOs service to customers.

3. Pre-storage of secret keys within the SE-SIM and the use of public key infrastructure minimise key distribution worries, and customer signatures ensure the authenticity and consent of purchase (i.e. non-repudiation).

4. Payment information (PI) is protected from being manipulated by the shop POS.

5. Customers do not need to bring additional ID or payment cards as the endorsed registration means that the handset can prove its authenticity and also that of the customer (if the transaction PIN option is used).

6. In general the solution offers a more reliant and widely recognised user

registration process for mobile phone access to services.

Disadvantages: As well as the advantages mentioned above, there are also potential weaknesses that need further discussion.

1. With the current style of CDC card, an external contact smart card reader or a cradle is needed during endorsed registration. This is likely to limit registration to a trusted environment such as an MNO shop or government office, although it is probable that a contactless CDC interface will eventually be supported.

2. The payment process has been presented as on-line, although it is known that there are arguments for off-line support [174]. The endorsed credentials (which are at the core of the proposal) are considered equally valid for off-line use although there would be greater reliance on the attack resistance and integrity of the POS units. The credentials could also be used in a different kind of on-line transaction in which the customer scans his own purchases and transacts directly with the MNO over the cellular network.

3. A customer's MSISDN (phone number) is sent back in clear to the MNO for customer identification via the shop POS during a payment transaction. Although, phone numbers are not regarded as the most confidential of information when compared to secret keys for example, there is still

a privacy concern that phone numbers could be linked with customer purchasing habits.

4. The speed and ease-of-use of a transaction system will determine whether it is successful. The proposed solution requires a number of cryptographic processes including PKI functions, which may stretch the capabilities of limited resource devices such as security elements and mobile phones. A detailed performance analysis is planned as follow-on work.

5. The protocol uses PKI key-pairs for both encryption and signing purposes. Strictly speaking this does not follow best practice advice of using a key-pair for one purpose only, however this is also true of other major and widespread solutions such as credit card EMV chip and PIN transactions. Further key-pairs could be added, although this may have a practical impact on key storage and management.

6. We need modifications to CDC, since such a m-payment application is not built into in the existing CDC card, which would require further government approval for installation on a government controlled platform.

8.4 Conclusion

In this chapter, we proposed the binding of NFC mobile phone security technologies with the user identity security of the CDC card that is backed by a strong user registration process. The binding is achieved by an endorsed reg-

istration phase that cryptographically binds the PKI credentials of the CDC card and NFC phone in a way that is then nationally recognised.

The credentials can then be used for in-store payment transactions to provide authentication, integrity and non repudiation, and without the user needing to carry any payment or ID cards. The solution, which is applicable to multiple MNOs, has a number of interesting features, although the feasibility of implementation and associated performance required investigation. The practical work to investigate these issues is described in the following chapter.

Chapter 9

Prototype Implementation of the CDC Scheme

Contents

This chapter provides a simple proof-of-concept practical demonstration of the CDC m-payment scheme in Chapter 8.

9.1 Introduction

In Chapter 8, detailed descriptions of the protocols and architecture for the proposed CDC m-payment scheme were provided. Recall that a goal of the scheme is to exploit existing technologies such as a government PKI system, the 3G network and the NFC enabled contactless communication equipped within the mobile handset. Several entities are involved in this scheme: **the Mobile Network Operator (MNO), the Governement Certificate Authority (GCA), the shop Point-Of-Sale (POS) terminal, a user's NFC-enable handset, and user's CDC card (eID card).**

This m-payment scheme was designed to leverage from the eID card, which is conventionally used for authentication purposes for citizens to interact with government online services e.g. income tax filing. The government issued eID card's national recognition, legitimacy and the general-public trust are strong advantages that can be used in a wider range of services. The use of the GPKI endorsed eID card in cooperation with the handset concept can be utilised on diverse applications, although in this thesis, a m-payment scheme is taken as an example to show advantages of the combination of the NFC-enabled handset and the CDC card.

In proposing any new protocol, and especially one that directly interacts with the user it is necessary to show that that it is feasible to implement using realistic technology and that the performance will be sufficient. Therefore

a proof-of-concept implementation is presented in this chapter. The implementation and particularly the public key cryptographical calculations on the resource limited device (i.e. the handset) within a user acceptable time has been demonstrated as feasible.

9.2 System Overview

In the prototype implementation the main focus was on the interaction between the MNO and the user's handset (in the registration phase) and the shop POS terminal and the user's handset (in the payment phase). All backend processes for the user phone to be between the POS and the MNO were considered to be true/succesful. Two Nokia6131 NFC handsets were used, one acted as the user's handset, and the other emulated the POS. The whole payment scheme consists of two phases: the "registration phase" and the "payment phase" as shown in Figures 9.1 and 9.2.

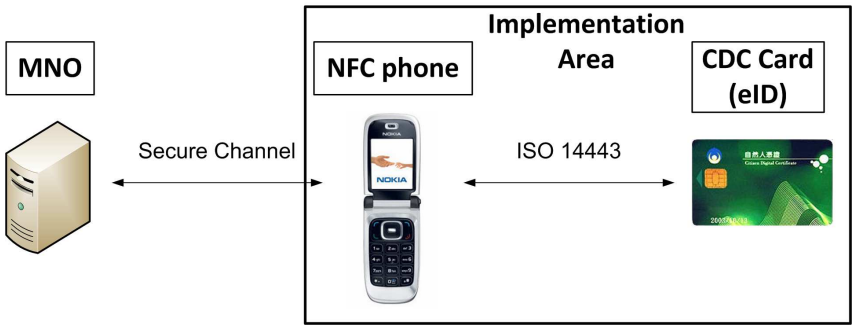


Figure 9.1: Implementation - Registration Phase

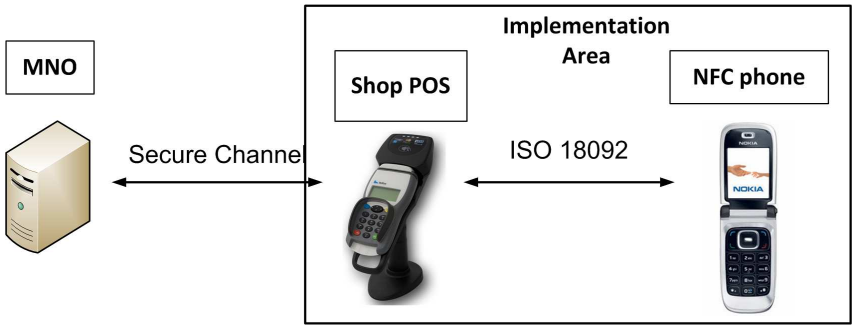


Figure 9.2: Implementation - Payment Phase

* Please note that the card and reader modes of ISO14443 standard are used in the registration phase; and the P2P mode of the standard ISO18092 is used in the payment phase.

9.3 Platform and Tools

The system development tools used are listed below:

– Eclipse SDK 3.4.2 win32 Ganymede

– SUN JAVA wireless toolkit 2.5.2

– Nokia 6131 NFC SDK 1.1

– JDK 6u25 windows i586

– NXP JCOP Plugins Generic3.2.8 Target1.2.9

- The Java phone applications MIDlets were developed using the Eclipse Integrated Development Environment (IDE).
- The SUN JAVA wireless toolkit provided the important "Security and Trust Services API (SATSA)(JSR 177) for J2ME "
- the Nokia 6131 Software Development Kit (SDK) provided "contactless communication API (JSR-257) and contactless communication API Extensions for NFC".
- The NXP JCOP Plugins were used for development of Java smartcard applications (Applets).

9.4 Nokia 6131

The demonstration handset used for this scheme was the Nokia 6131, which was a Nokia S40 phone with NFC support. A Nokia 6131 has an embedded Secure Element (SE). Its architecture is shown in Figure 9.4.

Figure 9.3: Nokia 6131 NFC handset.

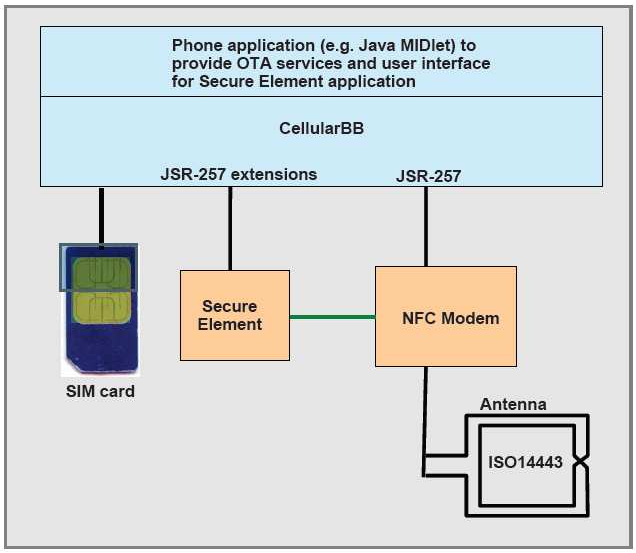


Figure 9.4: Nokia 6131 NFC architecture. [167]

The Nokia 6131 NFC device provides the following card emulations / target modes:

– ISO 14443-4A/ISO7816-4 Smart Card (Global Platform-based Java Smart Card)

– Mifare Standard 4k

– NFCIP-1 Target

The target types values supported by JSR-257[170] implemented in Nokia 6131:

– TargetType.ISO14443_CARD for ISO 14443-4 compliant smart cards accessed using APDU commands.

– TargetType.NDEF_TAG for a tag that contains NFC Forum formatted data.

– TargetType.RFID_TAG for general RFID tags.

The SE in Nokia6131 consists of a chip with a Java Card area and Mifare 4K area (which also behaves as Mifare 1k) for tag emulation. With respect to Java applications the memory size of the SE is approximately 65 kbytes. The overall memory size is 72kbytes, however some space is required for product specific applications and the Mifare 4k area. The JSR 257 also provides an API extension for NFC peer to peer connections. The com.nokia.nfc.p2p package contains the NFCIPConnection interface for communication between two NFCIP devices. [169]

The possible external passive tags by a Nokia 6131 for reading and writing include: [169]

– MIFARE STANDARD 1K and 4K

– MIFARE Ultralight

– MIFARE Desfire

– Sony FeliCa

– Innovision Topaz and Jewel (read only)

– Cards based on ISO 14443-4 (with or without ISO 7816-4)

– NFCIP-1 Initiator

For the practical implementation of the m-payment system , the ISO 14443-4 standard was selected.

