Security Protocol for NFC Enabled Mobile Devices Used in Financial Applications

By

Osama Bin Faridoon

2012-NUST-MS-CCS-05

Supervisor

Dr. Abdul Ghafoor Abbasi

Department of Computing

A thesis submitted in partial fulfillment of the requirements for the degree of
Masters of Science in Computer and Communication Security (MS CCS)

In

Department of Computing (DoC)
School of Electrical Engineering and Computer Science (SEECS),
National University of Sciences and Technology (NUST),
Islamabad, Pakistan
(Jan, 2015)

Approval

This thesis has been submitted in partial fulfillment of requirements for the Masters of Science in Computer and Communication Security at National University of Sciences & Technology.

It is certified that the contents and form of the thesis entitled "**Security Protocol for NFC Enabled Mobile Devices Used in Financial Applications**" submitted by **Osama Bin Faridoon** have been found satisfactory for the requirement of the degree.

Advisor: **Dr. Abdul Ghafoor**

Signature: _____

Date: 04/05/1015 _________________________

Committee Member 1: **Dr Zahid Anwar**

Signature: _________________________

Date: _________________________

Committee Member 2: **Dr. Awais Shibli**

Signature: Zahid Anwar

Date: 2/4/2015

Committee Member 3: **Mr. Muhammad Qaisar Choudhary**

Signature: _________________________

Date: _________________________

Dedication

Dedicated To My Father

Lt Col Faridoon Khan Jadoon

Whose motivation dedication and persuasion inspired and enabled me to complete it.

Certificate of Originality

I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at National University of Sciences & Technology (NUST) School of Electrical Engineering & Computer Science (SEECS) or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEECS or elsewhere, is explicitly acknowledged in the thesis.

I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics which has been acknowledged.

Osama Bin Faridoon

Signature: ______________________________

Acknowledgment

I seek Divine protection from satan evil mind and begin with the name of ALLAH the compassionate, the kind. Allah Almighty has been very gracious in bestowing me courage and will to accomplish this endurance seeking task.

Doing MS and thesis work at NUST SEECS KTH Lab was a unique blend of experiences. It is the biggest milestone of my academic career. I had my first interaction with Dr. Abdul Ghafoor when he taught us Data Communication Networks and Security. I was fortunate enough that he accepted me under his able supervision. I owe my interest in the field of access technologies especially Near Field Communication to my supervisor Dr. Abdul Ghafoor. I learned so many things from him, not just the research work. He has a special talent of breaking down complex problems into easy steps. I am thankful to him for proof reading my conference paper despite his busy schedule. I express my great respect for Dr. Abdul Ghafoor for giving me expert advice and insights which definitely were helpful in completing this thesis.

Once again I would like to thank you very much Dr. Abdul Ghafoor for giving me the opportunity to work with you and for our KTH-AIS lab. Your guidance, critical feedback and active research involvement have made a huge contribution to the quality and presentation of my work.

I am also grateful to my committee members who have guided me during presentation and for their constructive comments on my thesis during defense phase, especially Dr Awais Shibli for critically questioning my work. I feel obliged to my colleagues at KTH Lab especially Fowz Masood and Naveed Ahmed for discussing the problems and issues and steering me to the solution.

At the end I would like to state my earnest gratitude to my parents and family for being impatient and eager, which led to the successful completion of the tasks within deadlines.

Osama Bin Faridoon

.Table of Contents

List of Figures

List of Tables

Abstract

The fostering of NFC in everyday tasks and with growth in applications involving contactless transactions based on NFC; there is a requirement from users and industry to address the security issues affecting mobile payments. The current NFC security standards ECMA-385 and ECMA-386 are inadequate to address most of the security concerns such as privacy infringements, unauthorized access to financial data, theft of mobile data exchanged between terminal and mobile device. By considering the current and future security requirements, we designed a NFC based security protocol for financial applications, which addresses security requirements holistically and provides local and remote mutual authentication, confidentiality, integrity and non-repudiation. It is based on some common and extended security features which help to increase the reliability of NFC based systems. After designing, we verified our protocol using formal verification tools like Scyther and established our designed protocol resists against spoofing attack, man-in-the-middle attack, replay and skimming attacks. It ensures the secrecy of transaction data, privacy of the users and also ensures that only authenticated and authorized NFC device holder and PoS terminals are securely exchanging financial data to perform the transaction. As a proof of concept, we implemented our solution using Java Technology for Android based NFC mobile devices and successfully deployed it in our local environment to test its correctness and behavior. We also provided a comprehensive comparison of our protocol with other NFC based financial protocols. We found that the mutual authentication, confidentiality, integrity, authorization and non-repudiation services help to protect against most of the security attacks related to mobile financial transactions. Since this protocol is flexible, generalized and reliable, so the whole system is not depended on the third parties and any prior knowledge.

1. Introduction and Motivation

1.1 Introduction

Near Field Communication (NFC) is a wireless technology standard which is short range and uses high-frequency. It operates on the principle of magnetic field induction and has a range of 10cm theoretically and practically 4cm. NFC operates on the Industrial, Scientific and Medical (ISM) radio band at the frequency of 13.56 MHz with data rates of 106, 212 and 424 kbps. NFC has its roots with RFID technology and was built by converging the contactless characteristic of RFID and two way communication of other wireless communication technologies like WiFi and bluetooth. A comparison of NFC with other peer wireless technologies is also given later in the thesis book. NFC communication takes place between two points having NFC interfaces by just tapping or moving past one to another. It also allows access to RFID tags.

The number of applications and services provided by contactless cards are increasing day by day. Therefore a person needs to carry more than one contactless card for different applications and institutions. A more practical solution for providing flexibility and scalability is to adopt Near Field Communication (NFC) enabled devices, which provides Secure Element (SE) for keeping all the applications secure and independent of each other in our mobile phone. Furthermore, the associated data of each application should be managed by the individual applications and should not be shared with each other. For smooth and seamless experience, both in proximity and in internet based remote applications, NFC enabled mobile phones are considered more practical solution.

The ever increasing processing power and storage with reduced cost has made smart phones fast, ubiquitous and part of our everyday life. With NFC being part of billions of smart phones, mobile payment market is increasing exponentially. According to ABI, a technology market research company, the number of NFC-enabled devices will reach close to 1.95 billion in 2017 [1]. A number of different payment systems including MasterCard [2], Google Wallet [3], etc are using NFC feature because of its simplicity and convenience. But with varied financial services like payment systems for banks, billing, ticketing, buying medicine for a patient with history of disease etc, concerns about authenticity, confidentiality, privacy, integrity and reliability of the systems are arising.

The NFC security standards ECMA-385 and ECMA-386 provide only confidentiality and integrity. There is no protection from attacks against authentication, authorization and privacy mechanisms. As stated in [4], the privacy of users during payments is not ensured due to fixed keys used for confidentiality. In EMV (Euro, MasterCard and VISA) proximity payments, only the card has to authenticate to the PoS terminal and micro payments don't require the pin verification. So there is a requirement for the mutual authentication between NFC device and Point of Sale (PoS) Terminal.

Our solution which is a protocol addresses the security requirements of mobile contactless payment systems including remote and local mutual authentication, confidentiality, privacy, authorization, integrity and non-repudiation. It is a generalized solution which can be implemented for any payment system and is independent of third party solutions.

1.2 Motivation

NFC is the latest technology, being incorporated by billions of smart phones. It has changed the concept of carrying wallet and payment cards. Many countries have already introduced NFC based systems. With an NFC enabled smart phone, it is a whole lot easier to perform a huge range of tasks. But there are a number of risks associated with the usage of NFC enabled smart phones. It can be with the tags, i.e. by breaking the tag's encryption hackers can reprogram tags for their own purposes and load malicious code. It can be eavesdropping on the communication link. Other security risks involve spoofing or malicious readers, data corruption and manipulation, interception attacks and theft. According to BBC news [22], a number of vulnerabilities and weaknesses in NFC have been shown by the team of security experts at an event in Tokyo.

In order to reap full benefits of this technology, and for NFC based applications to be able to provide a reliable way of dealing with everyday business chores, it is necessary to cater for the security risks and threats involved with NFC. Implementation of the proposed security solutions will help in increasing the reliability and integrity of this time saving and user friendly technology. Our bills and banking transactions will be more secure. More businesses will adopt this less costly and efficient technology. Also it will provide new research directions in NFC security domain for researchers and students. Proposed security solution will also help implementation of NFC at government organizations, airports, ticketing, businesses, hospitals, sensitive installment etc.

1.3 Problem Statement and Scope

The objectives of the research work are

- To provide reliability in NFC Contactless cards.
- To provide strong mutual authentication mechanism between NFC card and NFC reader.
- To provide extended security features to secure NFC financial transactions.

Design and Implementation of formally provable Security Protocol in order to achieve Local and Remote Authentication, Confidentiality, Integrity and Non Repudiation in NFC based financial systems.

1.4 Research Methodology

Research helps us in establishing facts and conclusions of different phenomenon which we study. The two main approaches to scientific research are deductive and inductive. Deductive research is more close to top-down approach. On the other hand inductive research is a bottom up approach. In deductive research we move from general to the more specific conclusions. Contrary to this, in inductive research we move from specific observations to broader generalizations and theories [69].

The objective of the research work was to point out the issues and problems and then move to conclusion and solution by narrowing down. Hence, the approach which I have adopted is deductive. There are four methodologies in deductive research approach i.e. 1) Theory 2) Hypothesis 3) Observation and 4) Confirmation. A thorough literature review is necessary for deriving a hypothesis. The hypothesis is then approved or condemned in the light of observations made. To verify the hypothesis, I used automated verification tool; Scyther. These different phases of my research work have been mentioned in the chapters respectively. Chapter 2 and 3 presents the literature survey and the problem statement. In chapter 4, the architecture of the solution is provided. Chapter 5 analyses the solution with the help of automated verification tool Scyther.

1.5 Contributions

In order to reap full benefits of this technology, and for NFC based applications to be able to provide a reliable way of dealing with everyday business chores, it is necessary to cater for the security risks and threats involved with NFC. We designed and implemented a protocol that is going to cater the security requirements of mobile proximity payment systems by securing the communication between NFC reader and NFC mobile phone. Our protocol is providing security in terms of mutual authentication of both NFC mobile phone and NFC mobile reader, encryption and integrity of the communication taking place between them. The protocol is also catering to the privacy aspect of the communication taking place between the NFC mobile phone and reader. As a proof of concept we designed an NFC java card applet for both mobile phone and reader. Implementation of the proposed security solutions will help in increasing the reliability and integrity of this time saving and user friendly technology. Our bills and banking transactions will be more secure. More businesses will adopt this less costly and efficient technology. Also it will provide new research directions in NFC security domain for researchers and students. Proposed security solution will also help implementation of NFC at government organizations, airports, ticketing, businesses, hospitals, sensitive installment etc.