9.5 Practical Implementation

The proposed protocol relies on a number of cryptographic primitives. These included an RSA public key encryption and signature scheme with 1024 bits key, the SHA-1 hash function, a 3DES based Message Authentication function plus associated credentials such as X.509 certificates.

*Note that in the real practice the CDC card uses an RSA 2048 bits keys.

Note that it is recognised that to comply with best-practice today on would suggest a 2048 bit RSA key and a SHA-256, however this was thought beyond the capabilities of early resource constrained NFC devices. Considering that a design goal was to make best usage of existing technologies, evaluation with the older primitives was thought justified at the time of the experiments. Newer NFC phones would be expected to have better performance, sufficient to comply with information security best practices.

Before a citizen can make use of the m-payment protocol it is necessary to go through a registration phase in which the citizens CDC credentials and mobile credentials are securely bound together.

9.5.1 Registration Phase

Before a citizen can make use of the m-payment protocol it is necessary to go through a registration phase in which the citizens CDC credentials and mobile

credentials are securely bound together.

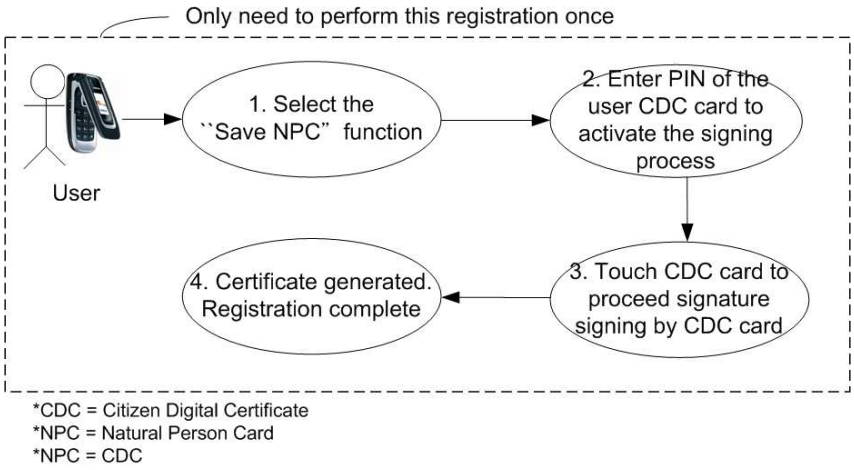


Figure 9.5: User action and phone display in registration phase.

Figure 9.5 presents the essential user action and the expected screen display on the user's handset when performing the registration. Note that the Natural Person Card (NPC) and the Citizen Digital Certificate (CDC) represent the same thing, the NPC is a term used by the general-public, whereas the CDC represents this in a more technical manner. Thus, on the phone display the NPC term was used, and the term, CDC, is used in most descriptions throughout this thesis. The implementation of this function would follow the steps shown in Figure 9.5.

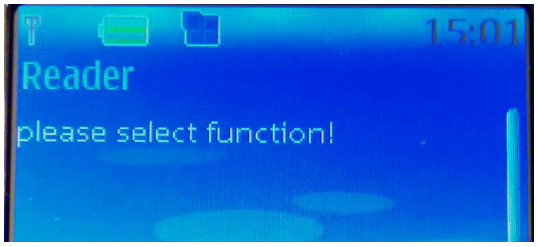


Figure 9.6: Application home page.

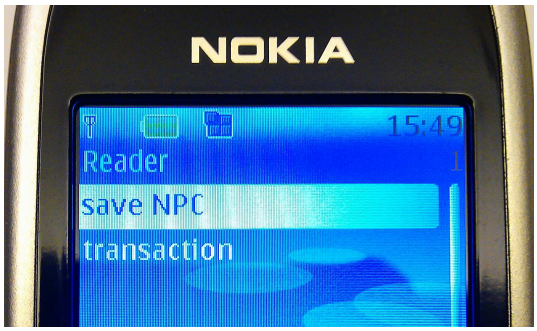


Figure 9.7: Function selection page.

In the design of this m-payment scheme, a service registration process is required in order to bind the user's identity, and the CDC card, to the user's SIM for the consequent purchasing action. Figure 9.6 is the welcome page for the phone application (Midlet prompting the user to choose one of the two functions in the display of Figure 9.7: "Save NPC[1]" and "Transaction"). In this registration phase, the first function is selected to save certificate endorsed by the user's own CDC/NPC card.

Please note that to simplify the implementation on the GUI display that most of the commands would need to be opened/found by pressing the "options" button bottom left of the screen.

[1]Natural Person Certificate

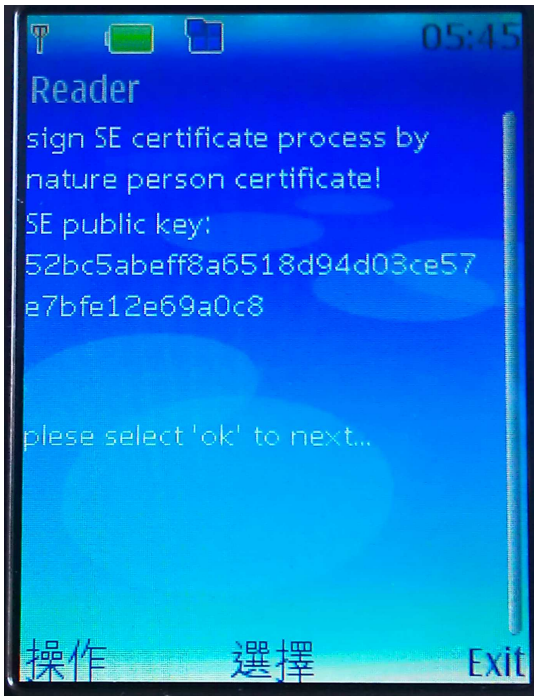


Figure 9.8: Sign SE page.

SE public key: 52bc5abeff8a6518d94d03ce57e7bfe12e69a0c8

Since an assumption of "all return messages are true/successful from the MNO to the user phone" was made for experiments, the return values and information from the MNO were pre-stored in the internal SE of the handset. Figure 9.8 shows the public key of the SE that was saved in the handset already and ready to be sent/signed by the CDC card once the user has confirmed the action.

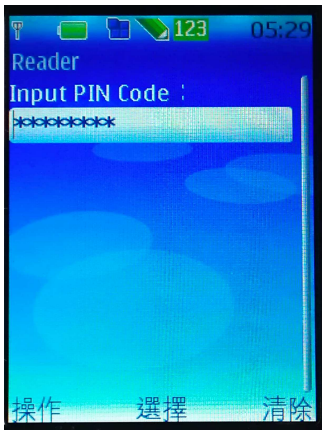
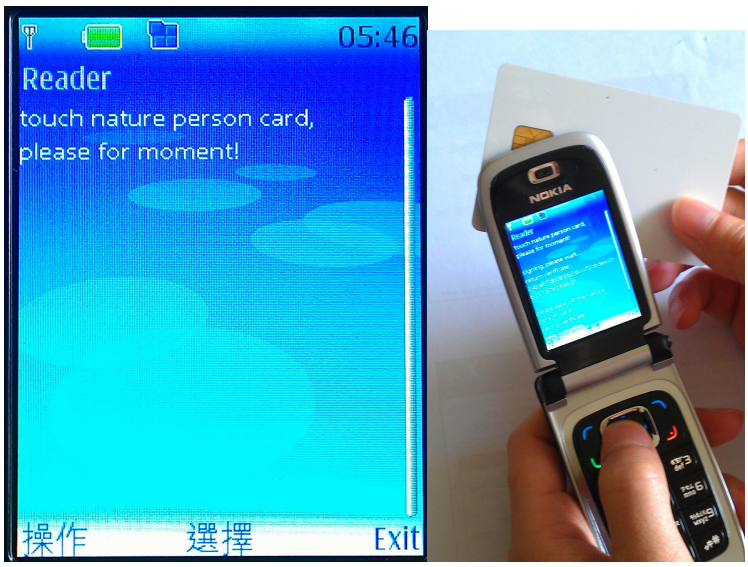


Figure 9.9: User's PIN input page.

User's PIN is required here to activate the endorsed signing process.



(a) (b)

Figure 9.10: CDC card interact with user's handset page

Figure 9.10a indicates the handset is ready and waiting to interact with the CDC card. The user just needs to put the CDC card and the phone next to each other to start the signing process. Bear in mind that the reader/writer capability of Nokia 6131 flip-phone is enabled only when the handset is open and

the backlight is on, since the antenna is built on the top part of the flip cover of the phone that is where to touch/interact with the external devices/tokens (as shown in Figure 9.10b).

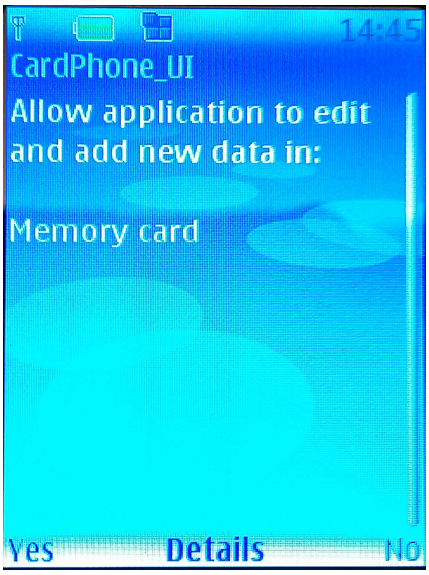


Figure 9.11: Save in memory card page.

Since the processes between the MNO and the shop POS are not part of the experiment at this stage, step12 to step15 of the protocol stated in Chapter 8 are skipped in this practical design. Therefore, for the simplicity of implementation, the certificate is replaced by the Endorsed Credential (EC) (a credential signed by the CDC card) in this design.