Our NFC mobile applet for reader requests for certificate. The NFC mobile applet sends its certificate containing public key of the card and ID of the card and applet. The mobile PoS terminal applet forwards the IDs and certificate to the Authentication and Authorization server for verification. The PoS applet then sends its certificate. NFC mobile applet extracts the certification authority root key and authenticates the POS terminal’s certificate, validating that the certificate is issued by the correct issuer and is authentic. This verifies the certificate and ID and activates the relevant applet. There are two steps involved in the verification of certificate. The first step is to verify originality of certificate by signature verification. Then revocation and expiry of the certificate is checked. Then both the applets exchange the challenge response packets. After the verification of responses from both the sides, the remote authentication process is completed. Remote authentication is based on certificate verification and Challenge Handshake Authentication (CHAP). Challenge response ensures that the entity is available and willing; whose certificate is being verified providing nonrepudiation. It also ensures whether the person or the device having the certificate also possess the corresponding private key. This process also helps avoid fake, forged and stolen certificates. The local authentication is done by entering the PIN code and its verification by PoS terminal applet.

The PoS applet then generates One Time Session Key and sends it to the NFC mobile in the encrypted form. This One Time Session Key is used for encrypting the session communication and also ensures privacy. All of the financial transactions are sent encrypted along with their hash.

We verified our protocol with Scyther [29], which is an automated security verification tool. The complete formal code for verification is given in Appendix. The results generated through Scyther show that our protocol possesses the attributes of secrecy, aliveness, injective synchronization, non-injective synchronization and non-injective agreement thus ensuring protection against man-in-the-middle attack, spoofing, skimming and replay attacks.

1.6 Thesis Organization

The first chapter of the thesis work provides a bird eye view of our research work, in the form of introduction and motivation, problem statement and research methodology. Chapter two gives the technical understanding of NFC, its ecosystem and how the NFC communication takes place. It also encompasses the applications of NFC and understanding of threats to NFC technology and mobile proximity payments. Chapter three discusses the related work and gives a comparison. Designing of the protocol to secure communication between NFC reader and NFC mobile phone as a solution to the security problems of NFC based mobile proximity payments is discussed in fourth chapter. In the fifth chapter, implementation and analysis of the protocol with the help of Scyther Tool is given.

2. Technical Background

2.1 Introduction

The working of RFID technology is based on the principle of mutual induction as discussed in [4] due to the coupling effect of two circuits with a magnetic field. Since NFC is based on RFID technology, the communication takes place by transferring energy from one circuit to another. When the reader and NFC card are placed close enough to the reader, the magnetic field from the reader coil will couple to the card coil. As a result a voltage is induced in the card that will be rectified and is used for powering the circuit of tag. For modulating data from the card to the reader, the load is changed on the coil of card circuitry and this can be detected by the reader as a result of the mutual coupling.

The distance between the coils must be less than 4 cm for communication to take place, as inductive coupling is a near field effect, so. The coupling between the polling device (initiator) and listening device (target) is due to magnetic near-field of two conductors.

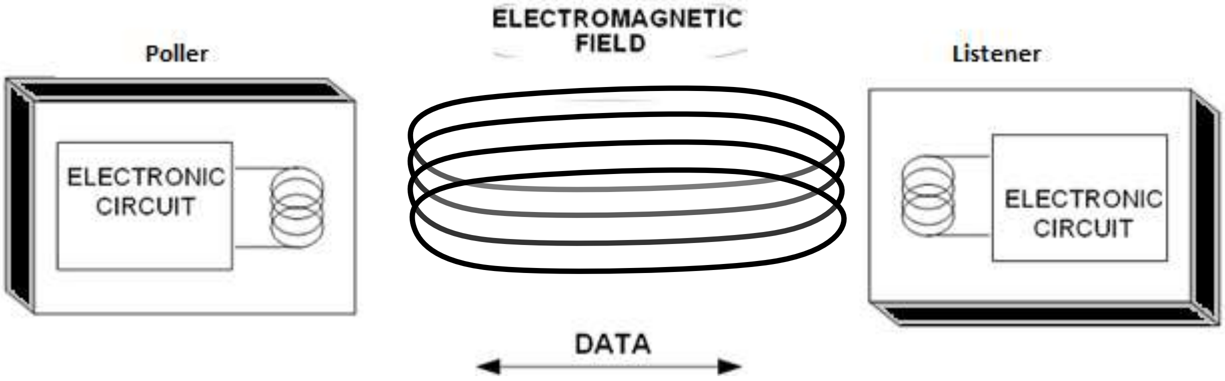


Figure-1 Diagram of Inductive Coupling

There are two modes of communication for NFC. In the Active communication mode, both the Initiator (Reader) and the Target (card) use their own RF / magnetic field to communicate. Upon initiating the NFCIP-1 transaction, the Target responds by modulating its own RF field. In the active communication mode the initiator first of all performs the RF collision avoidance.

In the Passive communication mode, the target responds to an Initiator command by modulating the Initiators’ RF field which is referred to as load modulation. The start of the Passive communication shall be detected by the presence of the carrier frequency. NFC devices detect external RF fields with field strength higher than the certain threshold level. The basic technique for device detection among many in NFC is Time Slot method.

The transport protocol for NFC is handled in three parts including activation of the protocol, which includes the Request for Attributes and the Parameter Selection. The other two parts are the data exchange protocol, and the deactivation of the protocol including the Deselect and the Release.

NFC devices operate in three modes [4].

- **Card Emulation Mode:** is a passive mode in which NFC device acts like a smartcard and conforms to standards like ISO-14443 and ISO- 7816. This helps in substituting the plastic smartcards with NFC enabled mobile device.
- **Peer-to-Peer Mode:** is an active mode and requires less power as the two NFC devices generate their own RF beam to exchange information. The initiator device is also known as polling device. The target device is also known as listener device. In NFC Peer to Peer mode data is transmitted using Near Field Communication Data Exchange Format (NDEF).
- **Reader/Writer Mode**: is an active mode in which the NFC device actively reads or writes to a passive RFID tag.

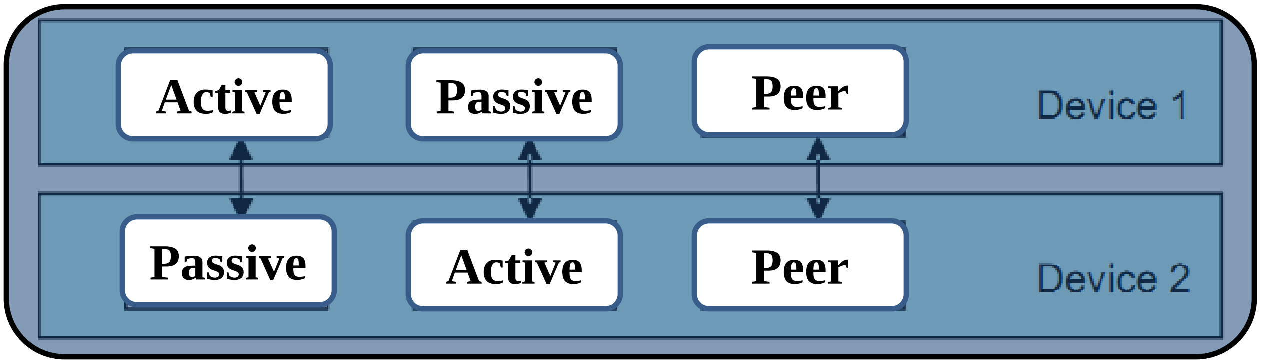


Figure-2 Modes of Communication

All the three operating modes card emulation, peer-to-peer and reader/writer can be combined with either NFC-A, NFC-B, NFC-F or NFC-V. NFC-A is backward compatible to ISO/IEC 14443 A. NFC-B is backward compatible to ISO/IEC 14443 B. NFC-F is backward compatible to JIS X 6319-4. NFC-V provides access to NFC-V (ISO 15693) properties and I/O operations on a Tag. An NFC polling device first tries to get responses from NFC-A, NFC-B, NFC-F and NFC-v tags with the corresponding request signals. On getting a response from a compatible device, the NFC device sets up the requested communication mode.

NFC uses different modulation and bit encoding schemes for different bit rates. While establishing the communication, the Initiator starts the communication in a particular mode and target answers accordingly [4].

NFC–Forum Standard	**Polling / Listening**	**Coding**	**Modulation**	**Data Rate**	**Carrier Frequency**
NFC-A	Polling	Modified Miller	ASK 100%	106kb/s	13.56 MHz
	Listening	Manchester	Load Modulation(ASK)	106kb/s	13.56 MHz +_ 848 kHz subcarrier
NFC-B	Polling	NRZ-L	ASK 10%	106kb/s	13.56 MHz
	Listening	NRZ-L	Load Modulation(BPSK)	106kb/s	13.56 MHz +_ 848 kHz subcarrier
NFC–C	Polling	Manchester	ASK 10%	212 / 424 kb/s	13.56 MHz
	Listening	Manchester	Load Modulation(ASK)	212 / 424 kb/s	13.56 MHz (without subcarrier)

Table-1 NFC Technical Standard Specification of the Air Interface

2.2 NFC Hardware

2.2.1 Design of NFC Mobile

An [5] NFC mobile device is typically composed of SEs and an NFC interface in addition to other integrated circuits. The NFC interface consists of a contactless; analog/digital front-end called an NFC Contactless Front-end (NFC CLF), an NFC proximity antenna and an IC called an NFC controller to enable NFC transactions. There is a Secure Element SE which provides secure environment to programs and data and is connected to the NFC controller. This helps in carrying out secure proximity transactions with external NFC devices. The interfaces between SEs and the NFC controller are the Single Wire Protocol (SWP) and the NFC Wired Interface (NFC-WI). The interface between the NFC controller and the host controller is Host Controller Interface (HCI). The HCI helps host controller in setting the operating modes of the NFC and establishing connection between the NFC controller and the SE.

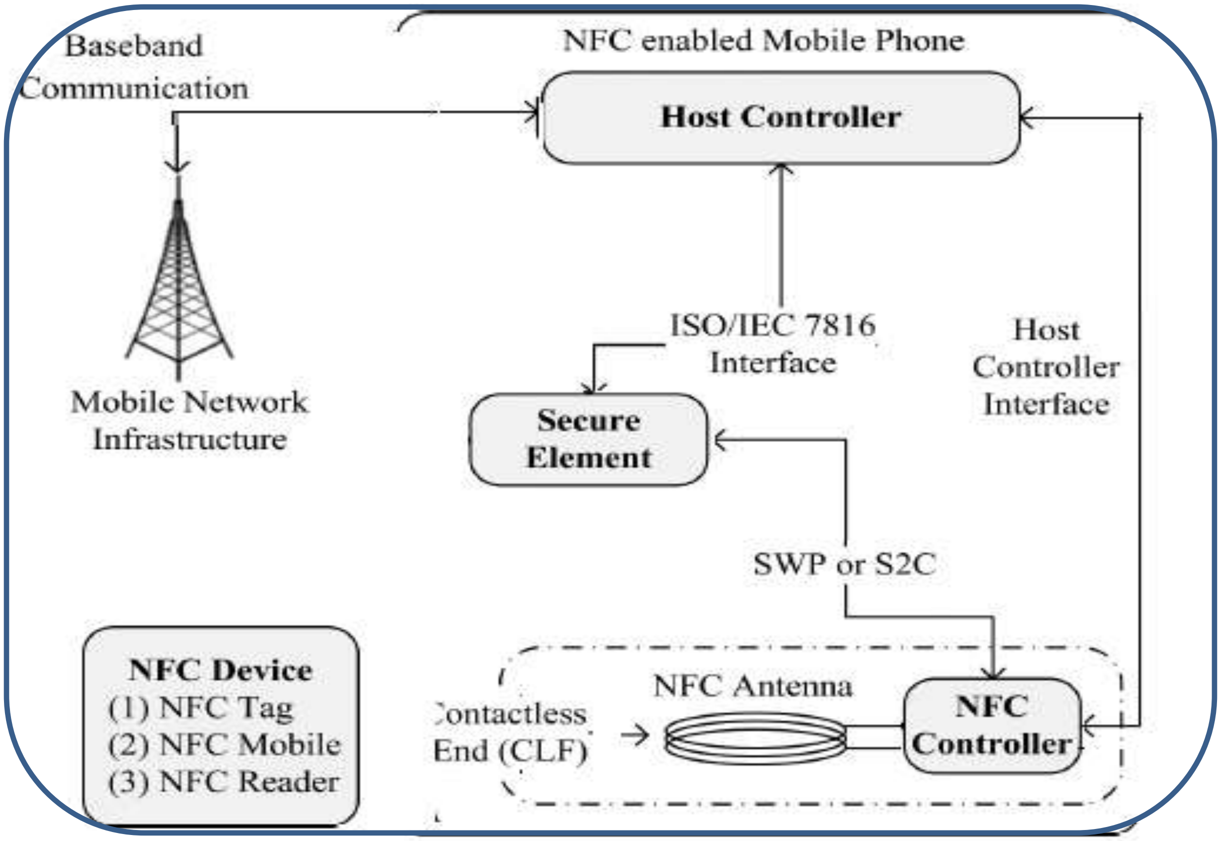


Figure-3 NFC Mobile Architecture

2.2.2 Secure Element

According to global platform [6] a Secure Element (SE) is an architecture which resists tampering and is used for securely hosting applications and their cryptographic credentials. It is a secure microcontroller containing a processor, operating system, different types of memories, crypto engines, sensors, timers, random number generators and communication ports[7]. In Secure Element (SE) different applets representing various physical smart cards are executed on virtual machines.

Generally the form factor for Secure Element (SSE) can be divided into Removable and Non-Removable Elements. Removable form includes Universal Integrated Circuit Card (UICC) and micro SD whereas non-removable is in the form of embedded chip. Each of the form has its own usage scenarios along with specific and pros and cons.

Due to strong security, remote access control and over the air provisioning of the application and credentials, the most suitable choice for SE is sim based. In such a case the complete control and responsibility lies with the mobile operator and trusted service manager. However, this form factor is not suitable in case of multiple applications from different vendors residing in the same secure element, as it is operator dependent which creates security and control issues.

The embedded chips for secure element also provide strong security and protection from different attacks but lacks in flexibility and scalability, as it involves a tedious task of transferring applications from one handset to the other [8].

Although micro SD card option for SE is independent of mobile operators and Trusted Service Managers (TSMs) but it lacks standards and specifications yet. Also it will require multiple cards slots in a handset for multiple applications [9].

A number of other options for providing a secure and tamper resistant environment to the applications and their secure credentials are being considered. These options need to be flexible, scalable, affordable and free of monopoly of any one entity in the NFC ecosystem.

Use of exclusive hardware can help in achieving isolation for the applications execution environment. But it comes at the cost of limited space, and computation in NFC. The end user also has limited access to the applications. Furthermore, applications transfer from one handset to the other and their updation is dependent on third party. Hence, it is time consuming and costly. So a viable option can be based on secure virtualization platform as described by author in [10]. Another option [11] for implementing a SE in software can be the execution of virtual machines inside Mobile Trusted Module (MTM) as suggested by the Trusted Computing Group (TCG). In [12] Ahmad et.al used TEE in combination with Universal Subscriber Identity Module (USIM) for the execution of secure mobile applications.

In cloud based secure elements the sensitive data is stored on the cloud in the encrypted form and is transferred to the mobile phone for transaction; decrypted and then transferred to the reader or PoS terminal [13]. Although it solves the problem of limited space and computing but the bottle neck is the network latency and encryption decryption complexity at the mobile phone. In addition, it gives a large surface area for launching attack.

Google recently introduced the concept of Host Card Emulation (HCE), which does not rely on secure element and hence not dependent on mobile network operators, equipment manufacturers and TSMs. It allows the applications on android device to both emulate NFC card and NFC reader by allowing the applications to directly communicate with the NFC antenna [14][15]. The security of Google's HCE is yet to be proved, especially in case of multiple security sensitive applications using NFC.

The more secure an application or a solution is, the less easiness and flexibility it provides. In the end it all comes to the compromise between cost, ease and security of different solutions. We also need thorough standardization and certified security test-ing of various solutions of Secure Element (SE) implementation.

2.2.3 NFC Tag Types

NFC tags are passive devices that communicate with active NFC devices. They are used to store data and transfer it to active NFC devices. There are four tag types each with different format and capacity. These NFC tag type formats are based on ISO 14443 Types A and B and Sony FeliCa.

	Type 1	**Type 2**	**Type 3**	**Type 4**
ISO / IEC Standard	14443 A	14443 A	JIS 6319-4	14443 A/B
Compatible Product	Innovision Topaz	NXP MIFARE	Sony Felica	NXP DESFire, Smart MX-JACOP
Data Rate	106kb/s	106kb/s	212 / 424 kb/s	106 / 212 / 424 kb/s
Memory	96 bytes expandable to 2kbytes	48 bytes Expandable to 2kbytes	Variable max 1Mbyte	Variable max 32 kbyte
Anti-collision	No	Yes	Yes	Yes

Table-2 NFC Type Definition

2.3 NFC Standards

Although RFID is a mature technology, which was first introduced in early eighties. The NFC was first introduced by Sony and Philips in 2002 [17]. A major breakthrough took place when Nokia manufactured the first NFC mobile phone Nokia 6131, in the year 2006. Most of the standards are defined by NFC Forum, which was founded in 2004 by Nokia, Philips and Sony. GSMA has worked to define standards related to NFC in mobile phones. These standards are related to Trusted Services Manager, Single Wire Protocol, testing and certification of secure element.

NFC is backwards compatible with the protocols related to Smart Card infrastructure like ISO/IEC14443A (e.g. NXPs MIFARE technology), ISO/IEC14443B and the Sony FeliCa card. NFC standard ISO/IEC 18092 now ECMA 340, describe communication modes for Near Field Communication Interface and Protocol (NFCIP-1) using inductive coupling at the frequency of 13.56 MHz. It also defines the Active and the Passive communication modes ofNFCIP-1 and specifies modulation schemes, codings, transfer speeds, and frame format of the RF interface, as well as initialization schemes and conditions required for data collision control during initialization.

ECMA 352 is a Near Field Communication Interface and Protocol (NFCIP-2) standard which specifies the selection mechanism for the three communication modes of NFCIP-1 standards in such a way that ongoing communication is not disturbed. ECMA-340, ISO/IEC 14443 and ISO/IEC 15693 work on 13.56 MHz frequency and specify NFC, PCD and VCD as communication modes respectively.

This Ecma-356 specifies RF interface test methods for compliance, for NFCIP-1 devices which conform to ECMA-340. The ECMA-362 (ISO/IEC 23917) standard specifies protocol test methods for ECMA-340.

Ecma-373 Standard specifies the two-wire digital wire interface between Transceiver and Front-end and gives specifications about the signal wires, binary signals, the state diagrams and the bit encodings for three data rates.

ECMA-385 specifies the NFC-SEC secure channel and shared secret services for NFCIP-1. It also defines the PDUs and protocol for these services. These services and protocols are used by NFC-SEC cryptography standards. ECMA-386 is a NFC security series standard and explains cryptographic operations that use the Elliptic Curves Diffie-Hellman (ECDH) protocol for key agreement and the AES algorithm for data encryption and integrity. It secures communication between two NFC devices not sharing any common secret.

ECMA-390 This Standard specifies commands for NFC-WI (ECMA-373), which allow exchange of control and state information between the Transceiver and the Front-end. ECMA-403 specifies requirements to verify NFCIP-2 mode selection and initial communication in the selected modes.

NFC ecosystem is composed of a number of different industry players having versatile roles and operations. NFC industry is in a continuous evolution mode, with constant changes in dependencies on each other. The trend is towards flexibility and ease of scalability. Since NFC is an access technology and provides a number of benefits like increased mobility, easy data exchange and access, decreased physical effort, seamless device pairing and above all ability to be adapted for many scenarios, several industries and organizations providing financial services are adopting NFC technology.

Generally NFC ecosystem consists of mobile network operators, Mobile Phone Producers, banking and payment services, semiconductor (SE) producers, application developers, Trusted Service Managers (TSM), and merchants.

There are no strict boundaries between the parties involved in NFC ecosystem and no party can provide NFC experience to end customers single handedly. All the players need mutual cooperation and there should be a regulating body with regards to NFC ecosystem.