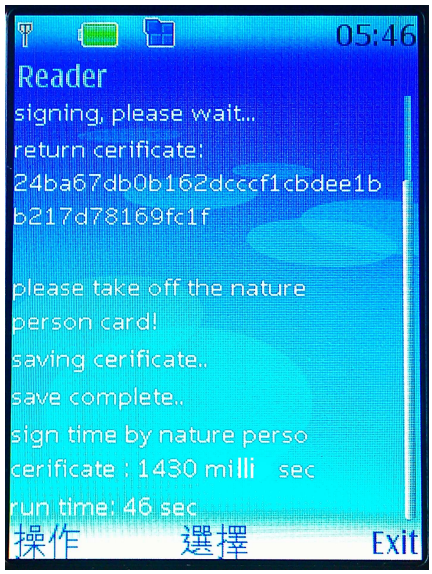


Figure 9.12: Saving certificate page.

return certificate: 24ba67db0b162dcccf1cbdee1bb217d78169fc1f

A return certificate (it is actually the EC) is displayed on the screen to prove the success of the signature signing. "Save complete" message is shown to state the certificate is successfully saved in the memory card. The **total executive time for the signature signing** is **1430 milliseconds** and the **total executive time for the this function**, including the waiting time for user to put the phone and the CDC card close to each other, is **46 seconds**.

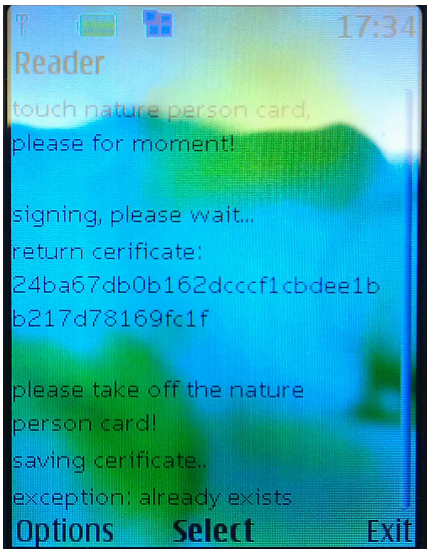


Figure 9.13: Certificate existed exception page.

exception: already exists

Figure 9.13 shows an error message displays if a certificate has already existed in the phone. Basically only one certificate is needed to execute the payment transactions which is explained in the next phase.

9.5.2 Payment Transaction Phase

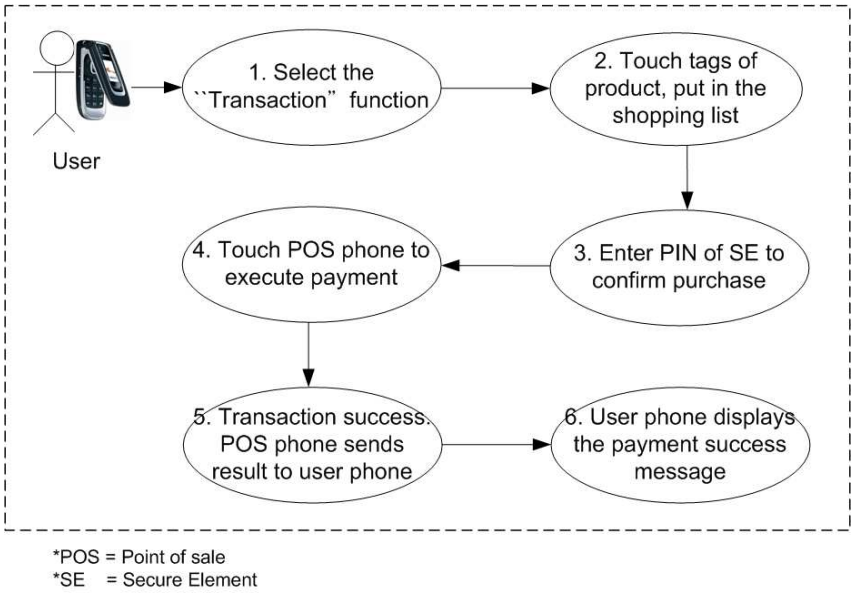
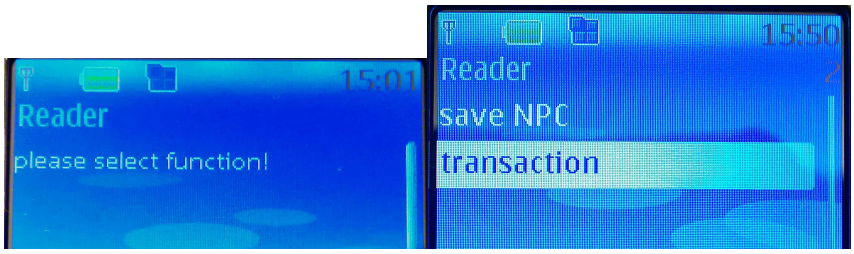


Figure 9.14: User manual and phone display in payment phase.

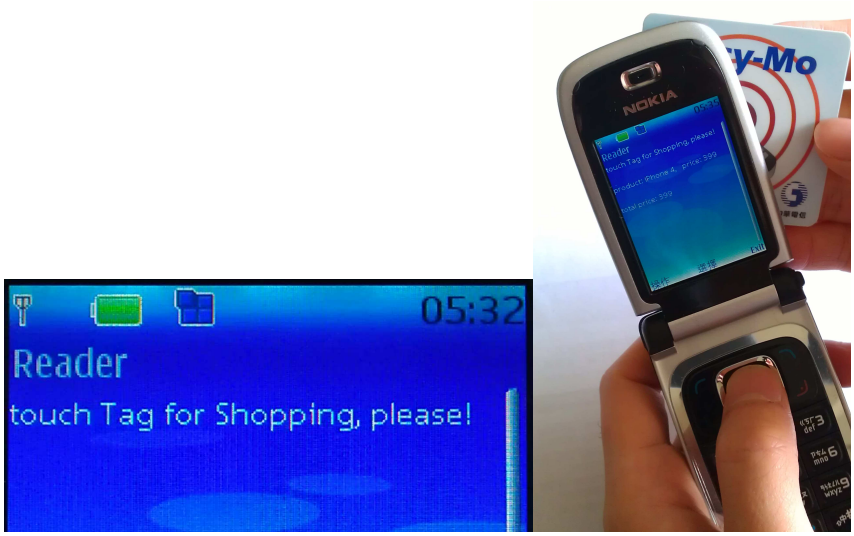
In Figure 9.14 displays the flow for the user to execute the payment transaction function after the successful installation of the certificate in the registration phase. Basically user would hold user's phone to touch with what they want to purchase first then head to the POS phone to check out.



(a) (b)

Figure 9.15: (a) Application home page. (b) Function selection page.

The payment function has to be selected from the application home page.



(a) (b)

Figure 9.16: (a) Product tags reading page. (b) Product information display page.

After the selection of the "transaction", the user is allowed to use the phone to interact/touch the tag on each product to extract the information such as the name, cost, product code and etc.

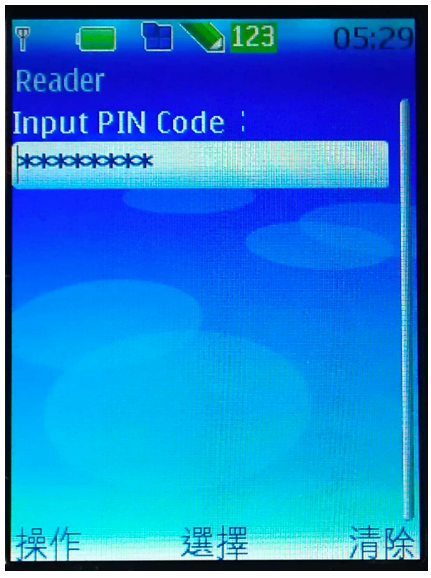


Figure 9.17: User's PIN input page.

Again, the input of the user password is required to confirm the purchase action and to prevent misuse and eavesdropping attacks.

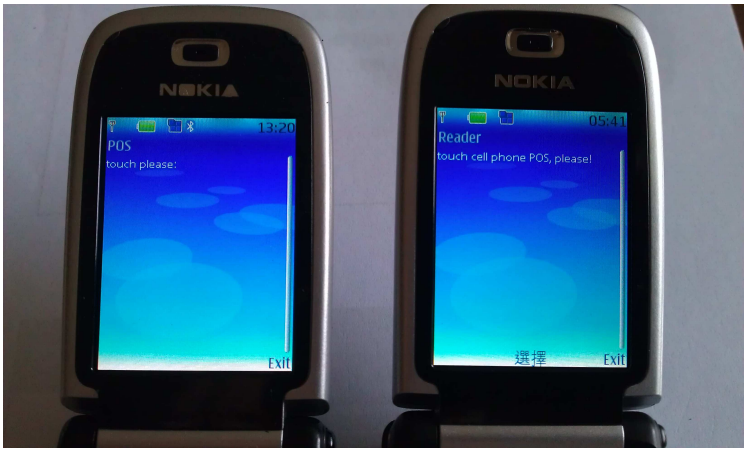
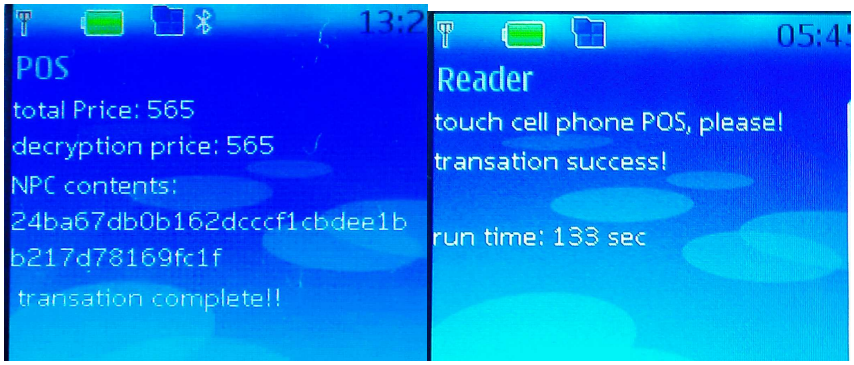


Figure 9.18: (Left): POS phone, ready to interact with the user's phone for payment. (Right): User's phone, ready to check out.

Figure 9.19: Interaction between POS phone and user's phone for payment transaction.

Figure 9.18 presents the state for both the POS phone and the user phone before the payment transaction interaction (via NFC peer-to-peer mode) between each other. Figure 9.19 shows how both phones interact with each other

at the flip cover of the Nokia 6131 phone.



(a) (b)

Figure 9.20: (a) POS phone transaction complete page. (b) User's phone transaction success page.

The transaction result are shown on both of the phones in Figure 9.20. The display of the certificate value in Figure 9.20a is equivalent to the original certificate in Figure 9.12, which means the POS phone successfully verified, by the user's/SE's public key, the received data sent from the user phone. In total, the POS phone retrieved the certificate and the product information for check-out. The received certificate was originally signed by the user's/SE's private key, and sent to POS phone for authentication and identification for the payment service.

After the certificate check and the money deduction from the user's account within the MNO (assuming they are all successfully done and returned with a transaction result), the transaction result would be displayed on both the POS phone and user phone to inform the completion of the transaction.

On the screen display in Figure 9.20b 133 seconds was shown that indicates

the total time span used for the payment transaction, including the waiting time for the user phone to touch the POS phone.

9.6 Evaluation

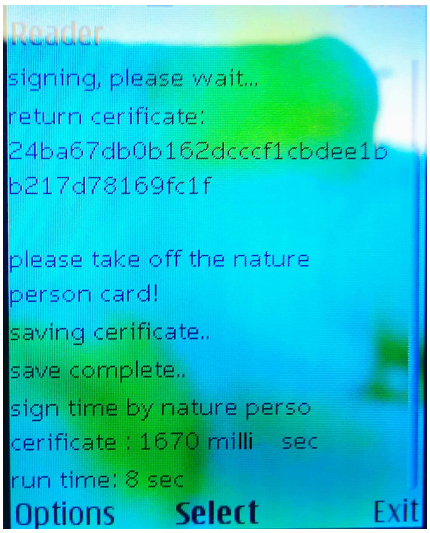


Figure 9.21: Certificate Signing Runtime.

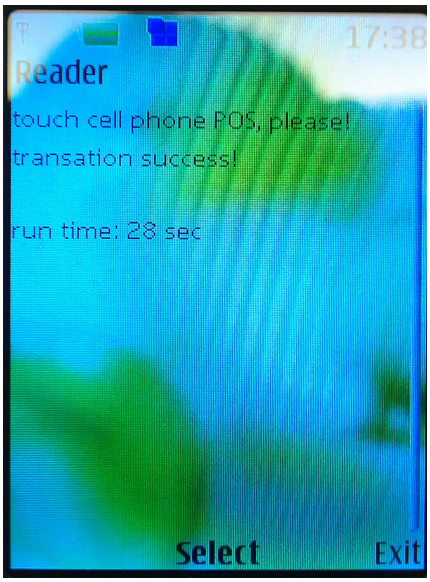


Figure 9.22: Total execution time of the application display page.

Figure 9.21 and 9.22 present time spans for the customer to carry out both registration and payment processes in a timely manner. The main goal of this simple demo is to show the execution time of payment procedures is likely to be acceptable to customers.

Please note that a proprietary PKI card was used; and hardware cryptographic calculations were offered by the PKI card and the SE. In the beginning RSA2048 was used/implemented, but the Nokia6131 SE was unable to interact with the PKI card generating RSA1024 signature.

A website offering JavaCard's algorithms and supporting tests on Nokia 6131 NFC phones [171], indicates the Nokia6131 SE does not support RSA2048 signature (this meets the result as mentioned earlier). Moreover, for message digest algorithms only SHA1, MD5 and RIPEMD160 are supported.

	RSA1024 Signature (millisec):	Registration completed (sec):	Payment completed (sec):
1	1454	8	23
2	1867	7	15
3	1493	6	11
4	1475	6	13
5	1566	8	12
6	1438	6	12
7	1444	6	11
8	1472	7	12
9	1518	8	14
10	1509	6	13
11	1620	7	12
12	1476	6	9
13	1529	6	8
14	1420	5	11
15	1470	5	9
16	1377	5	11
17	1480	7	12
18	1614	7	11
19	1366	5	13
20	1448	6	8
Average	**1501.8**	**6.35**	**12**

Figure 9.23: Stats of time span in registration and payment procedures

In Figure 9.23 a table of Statistics with running 20 times for each registration and payment procedures. The average time for forming a signature is 1501.8 milliseconds; and for completing the registration procedure takes around 6.35 seconds. A line chart regarding to the RSA1024 signature running 20 times is displayed in Figure 9.24.

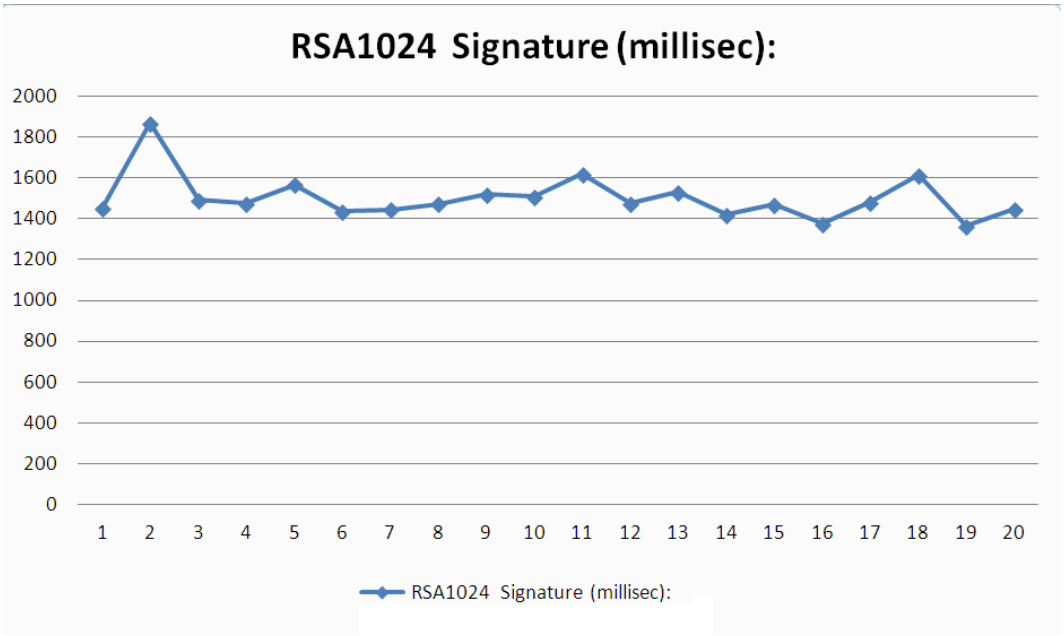


Figure 9.24: Statistics of performing RSA1024 Signature x20

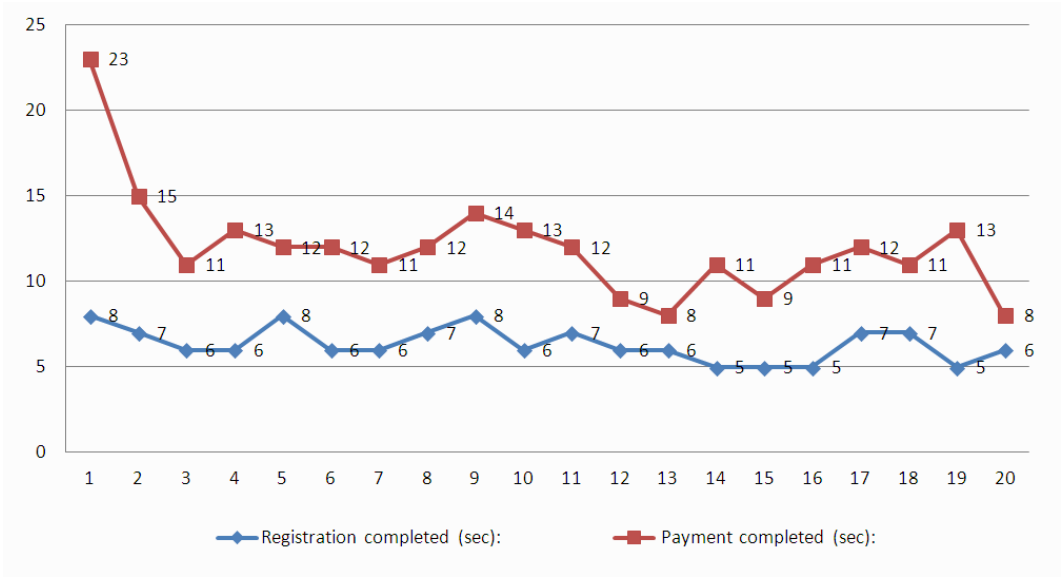


Figure 9.25: Statistics of performing registration and payment procedures x20

Apart from generating the signature, other steps like retrieving the SE public key, selecting file, inputting PIN and generating/saving a hashed credential (acts as a certificate in the protocol) used up the time for registration.

The time spent for the payment procedure is almost double of it takes during the registration. Its average time span is 12 seconds (including the user control). This includes the time of retrieving the certificate, encryption/decryption of the binding credential sent to the POS.

In conclusion, the Nokia6131 provided a constrained resource NFC mobile environment, an SE capable of supporting limited, but usable cryptographical algorithms. The major information required for this payment application was secured by RSA1024 signature and encryption/decryption payloads were smaller than 1Kbyte, resulting in tolerable an overall runtimes for the each registration and payment phases. Considering that more modern NFC mobile devices have greater performance than the Nokia 6131, both the speed of transactions and strength of cryptographic functions may be considerably improved, suggesting that the proposed protocols are practically feasible.

Chapter 10

Overall Conclusion

Contents

This chapter summarises the primary contribution of this thesis and concludes with suggestions for further work.

10.1 Conclusion

A major goal of the research described in this thesis was to investigate the practical and secure use of short-range NFC technology in conjunction with existing and well proven long-range wireless technologies, and in particular GSM and 3G cellular systems with their well proven security solutions. A guiding principle was to maximise the re-use of legacy wireless systems in combination with the newer NFC technology to provide a practical route and options, for improved user experience and efficiency, and yet offering strong security protection. In short, complementary advantages from each technology generated a solution with strength that was more than the sum of its parts.