The three modes of NFC communication reader/writer mode, card emulation mode and peer to peer mode have their own uses and application scenarios. The most common usage scenario for reader/ writer mode is information gathering and writing tags. The information can be text, a URL from a smart poster or a product description. Hence, the reader/writer mode can be used for developing a wide range of applications in health, education, and entertainment. Smart posters are very common example of usage of reader/writer mode.

Card emulation mode provides the opportunity for an NFC enabled mobile device to store multiple contactless smart card applications in the secure element for example are credit card, debit card, loyalty card, transport cards, identity or access cards, key and tickets. It removes the need for physical cards. NFC enabled mobile phones provide mobility and ease also to perform everyday tasks.

Peer-to-peer mode can be used for exchanging information such as a text message, contacts, or any other kind of data for pairing, file transfer and networking operations between two NFC enabled mobiles phones. Exchanging business cards, pairing bluetooth devices, and gaming are other possible usage scenarios of this mode.

There are a number of NFC applications and a lot more opportunities for NFC in different industries as explained in [27]. For example in healthcare industry NFC can be used for remote health monitoring, controlling, tracking systems, data collection and drugs related services as evident from [19,20,21,22,23,24,25,26,].

NFC tags are used in smart environment to bring ease, simplification and automation to the existing systems and their usage like in [28, 29, 30, 31, 32,]. There are many mobile payment solutions worldwide making use of NFC technology, like e.g., Payez Mobile Project [33], Pay-Buy-Mobile Project [34], SIESTA Project [35] are some of the well-known applications.

Some other NFC based projects include ticketing systems include [36], secure m-Coupon protocol [37], payment service by Smart Touch Project [38], automated reservation and ticketing service for tourists, and a system for car parking [39,40].

The advantages of NFC in retail industry can be seen in [41, 42, 43]. Also NFC technology can be used in education industry for the interactive learning of students [44, 45, 46]. Some examples from the literature about entertainment and video games are Pass the Bomb and Whack-a-Mole game [47, 48]. NFC technology can also have a positive impact for Online

Social Networks (OSN) and can be integrated with the existing social network applications as evident from [49, 50, 51].

With NFC any object can act as a media or source of access to business and information. Virtually there is no difference between tags and objects having tags or NFC stickers, as NFC tags or sticker do not require power source for communication. We carry our GSM mobile devices every day and almost everywhere along with us. With NFC part of mobile phones, it is very easy and convenient to access any resource or give access to our secure resources like identity cards, ATMs, licenses and credit cards, as they are saved in soft copy in secure element of NFC chip in our mobile phones. So NFC is an interface between services, objects and our daily life chores.

2.4 Comparison with Other Technologies

NFC seems to have taken the characteristics of identification from RFID and two-way communication from other wireless technologies like Wi-Fi etc. Below table gives a very comprehensive comparison between NFC and other technologies [52]. The main difference between RFID and NFC is that RFID is just identification technology whereas NFC is an access technology and provides two-way communication. RFID is one way and point to multi point. NFC is device can communicate to only one device at a time.

Aspect	NFC	Bluetooth	RFID
Tag requires power	No	Yes	No
Scan Tags Simultaneously	No	Yes	yes
Standardization	ISO/IEC 14443, 18000, 15693	Bluetooth SIG	ISO 14443
Network Type	Point-to-point	WPAN	Point-to-point
Cryptography	Available	Available	Not available
Range	~ 3cm	~100 m (class 1)	~ 1m
Frequency	13.56 MHz	2.4–2.5 GHz	13.56 MHZ
Bit rate	424 kbit/s	2.1 Mbit/s	
Set-up time	< 0.1 s	< 6 s	~0.1 s
Communication	Two way	Two way	One way

Table- 3 Comparison of NFC with Bluetooth and RFID

2.5 Security in NFC

NFC has evolved from RFID and is inherently insecure. Ecma International-European association for standardizing information and communication systems developed a security protocol for NFC which lacks in a number of aspects like mutual authentication and privacy. There are a number of security vulnerabilities and attacks on NFC ecosystem comprising of NFC Endpoint Hardware, the NFC link/ communication and the backend infrastructure. These attacks include relay attack, cloning and skimming attack, eaves dropping, man in the middle, fuzzing attack, privacy, and denial of service attack. These attacks exploit vulnerabilities in all the operating modes of NFC consisting of reader/writer mode, peer to peer mode and card emulation mode, NFC Data Exchange Format (NDEF) and application loading and personalization using Over the Air (OTA) link.

2.5.1 Security Issues Related to Mobile Payments

Mobile payment refers to the use of mobile device to pay bills instead of paying with credit cards. Proximity mobile payments involve transactions, having consumer inter-acting with a PoS terminal using mobile device like contactless NFC payment [53].An NFC payment constitutes an NFC enabled mobile phone personalized with a payment application and account respectively, waved or held near a PoS terminal capable of contactless payment. The issues of cost and distribution of hardware are associated with any rollout of new technology. As mobile phones have modest cost and wide-spread ownership, the integration of contactless payment in mobile handsets is the main reason of its wide acceptance as the dominant mode of payment. Also the built-in display and keyboard is very handy for the confirmation, code entry or activa-tion/deactivation of the payment functionality.

Since the payment processing infrastructure for the proximity contactless payment is the same as that for contact payments, following are the security requirements of the mobile NFC contactless payments transactions taking place.

- **Confidentiality:** The foremost requirement is of confidentiality of the payment transaction. These transactions need to be encrypted from the source to the destination including the contactless link between the NFC mobile and the contactless POS terminal.

- **Authentication:** The NFC enabled mobile device as well as the POS terminal needs to be authenticated in order to avoid fraud through spoofing, skimming and man in the middle attacks.

- **Integrity:** The integrity of payment data needs to be ensured. There shouldn't be any modifications or replacements in the transaction data on the way between customer and POS terminal.

- **Authorization:** Once in the vicinity of the reader, the NFC card or tag activates at its own. It does not require pairing as in the case of bluetooth. Hence, the application and transactions need to be authorized before they can start the transaction.

- **Non repudiation:** Both the ends, the customer and the merchants should not be able to deny having carried out the payment transaction.

- **Privacy:** The details of the customer purchase, shopping priorities and purchase intervals, need to be kept private and confidential.

3. Related Work

The privacy issue in NFC security protocol is catered in [54] by offering only conditional privacy through pseudonyms. Since the first step in the exchange of secret in NFC security protocol is exchanging public keys, it infringes the privacy of the users. A public key is issued by the trusted third party and is updated each time a pseudonym is to be generated. The shared secret is established by exchanging the pseudonyms instead of public key. According to author, in the proposed method identity of the users in electronic payments is verified by trusted third party but the two entities communicating cannot identify each other.

In [55] author has designed a protocol for NFC communication between payer and merchant for micro and macro payments with the assumption that the merchant has the knowledge of payment amount. This very assumption limits the applicability of the protocol, as the transaction amounts can vary according to requirement. Both payer and merchant including the third party create a common secret based on some secret formula. The establishment of a shared secret is a difficult task and also hinders the scalability. The identification data for each entity is encrypted with this shared secret and is part of every message. The protocol is vulnerable to man-in-the-middle attacks and also lacks privacy as only a part of message is encrypted using a fixed key. It does not provide authentication of the entities involved as well.

For the mutual authentication between NFC device and Point of Sale (PoS) Terminal, Ceipidor et.al [56] provided a solution based on trusted third party verification of NFC phone and PoS. Since in EMV (Euro, MasterCard and VISA) proximity payments, only the card has to authenticate to the PoS terminal and micro payments don’t require the pin verification, it is possible for any illegal reader device to perform fraud payment and also get the contactless card sensitive information. Also the transactions can be performed with the stolen NFC mobile phone. Both NFC phone and PoS terminal share a secret key with authentication server and are first authenticated to authentication server AS. AS provides a common session key to both of them and random values along with timestamps are used for verification of both the parties and session. The solution uses symmetric key encryption, which can be target of man in the middle attack.

Ali et.al [57] provides a security protocol for the mobile payment system by integrating the existing GSM network with NFC. NFC mobile phone reads a NFC tag, and requests the BTS for the dedicated channel. After the verification of the client mobile phone, the channel is allocated. The NFC mobile phone verifies the payment and order information to the PoS terminal, which asks the VLR for customers account check. If the account and credit is verified, the VLR sends the transaction number to PoS.

Nadra et.al [60] proposed a payment architecture for cafeteria using NFC. The users need to register themselves first with the payment system. The request for registration and credit reload is sent by the payer to the admin through NFC. The admin sends it over the internet to the server for processing. Similarly for the payment against any item purchased is performed by first reading the tag and then sending a request to the merchant through NFC, which forwards it to the server, over the internet. Privacy is not catered as the data is not encrypted. The system gives no protection from man in the middle attack. Scalability is also an issue. The key generation and revocation is not addressed.

Urien et.al [65] also presented an authentication protocol for retail environment based on peer-to-peer payment transactions using Logical Link Control Protocol (LLCP) secured by Transport Layer Security (TLS). LLCP is an OSI layer-2 protocol which enables peer-to-peer bidirectional communication between two NFC enabled devices [66]. It provides a solid base for peer-to-peer applications by enhancing the basic functionality offered by ISO/IEC 18092 without affecting the interoperability of NFC apps and chipsets. The authentication of the customer is done by signing in with NFC enabled phone at the sign in terminal upon entering the store. Then customer scans the bar codes on different items to be purchased with his smart phone. For payment the customer brings his phone close to the PoS Terminal, which processes the transaction. In this way, it removes the bottle neck of scanning the items at the PoS terminal. During the initial signin process, the keys exchange and authentication is performed using elliptic curve based public key cryptography.

A payment system for retail environment has also been described by Cha and Kim [67], which is based on message digest authentication and for providing privacy the concept of tokenization is used. The token replaces the sensitive data of a customer. The original data is stored in the encrypted form on payment gateway server. The tokens are exchanged between client and the payment gateway server encrypted symmetrically. The payment transaction data is transferred between customer and tag, in NFC peer to peer mode. Although this approach is simple but the overall system security is dependent on the security of the server and the symmetric encryption.

In Europay, MasterCard and Visa Corporation EMVCo [58, 59] security provided in contactless payment is similar to that of chip card based contact payment. The mobile device plays the role of card. It does not play the role of PoS terminal. There is no mutual authentication of the PoS terminal and contactless card. Only contactless card is authenticated either online or offline. For offline authentication, the IC card data signed with the private key of the issuer is verified by the terminal. In case of online authentication, the dynamic data for verification to be performed by the terminal includes that provided by the IC card, the terminal and the transaction specific data. The public key certificate of the IC card is also verified by the PoS terminal.