This thesis records the progression of the research and how the associated legacy systems considered for use with NFC started with GSM then moved to 3G and finally incorporated a citizen ID card systems and associated. PKI infrastructure. These were also clear stages that were associated with conference publications [173][174][175]. They described how the core system security mechanisms migrated from symmetric only to also include asymmetric cryptographical security protection and the underlying algorithms, key lengths and protocols offered by legacy systems also improved Tradeoffs in algorithm complexity, key and data size, processing speed and usability are important for the success of the system and further improvements are expected as smartphone capabilities continue to advance.

However, by focusing on technology alone there is a danger that a closed and proprietary system results that is not accepted or trusted by third parties. The initial stages of the research focused on solutions that were completely MNO centric, but it was recognized that an independent trust hierarchy with strong user registration procedures would complement the MNO approach, permitting more significant and trusted transactions. As a result the final stage of the research combined the government CDC credential with the NFC and MNO solution.

In summary the resulting m-payment schemes proposed in this thesis have achieved all met their essential security requirements such as providing: user authentication, privacy, key management, data integrity and confidentiality, and digital signatures / non-repudiation (for the CDC scheme especially). The proposed solutions are not equally strong, however that is to be expected when re-using legacy systems and technology, with the minimum of disruption to the user.

In the final proposals the combination of PKI trust hierarchy, cryptography, anddigital signatures with NFC technology can protect high value transactions within a secure mobile communication environment, and so may handle applications that require higher security levels. Core to this was the PKI-based credential binding concept using the Secure Element (SE) to keep the user's unique private key for the consent of user action and data protection.

10.1 Conclusion

Although the research, kept to the goal of re-using technology and functionality as much as possible, any new protocol will have some changes and so it is reasonable to question the performance impact of the proposal. Therefore within the research we have evaluated the performance of the implementation by measuring the processing time, the code size and the size of the produced signature records. The result has shown that it is possible to process signatures and certificates in mobile devices and that signature records can be put on the SE and that overall the user would not be significantly delayed or inconvenienced.

A conventional PKI system requires a responsible party to be responsible for managing certificates.

The proposed government endorsed m-payment scheme is Mobile Network Operator (MNO) centric, which means the certificate management jobs such as certificate registration , certificate/identity verification, Certificate Revocation List (CRL) update and etc. can be apportioned to the mature MNO infrastructure. A potential drawback of such as system is that the MNO may not be universally trusted making transactions difficult for parties on different netw orks. In our proposed scheme, users are allowed to enjoy convenient cross-network

NFC services without back office barriers at the backend for the MNOs. This is possible because of the inclusion of an existing and nationally recognised

trust mechanism via the national CDC credential. The associate transactions would have a strong binding to the user identity (established by rigorous national registration processes) and so applications of high significance could be supported. The NFC phone could become the preferred identity credential and/or terminal as people may prefer to keep the real national ID card (as the master reference) and use the rich phone functionality instead. In which case MNOs may gain valuable insight into user behaviour when engaged in a wider variatey of transactions.

The success of such a proposal is of course dependent not only on security, but of the user experience, of the entire transaction. Some experiments, relating to an m-payment transaction were conducted, to investigate this aspect. Encouragingly, in a practical demonstration, it was shown the total time for completing a payment transaction was within an acceptable time frame for use by the general public.

The practical binding of NFC mobile capabilities with strong user identity could lead to many possible applications. For example an unbound phone/user may have very restricted payment limits, whereas the ID bound mobile could have much greater purchasing power. It might also be used in an identification area, for example an alcohol/cigarettes vending machine might verify the age of the user as part of the payment process.There are also applications to identification and payment in roaming scenarios. For example a foreigner can bind part of their ID information with the local MNO/SIM, and be accepted to use

value added the local mobile contactless services and to get special offers and discounts (advertising, sightseeing and shopping recommendations) or perhaps to execute money transfers.

There are many ways this research could be taken further in future, however two in particular will be noted here, as they would have been investigated further had more time been available. The first proposal still relates to m-payment via NFC phone; however it expands into the wider shopping experience. In the not-too-distant future it is reasonable to predict that items in shops and supermarkets will be RFID tagged and that the radio aspects of NFC technology will evolve to be compatible with all such tags. Therefore the proposed solution could be extended to "shopping" by scanning the required items prior to adding to the shopping bag. On leaving the shop the phone (either automatically or by touching a checkout tag) would calculate and make payment. Because of the strong ID binding payments of several £100s could be made and should fraud be suspected the strong binding with the end user could be used to identify the user and take appropriate action.

The second proposal is to use ICAO compatible passports with RFID chips as an alternative to the CDC card. Experiments have shown some practical aspects of this to be feasible and it could lead to a more internationally recognized solution than the CDC card.

Chapter 11

Addendum

Contents

The following clarifications were provided on the draft version of the thesis and are included here at the request of the examiners.

11.1 Additional Information on the 2G Protocol

The 2G protocol was a stepping stone towards the 3G version. It is inferior to the 3G version and has a number of security limitations arising from practical restrictions and re-use; putting more reliance on the phone. It is included to show the motivation and progression towards improved solutions.

Implementation Assumptions:

- The phone can support custom applications in the form of Java MidLets.
- The Midlets have access to a basic Crypto API.
- The phone can only be temporarily trusted with session keys for encryption/decryption and integrity checking.
- Existing SIM application crypto functions are used for authentication and key generation; the functions can be slightly modified, but no extra crypto functions added
- Normal communications should be disabled during a transaction

11.1.1 Encryption/Decryption and Integrity Checks

The simplest phone Midlet API supported a DES/3DES block cipher/MAC, and hash functions, SHA-1 and MD5. For this protocol DES/3DES encryption/MAC and SHA-1 were selected. It was recognised that these would no

longer comply with best-practice recommendations, however Kc (used in the protocol) has a maximum of only 64 bits and some older implementations use only 54 of these bits. The 2G communications algorithms were not available via the phone APIs and the encryption/decryption is thought likely to be a hardware implementation dedicated to radio communications purposes. Kc and S are not used for their traditional purposes, so normal communication is disrupted by a transaction.

In steps 10 to 11 of Fig 6.1 a DES/3DES CBC-MAC is used to check that the random challenge originated from a valid source, and Kc is used. A DES CBC-MAC only uses 56 key bits whereas the Kc could have up to 64 bits and so an alternative approach is to expand the key and used it in a 2-key 3DES mode; however the improvement is marginal as 64 bits is still "small" by best-practice guidelines.

The key ($Kc1$) that is derived from SHA-1 takes the LSBs of the hash output (recognising that the entropy of the output key is no better than that of the input). Encryption/decryption between the entities (steps 15.1 through 22) is based on DES (but 2-key 3DES is possible as mentioned earlier). Where the message size is larger than 64 bits the encryption/decryption algorithms are used in CBC mode.

The Payment Information (PI) message is subsequently encrypted (to prevent eavesdropping) between the phone and the POS/Gateway using $Kc1$. The

message includes an integrity check value computed over the fixed length message $(PI, S, IMSI)$ for use by the gateway; the SIM has no MAC capability and so the calculation has to be done in the phone. DES (or 2-key 3DES) CBC-MAC is used. which is equivalent to a fixed message encryption, however the correct terminology is $MAC_{Kc}(PI, S, IMSI)$ and not $E_{Kc}(PI, S, IMSI)$.

There is also an application level check performed at the POS for the benefit of the Merchant/Cashier to be sure the correct order and value is being processes. There is a final MAC_{Kp} on the message sent at step 26 of Fig 6.1 for verification by the POS/shop. Note that Kp does not have the size restrictions of Kc so could be made larger; although the system is only as strong as the weakest link.

11.2 Additional Information on the 3G Protocol

Implementation Assumptions:

- The phone can support custom applications in the form of Java MidLets.
- The Midlets have access to a basic Crypto API.
- The phone can only be temporarily trusted with session keys for encryption/decryption.
- Existing SIM application crypto functions are used for authentication, key generation and integrity checks; the functions can be slightly modi-

fied, but no extra crypto functions added.

- Normal communications should not be blocked during a transaction.

11.2.1 Encryption/Decryption, Verification and Integrity Checking

The available 3G phone Midlet API supported block ciphers 3DES and AES (which can also be used for CBC MACs). AES with a 128 bit key is recommended for phone/POS/gateway encryption/decryption, based on its security strength and convenient 128 bit block size. 3DES is also possible, but there are only enough key bits (easily obtainable from the SIM) to operate it in two key mode, which would be below best practice standards. The 3G communications algorithms were not available via the phone APIs and the encryption is thought likely to be a hardware implementation which should not be disrupted from its normal communications use.

The key used is $IK1$ which is generated by a call to the SIM's f4 function via the new SIM command "CRYP" (see definition below). Note that this extra key is only necessary because we want the phone to be able to communicate during a transactions so do not wish to re-use the CK or IK values.

The Payment Information (PI) is subsequently encrypted between the phone and the POS/Gateway.

11.2.2 Verification and Integrity Checking

At step 22 in Fig 7.1 the checking is done at the application level and visible to the merchant - basically checking that the Order Information (OI) is as expected. The message does require a SIM generated integrity check for use at step 24 (by the gateway). This was a challenge as the SIM is not normally used for general purpose message integrity check calculation (or verification).

The f4 function was chosen initially as it was accessible i.e. its output normally leaves the SIM as a result field and because it would have to be modified anyway to support the CRYP command. Its use was considered not to reveal the input key field, however its quality as a MAC function is unknown as it is intended for key generation.

The SIM does however include a function (f1) that should have suitable MAC properties as it was designed for MAC computation as part of the authentication process, although the f1 output does not normally leave the SIM as a result/output. Providing the f1 output is visible to the SIM application (and not hidden in low-level hardware/OS) then modifying the access to f1 as well as f4 (or indeed f2, 3 and 5) is not thought difficult, and the same CRYP command could be used with different parameters.

Therefore the protocol in Figure 7.1 could benefit from using f1 instead of f4 from steps 21 onwards and so the descriptive text on pages 141 to 143 and the analysis text on page 145 should be updated. Of course it would be possible

to implement any new algorithm in place of the current functions, but that would go against the goal of re-use and could require significant added testing and evaluation.

11.2.3 CRYP COMMAND

CRYP COMMAND

COMMAND	CLASS	INS	P1	p2	P3
CRYP	0x00	0x8F	FSELECT	FMode	FLENGTH

Valid Parameter Combinations

FSELECT	FMODE	FLENGTH	DATA (all fields 16 bytes)	Comment
0x01	0x00	0x20	Key‖Input1	f1 e.g. = f1(Key, Input) Note AMF and SQN = 0
0x01	0x01	0x10	Input	f1 e.g. = f1(K, Input) Note AMF and SQN = 0
0x04	0x00	0x20	Key‖Input	f4 e.g. = f4(Key, Input)
0x04	0x01	0x10	Input	f4 e.g. = f4(K, Input)

Response data

FSELECT	Bytes(s)	Description	Length
0x01	0x00 - 0x07	Output (normally MAC)	0x08
0x04	0x00 - 0x0F	Output (normally key)	0x10

Mode Usage: Mode 0x00 used at step 12 and 21 of Fig 7.1; Mode 0x01 used at step 29.2

11.3 Additional Information on the CDC Protocol

The PKI algorithm in CDC is RSA and so that is used for the protocol. The CDC key size is 2048 bits which again is the protocol recommendation, however the phone used for practical work could only support 1024 bits and so there was a compromise for testing.

In the registration phase, RSA is used for encryption/decryption (with suitable padding). In the transaction phase AES is used with the 128 bit MSK, partly because it is faster than RSA.

Bibliography

[1] Nokia NFC Background.
http://www.developer.nokia.com/Community/Wiki/images/c/cd/NFC_backgrounder.pdf?20071212114943

[2] NFC Forum. www.nfc-forum.org

[3] ECMA-340, "Near Field Communication Interface and Protocol - 1 (NFCIP-1)".

[4] ISO/IEC 18092, "Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1)".

[5] ETSI TS 102.190, "Near Field Communication (NFC) IP-1; Interface and Protocol (NFCIP-1)".
http://www.etsi.org/deliver/etsi_ts/102100_102199/102190/01.01.01_60/ts_102190v010101p.pdf

[6] ECMA-352, "Near Field Communication Interface and Protocol - 2 (NFCIP-2)".

[7] ISO/IEC 14443, "Identification cards - Contactless integrated circuit cards - Proximity cards".

[8] FeliCa. www.sony.net/Products/felica/.

[9] ISO/IEC 15693, "Identification cards - Contactless integrated circuit cards - Vicinity cards".

[10] ECMA-373, "Near Field Communication Wired Interface (NFC-WI)", 1st Edition, June 2006.

[11] Stolpan, "Near Field Communication", 16th IST Mobile Summit 2007, Budapest, Hungary.
http://www.stolpan.com/uploadfiles/1_Mobilesummit2007_workshop.pdf

[12] NFC Forum, "Near Field Communication Technology and the Road Ahead", NFC Forum Press and Analyst Briefing Slides, 2007.
http://www.nfc-forum.org/resources/member_videos/NFC_Forum_14Feb07_Press_and_Analyst_Briefing_Slides.pdf

[13] Nokia, "Introduction to NFC", version 1.0, April 2011.
http://www.adafruit.com/datasheets/Introduction_to_NFC_v1_0_en.pdf

[14] Frank Graeber, "NFC is the double click in the internet of the things", 2007.
http://www.rfid-systech.eu/20070612_1A_1235_Graeber_NFCIsTheDoubleClickInTheInternetOfThings.pdf

[15] Steffen Steinmeier, NXP, "The Near Field Communication (NFC) Technology Roadmap", 2006.

[16] Jeff Fonseca, NXP, "NFC Market Update and Technology Overview"
http://www.sourcemediaconferences.com/CTST09/PDF09/new/fonseca.pdf

[17] NFC Forum, "Smart Poster Record Type Definition, Technical Specification, ver.1.0",Jul. 2006.
http://www.rfidconsultation.eu/docs/ficheiros/Graber.pdf

[18] PHILIPS, "S2C Interface for NFC", Adding a general purpose interface between NFC and Secure IC to Secure NFC, survey V1.0, 2005.
http://www.classic.nxp.com/acrobat_download2/other/identification/S2C_survey_10.pdf

[19] vCard Overview.
http://www.imc.org/pdi/vcardoverview.html

[20] SmartMX Secure Chips.
http://www.tw.nxp.com/news/news-archive/2009/500-million-smartmx.html

[21] SmartMX Contact Interface Controllers.
http://www.nxp.com/products/identification_and_security/smart_card_ics/smartmx_contact_interface_controllers/

[22] Consult Hyperion, "Soft and hard SIMs", 2010.
http://www.chyp.com/media/blog-entry/soft-and-hard-sims

[23] Over-The-Air (OTA) technology.
http://www.3gpp.org/ftp/tsg_sa/wg3_security/TSGS3_30_Povoa/Docs/PDF/S3-030534.pdf

[24] 3GPP TS 23.048: "Security mechanisms for the (U)SIM application toolkit".

[25] DeviceFidelity. "A NFC microSD Specialist".
http://www.devifi.com/index.html

[26] Spring Card System.
http://www.springcard.com/products/index.php

[27] Moneto. "Moneto Prepaid Master Card". http://www.moneto.me/

[28] Androidincanada, "Moneto Has Those NFC SD Cards Ready".
http://www.androidincanada.ca/news/moneto-has-those-nfc-sd-cards-ready/

[29] Techmagister, "Moneto NFC SD Card Gives NFC Functionality To Your Non-NFC Gadget".
http://techmagister.com/2012/01/14/
\moneto-nfc-sd-card-gives-nfc-functionality-to-your-non-nfc-gadget/

[30] "Moneto NFC microSD to bring contactless features to any Android phone".
http://www.engadget.com/2012/01/11/
moneto-nfc-microsd-contactless-payment-Android-iPhone/

[31] S. Clark, OTI introduces Copni NFC SIM+antenna device, January 2011.
http://www.nfcworld.com/2011/01/05/35541/oti-copni-nfc-sim-plus-antenna/

[32] NFC Times, Taiwan: Bank Tries Out MicroSDs in Full NFC Phones.
http://nfctimes.com/project/taiwan-bank-tries-out-microsds-full-nfc-phones

[33] ETSI TS 102 613: "Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer chasracteristics".

[34] ETSI TS 102 221: "Smart Cards; UICC - Terminal interface, Physical and logical characteristics".

[35] Gemalto and NXP Join Forces to Boost Mobile NFC Solutions Deployment Around the Globe.
http://www.gemalto.com/press/archives/2007/08-21-2007-nxp_gto.pdf

[36] NFC (Near Field Communication) Technology and Applications.
http://www.gs1tw.org/twct/gs1w/download/7.pdf

[37] Reseach of NFC SIM solutions.
http://read.pudn.com/downloads94/doc/374050/sim.pdf

[38] Dr. Klaus Vedder , ETSI, "The UICC, The Security Platform for Value Added Services".
http://docbox.etsi.org/workshop/2009/200901_SECURITYWORKSHOP/G&D_
Vedder_UICC_SecurityPlatformforValueAddedServices.pdf

[39] NFC Forum, "Smart Poster Record Type Definition, Technical Specification", NFCForum SmartPoster RTD 1.0.

[40] Philips Semiconductors, "Near Field Communication RFID Workshop", 2006.
http://www.rfidconsultation.eu/docs/ficheiros/Graber.pdf

[41] GSMA, "Requirements for Single Wire Protocol NFC Handsets", 2008.
http://www.gsmworld.com/documents/reqs_swp_nfc_handsets_v2.pdf

[42] G. Romen, Nokia, NFC Forum,"NFC and the NFC Forum".
http://www.nfc-forum.org/resources/presentations/Gerhard_Romen_
NFC_Forum_Transport.pdf

[43] Rodolfo Gomes,NXP, INTRODUCTION TO NFC (Near Field Communication), 2007.
http://www.stolpan.com/uploadfiles/1_Mobile_Summit_Budapest_NFC_TechnicalIntroduction.pdf

[44] G. Madlmayr, J. Langer, C. Kantner and J. Scharinger, "NFC Devices: Security and Privacy", *Proceedings of 3rd International Conference on Availability, Reliability and Security (ARES '08)*, 2008.

[45] E. Haselsteiner and K. Breitfus "Security in Near Field Communication (NFC)". *Proceedings of Workshop on RFID Security(RFIDSec)*, 2006.

[46] "Bluetooth Core Specifications, Core Version 4.0", 2010.
https://www.bluetooth.org/Technical/Specifications/adopted.htm

[47] "Bluetooth SIG, NFC Forum come together, right now, over pairing".
http://www.engadget.com/2011/12/20/bluetooth-sig-nfc-forum-come-together-right-now-over-pairing/

[48] NFC Forum, "Connection Handover 1.2, Technical Specification", NFCForum-TS-ConnectionHandover 1-2.doc.

[49] NFC Forum and Bluetooth SIG, "Bluetooth Secure Simple Pairing Using NFC, Application Document", NFCForum-AD-BTSSP 1.0.
http://www.nfc-forum.org/resources/AppDocs/NFCForum_AD_BTSSP_1_0.pdf

[50] "How near-field communications can compliment the drawback of Bluetooth".
http://www.52rd.com/S_Txt/2006_3/TXT3660.htm

[51] "Quick NFC pairing in the Nokia Music Accessories".
http://www.selfproclaimedgenius.com/quick-nfc-pairing-nokia-music-accessories/

[52] "Nintendo Wii U controller to rock NFC to enhance gaming".
http://www.nfcrumors.com/01-27-2012/nintendo-wii-controller-rock-nfc/

[53] Philips, "Near Field Communication".
http://www.sacg.com.tw/sacweb/marcom/epaper/images/NFC.pdf

[54] Ernst Haselsteiner and Klemens Breitfuss, Philips Semiconductors, "Security in Near Field Communication (NFC)", RFIDSec06, 2006.
http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002\%20-\%20Security\%20in\%20NFC.pdf

[55] Radio-Electronics. "NFC Security".
http://www.radio-electronics.com/info/wireless/nfc/nfc-near-field-communications-security.php

[56] G.V. Damme, K. Wouters. Katholieke Universiteit Leuven, Belgium. "Practical Experiences with NFC security on Mobile phones". COSIC - Computer Security and Industrial Cryptography.
http://www.cosic.esat.kuleuven.be/publications/article-1288.pdf

[57] G.P. Hancke. "Practical Eavesdropping and Skimming Attacks on High-Frequency RFID Tokens". Journal of Computer Security. Vol 19, Issue 2, pp. 259-288, Mar. 2011.