Google Wallet app is a digital wallet application and is based on EMVCo. It provides a secure alternate to plastic credit cards, debit cards, gift cards, loyalty cards etc and enhances the functionality of android mobile devices by enabling online shopping, and monetary transactions. It also makes use of NFC tap and pay if the device is NFC-enabled [61]. Google wallet security depends on the four digits PIN required to access the application and the transmitting antenna is disabled by cutting the power supply upon locking of the screen or completion of the transaction. The credit card credentials are stored in the encrypted form on Google servers and the related wallet ID is stored on the phone. The application has a limited access to only a part of your credit card information which is stored in encrypted form on the servers. The Google wallet can be remotely disabled through online and transaction data can also be cleared [63]. There are certain issues in Google Wallet which can cause security breach and need to be addressed. According to Nelenkov [62], application protocol data units (APDUs) are not completely encrypted during installation of the Google Wallet application, and hence man-in-the-middle attack can be performed. Also there should be a limited access to SE for applets and their APDUs. The MIFARE manager applet, which is part of the Google Wallet application, is susceptible to authentication and encryption attacks. In the new versions of the application, the intention is to store and verify the pin inside Secure Element (SE) but still pin ownership issues can arise in case of any breach.

Since access to SE of a mobile device, by applications developed by third party is blocked by smartphone and OS manufacturers, Mainetti et.al [64]gave an alternate to SE and a secure NFC mobile-to-POS micropayment system based on peer-to-peer NFC operating mode for Android mobile phones. The solution is to store the encrypted credit card information in the memory of the android phone instead of the Secure Element (SE). The file is first encrypted using public key of the payment gateway server and then using symmetric key derived from the pin. When a payment is to be performed, the user selects one of configured credit card on its Android smartphone. The IDA-Pay application prompts the user to enter the PIN, which is used to decrypt the encrypted credit card file. The file is sent to the Point of Sale PoS terminal through NFC peer to peer link, which acts as a Relaying Party (RP) to forward the credit card file to the payment gateway which is connected to the financial networks. The key distribution, confirmation and revocation for public key encryption are not elaborated in detail. Also the authentication of the user and authorization is based on the pin which can be subject to brute force attack.

The trial of a contactless mobile payment via paypass terminal which is compatible with EMV is presented in this paper [68]. The access to payment application is given on entering the PIN. The user is authenticated using combined data authentication for online transaction. The author used common criteria to evaluate the security of the NFC link between application and PoS terminal and the results presented in the paper were satisfactory.

3.1 Critical Analysis

Most of the existing solutions and work is for specific scenarios and environment. It lacks in independence of system, hardware and platform. Most of the solutions provide protection from only common limited attacks to mobile payment systems. If any work caters the privacy, it lacks the authentication aspect of the mobile payments. Also mutual authentication is lacking, which is very important aspect of financial transactions.

As presented in the table below, compared to other protocols for NFC based financial applications, our protocol provides a solution to most of the existing problems faced by NFC transactions such as confidentiality, mutual authentication, integrity, authorization and non-repudiation. Specifically mutual authentication is considered as the most important aspect for any financial transaction. Our protocol not only ensures that the certificates are verified but also makes sure that the entity claiming a public key has the corresponding private key. In other words, it does not only authenticate the existence of an entity but also ensures its willingness to communicate and nonrepudiation. The one time session key provides privacy to the user, in case the attacker is observing the shopping preferences and its intervals. Another advantage of our protocol is that, it is not limited to any specific domain or environment and can be applied for healthcare system, NFC immigration system and Physical Access Control etc. Furthermore, the designed protocol is not dependent on any third party for its functioning as in case of some of the solutions discussed in literature survey.

	Mutual Authentication	Confidentiality	Integrity	Non Repudiation	Authorization	Prior Knowledge	Third Party	Privacy
Husni et.al		✓	✓		✓	✓	✓	
Hasoo et.al		✓	✓				✓	✓
Ceipidor et.al		✓			✓		✓	
Ali et.al		✓	✓		✓		✓	
EMVCo		✓	✓		✓			
Nadra et.al			✓					
Google Wallet		✓	✓		✓		✓	

Mainetti et.al		✓			✓			
Urien et.al	✓	✓	✓		✓	✓		✓
Cha & Kim	✓	✓	✓			✓		✓
Pasquet et.al		✓	✓		✓			

Table- 4 Comparison with the Related Works

4. Architecture for NFC based Financial Transactions

4.1 Introduction

Our designed protocol consists of five entities as shown in the Figure 1. These entities are: Identity Management System, Certification Authority, Authentication and Authorization Server, Mobile PoS terminal, and NFC enabled mobile phone.

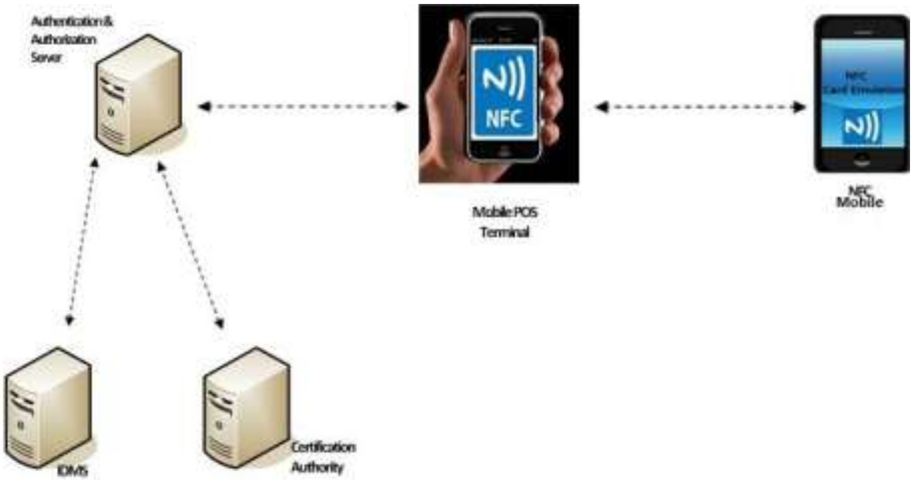


Figure- 4 Architecture Diagram for NFC based Financial Transactions

4.1.1 Identity Management System (IDMS)

In our protocol, it is assumed that all the valid users of the payment system are registered with IDMS. It maintains identities, required information about the users, and information about NFC mobile. It manages all the steps of Identity Management Life Cycle. It also holds the database of users PIN which are stored in hashed and encrypted format.

4.1.2 Certification Authority (CA)

CA issues public key certificates to all NFC mobiles used by the customers and also the mobile PoS terminals. The verification of users and PoS terminal's certificates is also done by CA. The CA uses its private key to sign the sensitive data and the public key certificates, during the process of personalization of card and PoS terminal. The signed data and the CA's public key are loaded in the secure element of mobile device.

4.1.3 Authentication and Authorization Server

Based on our security protocol, Authentication and Authorization server authenticates the NFC mobile applet of the customers and also authorizes the transactions. The users are authenticated on the basis of their verification against the IDMS identity database and Certification Authority. We used extended FIPS-196 standard for authentication. The authorization of transactions to the users is managed by using XACML 3.0 standard.

4.1.4 Mobile PoS Terminal

Financial applications are network sensitive and require end-to-end node security. For financial wireless applications in a distributed environment, a security mechanism at the application layer is critical. Mobile Point of Sale (MPoS) terminal contains our application, which carries financial transaction over NFC. The application is securely stored in Secure Element (SE) and the transactions are secured over the wireless link through our protocol. The mobile PoS terminal is certified. It passes the certificate of the customer and his identity to authentication and authorization server for verification. It also forwards PIN hash to authentication and authorization server for verification and hence authorizes the transaction. Once the certificates are verified and pin is matched and challenge response is complete, it allows the transaction and also secures the link between itself and NFC mobile through encryption.

4.1.5 NFC Enabled Mobile Phone

NFC enabled mobile phone's NFC chip card contains an applet that processes the requests from the PoS application and thus securing the transaction over the wireless link.

4.2 Security Protocol for NFC Enabled Mobile Devices

When NFC enabled mobile comes in the range of Mobile PoS terminal, the terminal initiates the communication by generating a field and requests for the certificate. The card responds by sending its certificate for authentication. The initial communication comprising of certificates exchange and challenge response is for the mutual authentication of NFC mobile and terminal. Once both the ends are authenticated and the keys have been verified, then the one time session key is sent by the terminal to the NFC mobile using public key encryption. The symmetrically encrypted pin is sent by the NFC mobile to the terminal, authenticating it locally to carry out the transaction. The transactions are encrypted and hashes are sent to ensure the integrity of the transactions.

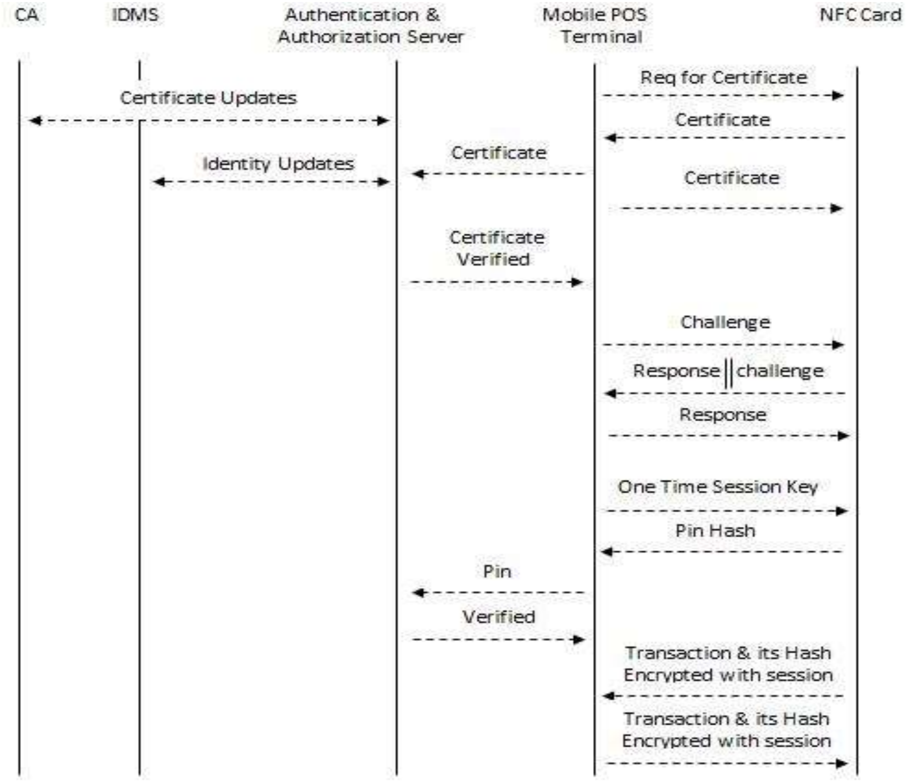


Figure-5 Security Protocol for NFC Enabled Mobile Devices Used in Financial Applications

Authentication and authorization server requests updates after regular interval from CA and IDMS. CA and IDMS respond by sending the latest changes in certificates and identities respectively. Authentication and authorization server updates its database.

Once NFC mobile is in the range of mobile PoS terminal, the PoS terminal requests the card for certificate. The NFC mobile sends its certificate containing public key of the card and ID of the card and applet. The PoS terminal forwards the IDs and certificate to the Authentication and Authorization server for verification. The PoS then sends its certificate. NFC mobile applet extracts the certification authority root key and authenticates the POS terminal's certificate, validating that the certificate is issued by the correct issuer and is authentic. This verifies the certificate and ID and activates the relevant applet.

Once the NFC mobile applet certificate is verified, the PoS terminal sends the challenge (like in FIPS-196) to the NFC mobile and also retains it.

Challenge from the PoS terminal: $T_N \mid T_t \mid T_{ID}$

Where T_N is nonce generated by the terminal, T_t is the timestamp and T_{ID} is the identity of the PoS terminal. The NFC mobile applet signs the challenge with its private key using RSA. And also generates a challenge for the PoS terminal and sends it to the terminal.

$$C_{ID} \mid RSA_{Sign}\{(T_N \mid T_t \mid T_{ID}), K_{Priv}\} \mid C_N \mid C_t$$

Where C_N is nonce generated by the card, C_t is the timestamp and C_{ID} is the identity of the NFC mobile applet.

The terminal decrypts and verifies the response. It then signs the challenge with its private key using RSA and sends it to the card.

$$RSA_{Sign}\{(C_N \mid C_t \mid C_{ID}), K_{Priv}\}$$

The NFC mobile applet decrypts the response and verifies it. After the verification of responses from both the sides, the authentication, both remote (via certificates) and local authentication (via challenge response) is completed. Challenge response ensures that the entity is available and willing, whose certificate is being verified providing nonrepudiation. It also ensures whether the person or the device having the certificate also possess the corresponding private key. This process also helps avoid fake, forged and stolen certificates. There are two steps involved in the verification of certificate. The first step is to verify originality of certificate by signature verification. Then revocation and expiry of the certificate is checked.

The PoS terminal then generates One Time Session Key and sends it to the NFC mobile for use in encryption during the session. The key is sent, first signed with the private key of the terminal and then encrypted with the public key of the NFC card.

$\text{RSA}_{\text{ENCRPT}}$ {RSA_{Sign} (One Time Session Key, K_{Priv}), K_{Pub}}

Once the one time session key is exchanged, rest of the session is encrypted using AES. For local authentication the NFC mobile applet calculates the PIN hash using message digest algorithm MD5 and sends it encrypted with the session key.

$\text{AES}_{\text{ENCRYPT}}$ (Pin Hash, K_{Session})

The terminal decrypts it and sends it to the Authentication and Authorization server for verification against the hash database. All of the financial transactions are sent encrypted with One Time Session Key using AES along with their hash calculated with using MD5.

$\text{AES}_{\text{ENCRYPT}}$ (Transaction +Hash, K_{Session})

5. Implementation and Analysis of Protocol

The proof of concept consists of a prototype mobile PoS application for Android operating system developed in Java. The corresponding java applet has been developed by using java card framework 3.0 Classic Edition uploaded. The PoS application detects (discovers) the target card and initializes java applet. After establishing connection, PoS Terminal sends APDU to fetch the certificate stored in the smart card. The certificate and keys for the card are stored in the applet buffer in the form of byte array. PoS terminal listens for NFC applet for its availability. Upon finding the NFC applet, it requests for the certificate. The CLA instruction value is for application-specific class of instruction. We have defined our own application-specific INS values, given in the table below.

INS Value	Command Description
01	Reader requests certificate
02	Reader sends its certificate
03	Reader sends challenge and asks for response
04	Reader sends response and asks for verification
05	Reader sends One Time Session key and asks for PIN

Table-5 Instruction Values for the Applet

The sequence of commands and response APDUs are as follow:

```
// code of CLA byte in the command APDU header for Security Protocol NFC

final static byte SP_CLA = (byte) 0x80;

// codes of INS byte in the command APDU header
//Certificate request form APP from PoS

final static byte CERT_REQ_FROM_APP = (byte) 0x10;

//Challenge from PoS

final static byte CHALLENGE = (byte) 0x20;
```

```
//Session Key from PoS

final static byte SESSION_KEY = (byte) 0x30;

//Certificate request form CARD from PoS

final static byte CERT_REQ_FROM_CARD = (byte) 0x10;
```

Since first request from mobile PoS terminal is request for certificate so the NFC card will fetch the certificate from its buffer and then sends back to the terminal. The send certificate function of our Applet performed this task as shown in following piece of code.

```
case CERT_REQ_FROM_APP:
        sendCerticate(apdu);
        return;
```

After exchanging certificates, the PoS Terminal sends challenge to the NFC card. The NFC card’s applet received this challenge and signs with private key corresponding to the card’s certificate. We implemented this function in signChallenge-WithRSA(apdu) as specified in following code.

```
//if incoming APDU request is to sign challenge.

case CHALLENGE:
{
m_sign=Signature.getInstance(Signature.ALG_RSA_SHA_PKCS1, false);

// initialize signature with private key and a signature mode

m_sign.init(m_privateKey, Signature.MODE_SIGN);

// encrypting incoming challenge

short signLen= m_sign.sign(buffer, ISO7816.OFFSET_CDATA, (byte) numBytes,m_ramArray, (byte) 0);

//sending encrypted challenge

short le = apdu.setOutgoing();
apdu.sendBytes(m_sign, signLen, le);
```

}

The other functions specified in the design of protocol are implemented in the same fashion and their APDUs are as follow:

PoS Terminal (Reader) requests the card for certificate.

CLA	INS	P1	P2
80	01	00	00

Card's Response with its certificate in response body.

Body	Trailer	
Data Field	SW1	SW2
2d 2d 2d 2d 2d 42 45 47 49 4e 20 43 45 52 54 49 46 49 43 41 54 45 2d 2d 2d 2d 2d 4d 49 49 42 6c 54 43 42 2f 77 49 47 41 55 75 63 6b 75 58 4c 4d 41 30 47 43 53 71 47 53 49 62 33 44 51 45 42 43 77 55 41 4d 42 45 78 44 7a 41 4e 42 67 4e 56 42 41 4d 54 42 6d 6c 7a 63 33 56 6c 63 6a 41 65 46 77 30 78 4e 54 41 79 4d 54 63 78 4d 6a 41 30 4d 44 5a 61 46 77 30 78 4e 54 41 79 4d 44 49 79 4d 44 49 79 4d 54 64 61 4d 42 45 78 44 7a 41 4e 42 67 4e 56 42 41 4d 54 42 6e 4a 6c 59 57 52 6c 63 6a 43 42 6e 7a 41 4e 42 67 6b 71 68 6b 69 47 39 77 30 42 41 51 45 46 41 41 4f 42 6a 51 41 77 67 59 6b 43 67 59 45 41 6f 2f 4b 6e 7a 43 49 6b 49 71 57 46 4a 79 2f 35 66 4c 54 57 39 7a 54 69 35 35 42 55 59 35 49 76 64 73 6f 78 4a 49 73 39 49 46 6b 37 76 44 46 68 6c 34 59 6d 4f 58 41 38 61 57 41 6d 2b 30 65 5a 44 62 72 72 55 50 62 6d 54 4c 30 65 33 44 39 30 6b 6a 55 44 47 2f 33 59 41 6e 69 39 38 45 41 45 64 70 57 59 39 70 46 59 33 45 51 78 2b 30 67 4f 53 2f 51 4b 4d 67 44 54 70 50 7a 75 51 42 4c 6d 32 57 46 57 78 79 51 71 57 42 45 55 7a 39 41 62 38 6a 53 32 6e 63 4d 57 47 48 66 45 36 59 39 54 77 6b 70 53 37 49 67 67 56 45 73 43 41 77 45 41 41 54 41 4e 42 67 6b 71 68 6b 69 47 39 77 30 42 41 51 73 46 41 41 4f 42 67 51 42 34 4e 6a 49 42 54 62 43 4e 6a 6d 68 44 64 5a 7a 5a 41 54 30 37 7a 57 38 71 62 7a 49 45 4f 58 56 4b 6f 6b 55 41 7a 34 43 58 43 46 7a 4e 4f 50 34 6c 48 52 59 70 4c 32 58 6c 72 30 6e 52 74 71 54 68 63 63 46 74 73 31 37 50 47 37 36 33 54 74 76 46 69 6b 51 50 32 46 4a 55 4f 4e 43 64 75 66 47 53 51 4d 4e 32 76 36 56 64 41 38 54 73 56 69 37 58 4d 78 62 71 74 5a 38 66 2f 37 55 53 62 44 67 33 4e 4a 37 74 4b 6c 6f 79 72 2f 37 49 63 73 41 68 4e 75 67 72 4f 73 62 66 55 68 62 6f 43 4c 57 39 6b 47 79 6b 50 72 70 6b 31 41 3d 3d 2d 2d 2d 2d 2d 45 4e 44 20 43 45 52 54 49 46 49 43 41 54 45 2d 2d 2d 2d 2d	90 00	

PoS Terminal sends its certificate to the card. The card verifies this certificate and the INS value for this instruction is 02.