[58] C. Mulliner, Fraunhofer Institute for Secure Information Technlogy. "Vulnerability Analysis and Attacks on NFC enabled Mobile Phones". International Conference on Availability, Reliability and Security, 2009.
http://www.mulliner.org/collin/academic/publications/vulnanalysisattacksnfcmobilephones_mulliner_2009.pdf

[59] Hill Associates Wiki, Global System for Mobile communications.
http://www.hill2dot0.com/wiki/index.php?title=Global_System_for_Mobile_communications&printable=yes

[60] Hexazona, GSM Overview, 2008.
http://www.hexazona.com/nexwave/docs/training/GSM%20Overview%2008.pdf

[61] L. Dryburgh and J. Hewett, "Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Services": "GSM Network Architecture", Cisco Press, August 2004, ISBN: 1-58705-040-4.
http://www.ss7-training.net/sigtran-training/ch12lev1sec1.html

[62] P. Arora, GSM System Architecture, Summer Training Report On GSM Mobile Services.
http://www.oocities.org/gsmmobilereport/architecture.htm

[63] M. Suominen, GSM Security, 2003.
http://www.netlab.tkk.fi/opetus/s38153/k2003/Lectures/g42GSM_security.pdf

[64] J. Eberspacher, H.J. Vogel, C. Bettstetter, C. Hartmann, "GSM: Architecture, Protocols and Services", 3rd edition, Wiley, 2008, ISBN 978-0-470-03070-7(H/B).

[65] GPRS White Paper, Cisco Systems, 2000.
http://http://webpc.ciat.cgiar.org/wireless/Documents/2002-gprs_overview.pdf

[66] C. Brookson, Can you clone a GSM smart card (SIM), July 2002.
http://www.brookson.com/gsm/clone.pdf

[67] P. Ekdahl, T. Johansson, "Another attack on A5/1 [GSM stream cipher]," Information Theory. Proceedings. 2001 IEEE International Symposium on , vol., no., pp.160, 2001.

[68] G. Rose, A precis of the new attacks on GSM encryption, QUALCOMM Australia, September 2003. https://opensource.qualcomm.com/assets/pdf/GSM_Attacks.pdf

[69] Y. Song, K. Zhou, X. Chen,"Fake BTS Attacks of GSM System on Software Radio Platform", Journal of Networks, Vol 7, No 2 (2012), 275-281, Feb 2012.

[70] M. Olawski, Security in the GSM network. http://ipsec.pl/files/ipsec/security_in_the_gsm_network.pdf

[71] "GSM (and PCN) Security and Encryption". www.brookson.com/gsm/gsmdoc.pdf

[72] J. Eberspaecher, H. J. Voegel, C. Bettstetter, "GSM - Architecture, Protocols and Services", 3rd Ed., Wiley, New York.

[73] 3GPP ETSI TS 41.061, "GPRS ciphering algorithm requirements".

[74] K.E. Mayes, K. Markantonakis, "Smart Cards, Tokens, Security and Applications", 2008, XXXVIII, 392 p. 128 illus., ISBN: 978-0-387-72197-2

[75] 3GPP http://www.3gpp.org

[76] 3GPP TS 25.101, User Equipment (UE) radio transmission and reception (FDD)

[77] 3GPP TS 25.102, User Equipment (UE) radio transmission and reception (TDD)

[78] H. Holma and A. Toskala , "WCDMA for UMTS: Radio Access for Third Generation Mobile Communications", 3rd edition, Wiley.

[79] 3GPP, Keywords and Acronyms: UMTS. http://www.3gpp.org/Technologies/Keywords-Acronyms/article/umts

[80] K. Etemad, CDMA2000 Evolution: System Concepts and Design Principles, Wiley, 2004, ISBN: 0-471-46125-3.

[81] V. Vanghi, A. Damnjanovic, and B. Vojcic, The CDMA2000 System for Mobile Communications: 3G Wireless Evolution, Prentice Hall, 2004, ISBN:0-13-141601-4.

[82] 3GPP2. http://www.3gpp2.org/public_html/specs/index.cfm

[83] L. Chang, "TD-SCDMA and China 3G - White Paper", Jan. 2012. http://www.marvell.com/communication-processors/assets/Marvell-TD-SCDMA-China3G-WP.pdf

[84] C.G. DENG, "TD-SCDMA wireless network planning optimization and radio resource management(Chinese Edition)", People Post Press Pub, 2007.

[85] F. Goh and S. Nomura, "RF Lecture Series - Modulation Fundamentals Introduction to TD-SCDMA".
http://www1.verigy.com/cntrprod/groups/public/documents/file/td-scdma-2.pdf

[86] K. Wang, "TD-SCDMA Standard Evolution and Industry Development", Global Standards Collaboration (GSC) 14, Jul. 2009.
http://www.itu.int/dms_pub/itu-t/oth/21/05/T21050000010003PDFE.pdf

[87] G. Myagmar, "3G Security Overview".
http://srg.cs.uiuc.edu/MobilSec/posted_docs/3G_Security_Overview.ppt

[88] "Wireless Security".
http://140.113.210.232/edu/video_ppt/wireless%20security20060918.ppt

[89] M. Walker, "Security for 3G Systems".
http://www.isrc.rhul.ac.uk/useca/OtherPublications/certicompres2.pps

[90] T. Aura, "Network Security: GSM and 3G SecurityGSM Security"

[91] B. Krister, H. Guenther, H. Peter and N. Valtteri,"UMTS Security", Electronics & Communication Engineering Journal, Vol.14, No. 5, pp. 191-204, Oct. 2002.

[92] 3G TS 33.120, "Security Principles and Objectives".

[93] 3G TS 33.133, "Security Threats and Requirements".

[94] 3GPP TS 33.102, "3G security: Security architecture".

[95] 3GPP TS 33.105, "Cryptographic Algorithm Requirements".

[96] 3G TR 33.900, "A Guide to 3rd Generation Security".

[97] 3GPP TS 35.201, "Specification of the 3GPP confidentiality and integrity algorithms. Document 1: f8 and f9 specifications".

[98] 3GPP TS 35.202, "Specification of the 3GPP confidentiality and integrity algorithms. Document 2: KASUMI algorithm specification".

[99] 3GPP TS 35.205, "Specification of the MILENAGE Algorithm Set. Document 1: General".

[100] 3GPP TS 35.206, "Specification of the MILENAGE Algorithm Set. Document 2: Algorithm specification".

[101] MILENAGE: An Example of Good UMTS Security.
http://www.mcit.gov.sa/nr/rdonlyres/d762830c-fbe7-4b36-aafc-780cfbafc92c/0/paper36.pdf

[102] C. Blanchard, Security for the Third Generation (3G) Mobile System
http://www.isrc.rhul.ac.uk/useca/OtherPublications/3G_UMTS%20Security.pdf

[103] UMTS Network Architecture.
http://conningtech.wordpress.com/2008/05/09/umts-network-domains/

[104] Y. Miyakawa, T. Kurokawa, A. Yamamura, and Y. Matsumoto, "Current Status of Japanese Government PKI Systems", Public Key Infrastructure, Lecture Notes in Computer Science Volume 5057, 2008, pp 104-117, Springer.
http://link.springer.com/chapter/10.1007\%2F978-3-540-69485-4_8?LI=true

[105] R. Rivest, A.Shamit, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems". Communications of ACM, Vol. 21, No.2, Feb. 1978, 158-164.

[106] IETF RFC 2104, HMAC: Keyed-Hashing for Message Authentication.
http://tools.ietf.org/html/rfc2104

[107] M. Bellare, R. Canetti, H. Krawczyk, "Message Authentication using Hash Functions - The HMAC Construction", RSA Laboratories CryptoBytes, Vol. 2, No. 1, Spring 1996.

[108] What is MD5?
http://www.accuhash.com/what-is-md5.html

[109] Message Digest 5 (MD5), Cisco.
http://www.ciscopress.com/articles/article.asp?p=25470&seqNum=6

[110] What is SHA-1?
http://www.accuhash.com/what-is-sha1.html

[111] Secure Hash Algorithm 1 (SHA-1), Cisco.
http://www.ciscopress.com/articles/article.asp?p=25470&seqNum=7

[112] FIPS-186-3, Digital Signature Standard (DSS), the third and current revision to the official DSA specification. June 2009.
http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf

[113] Descriptions of SHA-256, SHA-384, and SHA-512. IWS - The Information Warfare Site.
http://www.iwar.org.uk/comsec/resources/cipher/sha256-384-512.pdf

[114] IETF RFC 1321, The MD5 Message-Digest Algorithm.
http://tools.ietf.org/html/rfc1321

[115] DIGITAL SIGNATURE STANDARD (DSS), FIPS PUB 186, Federal Information Processing Standards Publication, 1994.
http://www.itl.nist.gov/fipspubs/fip186.htm

[116] B. Sotomayor, 9.3. Public key cryptography, Chapter 9. Fundamental Security Concepts.
http://gdp.globus.org/gt4-tutorial/multiplehtml/ch09s03.html

[117] J. Weise, Public Key Infrastructure Overview, Sun Microsystems, Inc. August 2001.
http://vlib.eitan.ac.il/digital_signiture/main_pdf/publickey.pdf

[118] D. Cheong, PKI Public Key Infrastructure.
http://www.unescap.org/stat/meet/dataprot/cheong05.pdf

[119] Public Key Infrastructure (PKI), Cisco.
http://www.cisco.com/en/US/products/ps6664/products_ios_protocol_option_home.html

[120] W. Stallings, Cryptography and Network Security: Principles and Practices, 5th edition, Prentice Hall, 2011.

[121] E-Signature Law.
http://www.e-signature.com/e-signature-law/

[122] United Kingdom, Electronic Communications Act 2000.
http://www.legislation.gov.uk//ukpga/2000/7

[123] T. Nykanen, "Attribute Certificates in X.509" http://www.tml.tkk.fi/Opinnot/Tik-110.501/2000/papers/nykanen.pdf

[124] IETF RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
http://www.ietf.org/rfc/rfc3280.txt

[125] M. Sonntag, "Electronic Signatures for Legal Persons"
http://www.fim.uni-linz.ac.at/research/telework/ElSigLegalPersons.pdf

[126] S. Magnus and M. Maron, "A Public Key Infrastructure in Ambient Information and Transaction Systems"
http://www.uni-koblenz.de/~maruhn/publications/gmr_2_09.pdf

[127] Y. Suzuki, "PKI - current and future", Workshop for Japan Germany Information security, October 2004.
http://www.teletrust.defileadminfilesDt-Jap-WS_04_4-2\%20Suzuki.pdf

[128] CPS 2.16.756.1.17.3.1.0, Swiss Government PKI - Root CA I, Certificate Policy and Certification Practice Statement of the Swiss Government Root CA I.
http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf

[129] What is Citizen Digital Certificate
http://moica.nat.gov.tw/html/en/what.htm

[130] Government Root Certification Authority, GRCA, Taiwan.
http://grca.nat.gov.tw/index.html

[131] C.M. OU, H.L. SHAN, and C.T. HO, "Government PKI Deployment and Usage in Taiwan", INFORMATION & SECURITY. An International Journal, Vol.15, No.1, 2004, 39-54.
http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ots591=cab359a3-9328-19cc-a1d2-8023e646b22c&lng=en&id=10508

[132] C.M. Ou, C.I. Fan, and H.L. Shan, "PKI Interoperability in Taiwan"
http://grca.nat.gov.tw/download/PKIinTaiwan.pdf

[133] Taiwan government public key infrastructure with CDC.
http://moica.nat.gov.tw/

[134] Information Center, MOICA Internet Tax Filing Service and Promotion Incentives, Ministry of the Interior, May 2011.
http://moica.nat.gov.tw/html/en/18-046-000-01903.htm

[135] The Citizen Digital Certificate issue statistical information
http://moica.nat.gov.tw/html/en/index.htm

[136] The state-of-the-art online ID card, A great success in Taiwan.
www.aeteurope.com

[137] S. Kadhiwala and S. Zulfiquar,"Analysis of mobile payment security measures and different standards", *Computer Fraud & Security*, Vol. 2007, No. 6. pp. 12-16, 2007.

[138] Smart Card Alliance, "Proximity Mobile Payments: Leveraging NFC and the Contactless Financial Payments Infrastructure", 2007
http://www.smartcardalliance.org/resources/lib/Proximity_Mobile_Payments_200709.pdf

[139] W. LIU, C. ZHAO and W. ZHONG, "The GPRS Mobile Payment System Based on RFID", *ICCT International Conference*, pp. 1-4, Nov 2006.

[140] H. Harb, H. Farahat, and M. Ezz, "Secure SMS Mobile Payment Model. Anti-counterfeiting", *The 2nd ASID International Conference*, PP. 1-17, 2008.

[141] S. Pradhan, E. Lawrence, A. Zmijewska, "Bluetooth as an Enabling Technology in Mobile Transactions," itcc, vol. 2, pp.53-58, *International Conference on Information Technology: Coding and Computing* (ITCC'05) - Volume II, 2005

[142] L.B. Bhajantri, S.S. Manvi, M.A. Vijayakumar, "Secure Mobile Payment System in Wireless Environment", *Proceedings of International Conference on Future Computer and Communication*, pp. 31-35, 2008.

[143] J. Meng and L. Ye, "Secure Mobile Payment Model Based on WAP", *Proceedings of 4th IEEE International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM apos '08)*, pp.1-4, 2008.

[144] Y. Xu, X. Liu, R. Yao, "A Payment Model of Mobile Phone Based on Third-Party Security," Management of e-Commerce and e-Government, 2009. ICMECG '09. International Conference on , vol., no., pp.400-403, 2009

[145] S.L. Ghiron, S. Sposato, C.M. Medaglia, A. Moroni, "NFC Ticketing: A Prototype and Usability Test of an NFC-Based Virtual Ticketing Application," nfc, pp.45-50, *2009 First International Workshop on Near Field Communication*, 2009.

[146] M. Jovanovic, and M.M. Organero, Analysis of the Latest Trends in Moibile Commerce using the NFC Technology, Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), May Edition, 2011.

[147] EUROPEAN COMMITTEE FOR BANKING STANDARDS, Business and Functional Requirments for Mobile Payments, TR603 VERSION 1, FEBRUARY 2003.
`http://www.it.iitb.ac.in/~tijo/seminar/disruption\%20analysis/Tecnical\%20Functional\%20requirement\%20of\%20m\%20banking.pdf`

[148] B, Manoj V, SMS Based Secure Mobile Banking, International Journal of Engineering and Technology Vol.3 (6), 2011, 472-479, Dec 2011- Jan 2012.
`http://www.enggjournals.com/ijet/docs/IJET11-03-06-29.pdf`

[149] J. Ondrus, Y. Pigneur, A Multi-stakeholder Multi-criteria Assessment Framework of Mobile Payments: An Illustration with the Swiss Public Transportation Industry, HICESS 2006.
`http://www.hec.unil.ch/yp/Pub/06-hicss39.pdf`

[150] M. Gusev, L. Antovski and G. Armenski, "Models of mobile payments", *Proceedings of WSEAS ICOMIV*, pp. 3581-3586, 2002.

[151] W. Guo, "Design of Architecture for Mobile Payments System", *Proceedings of Chinese Control and Decision Conference (CCDC)*, pp. 1732-1735, 2008.

[152] Q. Zhang, "Mobile payment in mobile e-commerce", *Proceedings of 7th World Congress on Intelligent Control and Automation (WCICA)*, pp. 6650-6654, 2008.

[153] J. Eberspaecher, H. J. Voegel, C. Bettstetter, "GSM - Architecture, Protocols and Services", 3rd Ed., Wiley, New York.

[154] IEEE 802.15.1 (Bluetooth)
`http://ieee802.org/15/Bluetooth/index.html`

[155] UICC - The Security Platform for Value Added Services
`http://portal.etsi.org/docbox/Workshop/2009/200901_SECURITYWORKSHOP/G&D_Vedder_UICC_SecurityPlatformforValueAddedServices.pdf`

[156] Y. Li, Y. Chen and T.J. Ma. "Security in GSM"
`www.gsmsecurity.net/papers/securityingsm.pdf`

[157] "GSM System Overview".
www.pcs.csie.ntu.edu.tw/course/pcs/2007/reference/04_GSM_System_Overview.pdf

[158] 3GPP, ETSI TS 41.061, "GPRS ciphering algorithm requirements".

[159] L.B. Bhajantri, S.S. Manvi and M.A. Vijayakumar, "Secure Mobile Payment System in Wireless Environment", *Proceedings of International Conference on Future Computer and Communication*, pp. 31-35, 2008.

[160] J.J. Chen and C. Adams. "Short-range wireless technologies with mobile payments systems", *ICEC '04: Proceedings of the 6th international conference on Electronic commerce*, 2004.

[161] J. Meng and L. Ye, "Secure Mobile Payment Model Based on WAP", *Proceedings of 4th IEEE International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM apos '08)*, pp.1-4, 2008.

[162] M. Massoth and T. Bingel, "Performance of different mobile payment service concepts compared with a NFC-based solution", *Proceedings of 4th International Conference on Internet and Web Applications and Services (ICIW '09)*, pp. 205-210 2009.

[163] T.S. Fun, L.Y. Beng, J. Likoh and R. Roslan. "A Lightweight and Private Mobile Payment Protocol by Using Mobile Network Operator". *Proceedings of International Conference on Computer and Communication Engineering (ICCCE 2008)*, pp. 162-166, 2008.

[164] F. Cheng, G. Zhang and C. Meinel, "SIMPA: A SIP-based Mobile Payment Architecture", *Proceedings of 7th IEEE/ACIS International Conference on Computer and Information Science*, pp. 287-292, 2008.

[165] "Barclay Credit Card + Oyster Card".
http://www.barclaycard-onepulse.co.uk/oysterCard.html

[166] M. Massoth, T. Bingel, "Performance of Different Mobile Payment Service Concepts Compared with a NFC-Based Solution," iciw, *2009 Fourth International Conference on Internet and Web Applications and Services*, pp.205-210, 2009

[167] M. Saarisalo, Software Development Kit for NFC device, WIMA, Monaco, April 2007.

[168] Nokia 6131 NFC SDK: Programmers Guide, Version 1.1, July 2007.

[169] Nokia 6131 NFC SDK: Users Guide, Version 1.1, July 2007.

[170] JSR 257: Contactless Communication API Java Community Process, 2006.
http://www.jcp.org/en/jsr/detail?id=257

[171] JavaCard's algorithms support test: Nokia 6131 NFC phone.
http://www.fi.muni.cz/~xsvenda/docs/Nokia6131_102008.pdf

[172] J. Gao, V. Kulkarni, H. Ranavat, Lee Chang, Hsing Mei, "A 2D Barcode-Based Mobile Payment System," *Multimedia and Ubiquitous Engineering, 2009. MUE '09*. Third International Conference on , vol., no., pp.320,329, 4-6 June 2009.

[173] W.D. Chen, G.P. Hancke, K.E. Mayes, Y. Lien, J.H. Chiu, "NFC Mobile Transactions and Authentication Based on GSM Network," nfc, *2nd International Workshop on Near Field Communication*, pp.83-89, 2010.

[174] W.D. Chen, G.P. Hancke, K.E. Mayes, Y. Lien, J.H. Chiu, "Using 3G Network Components to Enable NFC Mobile Transactions and Authentication," *Progress in Informatics and Computing (PIC-2010)*, 2010.

[175] W.D. Chen, K.E. Mayes, Y.H. Lien, J.H. Chiu, "NFC mobile payment with Citizen Digital Certificate," *Next Generation Information Technology (ICNIT), 2011 The 2nd International Conference on* , vol., no., pp.120,126, 21-23 June 2011.