CLA	INS	P1	P2	Lc	Data Field
80	02	00	00	Ff	2d 2d 2d 2d 2d 42 45 47 49 4e 20 43 45 52 54 49 46 49 43 41 54 45 2d 2d 2d 2d 2d 4d 49 49 42 6b 7a 43 42 2f 51 49 47 41 55 75 63 6b 75 56 2b 4d 41 30 47

					43 53 71 47 53 49 62 33 44 51 45 42 43 77 55 41 4d 42 45 78 44 7a 41 4e 42 67 4e 56 42 41 4d 54 42 6d 6c 7a 63 33 56 6c 63 6a 41 65 46 77 30 78 4e 54 41 79 4d 54 63 78 4d 6a 41 30 4d 44 5a 61 46 77 30 78 4e 54 41 79 4d 44 49 79 4d 44 49 79 4d 54 64 61 4d 41 38 78 44 54 41 4c 42 67 4e 56 42 41 4d 54 42 47 4e 68 63 6d 51 77 67 5a 38 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 67 59 30 41 4d 49 47 4a 41 6f 47 42 41 4a 74 33 74 57 65 46 4e 44 34 74 42 66 68 57 35 56 4f 36 42 71 36 56 58 6c 36 33 4b 48 41 74 65 78 61 32 36 32 46 63 37 36 79 45 2f 71 58 73 41 52 5a 57 47 39 6e 72 57 62 44 6d 79 4c 6e 52 4c 62 6a 54 61 2f 41 49 38 63 69 56 56 59 75 4d 51 62 2b 42 4a 41 59 6f 2f 62 67 58 4a 49 71 74 51 4d 50 59 4e 70 63 47 4d 6a 6f 6b 50 4f 36 54 4d 4e 2f 4d 4e 6c 50 4d 63 70 59 66 58 74 48 6b 5a 39 52 39 55 34 57 56 4e 41 5a 53 53 4a 4b 6f 51 67 35 65 34 45 76 37 68 69 37 38 46 71 43 4d 78 4e 43 58 31 62 56 4f 66 4a 32 76 41 67 4d 42 41 41 45 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 4c 42 51 41 44 67 59 45 41 63 65 55 56 53 42 54 56 75 77 50 46 79 43 57 62 61 32 6a 63 77 61 5a 41 63 39 31 4a 62 5a 57 30 6e 54 34 38 7a 38 37 4e 31 66 4d 32 49 6f 71 37 6c 54 57 71 44 4c 53 73 62 38 68 65 31 67 43 4c 6f 46 59 55 6a 56 58 44 7a 30 33 74 4e 35 5a 6a 67 52 71 61 79 34 58 72 30 50 4b 6c 76 2b 62 4a 39 56 33 4c 36 55 74 31 49 4b 73 2b 59 55 30 79 42 71 7a 57 30 41 51 63 6a 70 33 4a 41 45 30 6f 46 6b 6c 41 6f 67 4d 6b 63 33 47 66 30 56 30 71 42 33 4e 63 57 67 35 49 62 47 36 48 65 47 5a 43 77 34 6f 30 36 55 6d 36 30 44 45 3d 2d 2d 2d 2d 2d 45 4e 44 20 43 45 52 54 49 46 49 43 41 54 45 2d 2d 2d 2d 2d

At any stage of the protocol, if the corresponding party (either PoS terminal or Card) becomes dubious, the other party stops the process and sends an APDU showing execution error.

Body	Trialer	
Data Field	SW1	SW2
	64 00	

PoS terminal sends the challenge to the card and instructs it to respond by responding the challenge and and also sending its own challenge.

CLA	INS	P1	P2	Lc	Data Field	Le
80	03	00	00	22	31 39 31 35 37 32 34 34 36 7c 31 34 33 30 33 31 39 31 35 37 37 31 39 7c 30 30 30 30 30 30 30 30 30 39	Cf

The card responds to the challenge from the PoS terminal.

Body	Trialer	
Data Field	**SW1**	**SW2**
30 30 30 30 30 30 30 30 31 30 7c 35 33 37 39 31 39 38 39 32 7c 31 34 33 30 33 31 39 31 35 38 35 34 32 7c 69 38 7a 44 57 34 48 31 62 67 31 54 62 42 74 6b 39 57 37 6f 65 2f 42 69 4a 76 47 41 4a 70 78 44 64 31 4c 45 61 56 36 59 4e 43 6f 68 69 72 75 32 4a 68 4d 4e 7a 35 37 58 74 2f 61 2b 69 77 53 6f 4b 51 31 6d 75 6f 49 78 42 6e 73 59 6f 34 73 74 33 74 36 56 74 67 58 68 6a 4b 44 4b 31 4d 33 55 2f 54 6a 54 43 34 77 6a 71 56 6a 4f 42 70 79 74 47 31 53 41 6a 47 67 6f 78 37 34 63 77 37 53 2f 30 42 30 38 78 53 4b 62 71 4b 38 57 52 55 69 4e 5a 6f 4d 41 2b 65 4a 72 31 68 2f 62 55 64 56 4c 5a 63 64 64 75 47 70 61 69 76 41 3d	90 00	

The PoS terminal verifies the response and also sends its response to the card challenge and instructs the card to verify it.

CLA	INS	P1	P2	Lc	Data Field	Le
80	04	00	00	ac	48 4d 78 46 45 38 4e 75 66 56 4a 4b 74 6f 52 42 49 43 38 61 73 78 4b 72 49 49 47 54 2b 2f 75 6b 68 30 4d 30 4d 73 42 72 74 76 43 5a 6e 76 69 34 75 4a 48 38 68 68 34 77 54 62 44 41 69 66 46 4e 56 45 69 6c 53 35 65 33 44 6d 71 75 58 63 37 42 33 64 65 67 66 63 54 75 4c 69 72 6a 78 71 4c 73 44 61 62 4e 2b 52 57 6d 42 69 64 64 73 6f 73 46 42 50 6f 74 4c 6b 56 68 42 54 75 35 36 4b 49 55 36 48 51 79 68 55 34 6f 69 42 59 37 32 62 7a 35 73 46 50 52 35 2b 67 56 32 68 6d 37 43 4b 4e 73 52 32 47 4c 6c 75 50 66 32 49 45 3d	10

Card responds to the reader by sending ok.

Body	Trailer	
Data Field	**SW1**	**Sw2**
4f 4b	90 00	

The PoS terminal creates and sends one time session key encrypted with the public key encryption and instructs the card to decrypt it and use it for encrypting future conversation including pin.

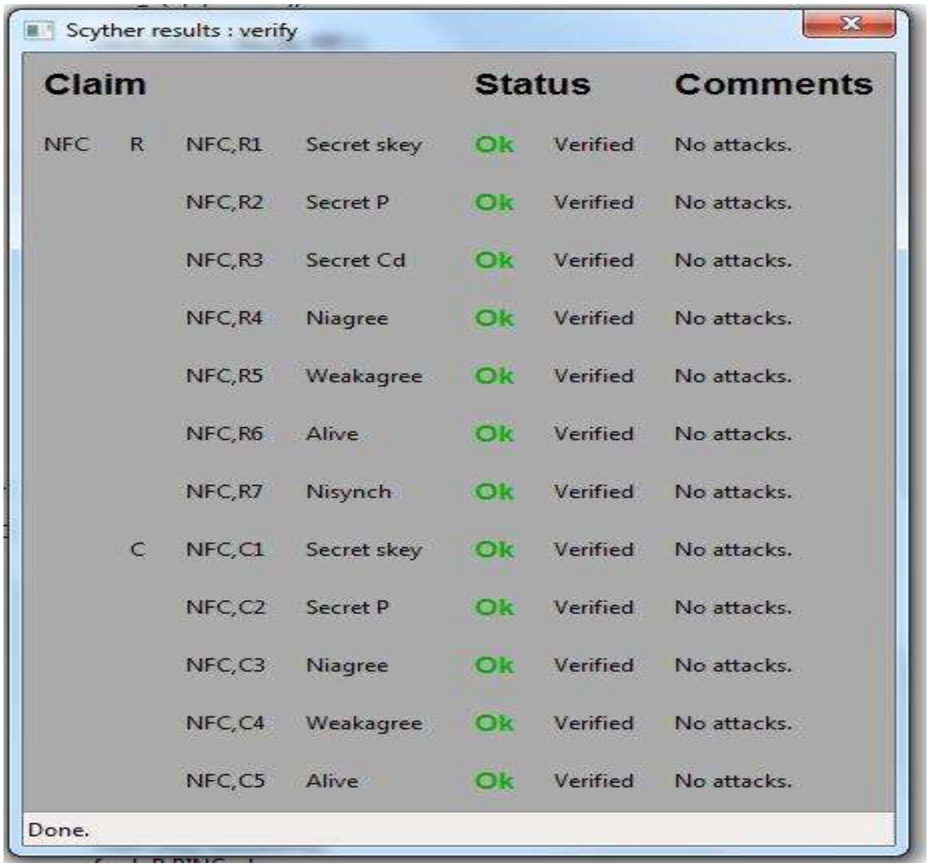
CLA	INS	P1	P2	Lc	Data Field	Le
80	05	00	00	Ff	6a 4a 58 34 61 4a 44 7a 78 51 67 5a 6a 36 50 66 57 76 70 6c 43 73 48 4b 6e 46 58 4e 78 4c 5a 4f 39 6e 45 57 48 73 4e 4e 53 6d 68 6e 6f 6b 71 4a 55 6c 66 4e 59 2f 76 6b 47 49 5a 4b 44 38 5a 67 65 4b 70 48 53 66 52 4d 6f 65 54 61 54 79 76 4b 77 69 70 31 32 70 72 46 70 31 39 53 73 45 52 43 51 34 4e 54 62 31 38 78 61 53 61 6a 71 4f 6b 6d 74 77 68 35 36 6e 76 63 49 68 4c 30 62 50 49 36 31 64 59 7a 75 51 4f 4f 66 30 66 64 33 50 77 77 43 49 44 2f 75 72 74 78 65 50 55 79 76 77 71 4f 76 62 45 49 33 4e 62 6c 44 53 64 4b 6c 6d 42 30 7a 4d 56 58 47 48 78 52 4c 4f 6e 4c 34 58 4d 7a 53 67 43 4f 69 45 76 6e 4a 54 37 35 79 6c 61 4f 59 2f 72 42 4b 59 6d 54 43 44 74 35 52 48 61 45 38 37 37 6e 44 4e 32 43 38 59 45 39 49 38 79 66 73 59 2f 6d 50 47 4c 56 6a 30 44 6b 45 5a 54 4c 50 6b 45 59 50 5a 64 5a 47 62 61 64 78 63 6d 57 41 41 58 74 2b 71 49 55 4c 50 65 35 51 4a 36 79 4f 68 42 55 59 6b 31 66 76 33 6d 46 75 64 43 62 4a 61 69 51 6f 78 4c 68 6f 4b 36 6b 69 33 58 6e 35 50 32 76 6d 50 2f 58 6c 64 34 64 33 30 59 31 71 43 61 70 4d 51 3d 3d	10

The Card responds by sending the PIN hash for local authentication. As soon as the PIN is verified, the financial application is loaded and starts transactions.

Body	Trailer	
Data Field	SW1	SW2
cb f4 f5 6c b9 152 e2 cc ff 1 47 160 5f bf 57 2122	90 00	

5.1 Scyther Verification

After designing security protocol for NFC mobile used in financial application, we analyzed it with Scyther [29], which is an automated security verification tool. The complete formal code for verification is shown in Appendix. The results generated through Scyther are shown in Fig. 3. In this verification, we assumed that all the credentials and sensitive data are safely stored in tamper resistant chip (SE) at POS terminal as well as NFC mobile. The adversary has access to the mobile PoS terminal and the NFC link between the PoS terminal and the NFC mobile. We specified in it, that the adversary can modify and create messages between the two ends in order to tamper the messages and launching replay attack as man-in-the-middle.



Scyther results : verify

Claim				Status		Comments
NFC	R	NFC,R1	Secret skey	Ok	Verified	No attacks.
		NFC,R2	Secret P	Ok	Verified	No attacks.
		NFC,R3	Secret Cd	Ok	Verified	No attacks.
		NFC,R4	Niagree	Ok	Verified	No attacks.
		NFC,R5	Weakagree	Ok	Verified	No attacks.
		NFC,R6	Alive	Ok	Verified	No attacks.
		NFC,R7	Nisynch	Ok	Verified	No attacks.
	C	NFC,C1	Secret skey	Ok	Verified	No attacks.
		NFC,C2	Secret P	Ok	Verified	No attacks.
		NFC,C3	Niagree	Ok	Verified	No attacks.
		NFC,C4	Weakagree	Ok	Verified	No attacks.
		NFC,C5	Alive	Ok	Verified	No attacks.

Done.

Figure-6 Verification of the Security Protocol Using Scyther Verification Tool

The secrecy attribute of the verification expresses that the confidentiality of the session key, PIN and the transaction data over an untrusted network is secured by our protocol during execution.

Authentication is the guarantee that the intended and aware partner is communicating in the network and as the protocol runs, the messages are transmitted exactly in the desired sequence. It is described by the properties of aliveness and synchronization. Aliveness property ensures that the communicating parities, both NFC mobile and PoS terminal are present and responding to each other. Synchronization is the exact exchange of the messages between the corresponding runs, for every entity as described in the protocol. It is possible, by ensuring that each entity performs its described role in the protocol. Agreement property of tool describes that, both the entities after successful corresponding execution, agree on the values of data variables. Satisfying aliveness, injective synchronization, non-injective synchronization and non-injective agreement property ensures the protection against man-in-the-middle attack, spoofing, skimming and replay attacks. Signed messages are used to meet the non-repudiation requirement of the protocol.

5.2 Scyther Script

```
usertype Certificate, TimeStamp, ReaderID, CardID, Data,
SessionKeY,PINCode;
protocol NFC(R,C)
{
role R
 {
  fresh RID: ReaderID;
var  CID: CardID;
fresh Rn: Nonce;
var Cn: Nonce;
fresh Rt: TimeStamp;
var Ct: TimeStamp;
fresh Rd: Data;
var Cd: Data;
hashfunction H;
fresh  CertR: Certificate;
var CertC:  Certificate;
fresh skey:SessionKey;
var P:PINCode;

   send_1(R,C,   CertR);
recv_2(C,R,   CertC);
send_3(R,C,   Rn, Rt, RID );
recv_4(C,R,   Cn, Ct, CID, {Rn, Rt, RID}sk(C));
send_5(R,C,   {Cn, Ct, CID}sk(R));
send_6(R,C,   {{skey}sk(R)}pk(C))
recv_7(C,R,   {H(P)}skey);
send_8(R,C,   {Rd}skey);
recv_9(C,R,   {Cd}skey);

     claim_R1(R,Secret,skey);
claim_R2(R,Secret,P);
claim_R3(R,Secret,Cd);
claim_R4(R,Niagree);
claim_R5(R,Weakagree);
claim_R6(R,Alive);
claim_R7(R,Nisynch);
}

role C
  {
      var RID: ReaderID;
      fresh CID: CardID;
var Rn: Nonce;
fresh Cn: Nonce;
var Rt: TimeStamp;
fresh Ct: TimeStamp;
var Rd: Data;
fresh Cd: Data;
hashfunction H;
var  CertR: Certificate;
fresh CertC:  Certificate;
fresh skey:SessionKey;
fresh P:PINCode;

 recv_1(R,C,   CertR);
send_2(C,R,   CertC);
recv_3(R,C,   Rn, Rt, RID );
send_4(C,R,   Cn, Ct, CID, {Rn, Rt, RID}sk(C));
recv_5(R,C,   {Cn, Ct, CID}sk(R));
recv_6(R,C,   {{skey}sk(R)}pk(C));
send_7(C,R,   {H(P)}skey);
recv_8(R,C,   {Rd}skey);
send_9(C,R,   {Cd}skey);

  claim_C1(C, Secret, skey);
claim_C2(C,Secret, P);
claim_C3(C, Niagree);
claim_C4(C, Weakagree);
claim_C5(C, Alive);
}
}
```

6. References

1. Abi Research, https://www.abiresearch.com/press/nfc-will-come-out-of-the-trial-phase-in-2013-as-28. Accessed on 27th June 2014.
2. Mastercard, http://newsroom.mastercard.com/press-releases/mastercard-to-use-host-card-emulation-hce-for-nfc-based-mobile-payments/. Accessed on 27th June 2014.
3. Wikipedia, http://en.wikipedia.org/wiki/Google_Wallet. Accessed on 27th June 2014.
4. Hasoo Eun, Hoonjung Lee, Heekuck Oh, "Conditional Privacy Preserving Security Protocol for NFC Applications", In: Consumer Electronics (ICCE), IEEE International Conference Volume 59, 4 April, 2013.
5. Near Field Communication (NFC) Technology and Measurements White Paper ROHDE & SCHWARZ
6. http://www.nfclab.com/aboutnfc.html
7. Globalplatform, http://www.globalplatform.org/mediaguideSE.asp. Accessed on 27th June 2014.
8. Smartcard allaince, http://www.smartcardalliance.org/resources/webinars/Secure_Elements_101_FINAL3_032813.pdf . Accessed on 27th June 2014.
9. Omkar Ghag, Saket Hegde, "A Comprehensive Study of Google Wallet as an NFC Application", In: International Journal of Computer Applications, Volume 58, November 2012.
10. Chunxiao Li, Raghunathan A, Jha, N.K. A, "Trusted Virtual Machine in an Untrusted Management Environment", In: Services Computing, IEEE Transactions,
11. Volume: 5 , Issue: 4, Fourth Quarter 2012.
12. Young-Ho Kim, Jeong-Nyeo Kim, "Building Secure Execution Environment for Mobile Platform", In: Computers, Networks, Systems and Industrial Engineering (CNSI), 23-25 May 2011.

13. Anwar W, Lindskog D, Zavarsky P, Ruhl R, “Redesigning Secure Element Access Control for NFC Enabled Android Smartphones using Mobile Trusted Computing”, In: Information Society (i-Society), 2013 International Conference, 24-26 June 2013.
14. Ahmad Z , Francis L , Ahmed T , Lobodzinski C , Audsin D, Peng Jiang, “Enhancing the Security of Mobile Applications by using TEE and (U)SIM”, In: Ubiquitous Intelligence and Computing, 2013 IEEE 10th International Conference on Autonomic and Trusted Computing (UIC/ATC), 18-21 Dec,2013.
15. NFC world, http://www.nfcworld.com/2012/09/25/318059/inside-secure-to-offer-cloud-based-nfc-secure-element-solution/. Accessed on 27th June 2014.
16. http://developer.android.com/about/versions/kitkat.html#44-hce. Accessed on 27th June 2014.
17. http://tomnoyes.wordpress.com/2013/11/01/hce-kills-isis/. Accessed on 27th June 2014.
18. http://www.ecma-international.org/publications/standards/Standard.html
19. http://developer.android.com/reference/android/nfc/tech/NfcV.html
20. Bravo, J., Hervas, R., Fuentes, C., Chavira, G., & Nava, S. W. (2008). Tagging for nursing care. In Proceedings of second international conference on pervasive computing technologies for healthcare, Tampere, pp. 305–30.
21. Bravo, J., et al. (2008). Enabling NFC technology to support activities in an Alzheimer’s day center. In Proceedings of the 1st international conference on pervasive technologies related to assistive environments, Athens, Greece.
22. http://www.bbc.com/news/technology-30036137
23. Iglesias, R., et al. (2009). Experiencing NFC-based touch for home healthcare. In Proceedings of the 2nd international conference on pervasive technologies related to assistive environments, Corfu, Greece.
24. Marcus, A., Davidzon, G., Law, D., Verma, N., Fletcher, R., Khan, A., et al. (2009). Using NFC-enabled mobile phones for public health in developing countries. In Proceedings of the 1st international workshop on near field communication, Hagenberg, Austria, pp. 30–35
25. Strömmer, E., et al. (2006). Application of near field communication for health monitoring in daily life. In Proceedings of 28th annual international conference of the

IEEE Engineering in Medicine and Biology Society, New York City, USA, pp. 3246–3249.

26. Morak, J., Hayn, D., Kastner, P., Drobics, M., & Schreier, G. (2009). Near field communication technology as the key for data acquisition in clinical research. In Proceedings of the 1st international workshop on near field communication, Hagenberg, Austria, pp. 15–19.
27. Jara, J., et al. (2010). Drugs interaction checker based on IoT. In Proceedings of internet of things, Tokyo, pp. 1–8.
28. A Survey on Near Field Communication (NFC) Technology Vedat Coskun · Busra Ozdenizci Kerem Ok Published online: 1 December 2012 © Springer Science + Business Media New York 2012
29. Steffen, R., Preißinger, J., Schöllermann, T.,Müller,A.,&Schnabel, I. (2010).Near field communication (NFC) in an automotive environment. In Proceedings of the 2nd international workshop on near field communication, Monaco, pp. 15–20.
30. Isomursu, M. (2008). Tags and the city. PsychNology Journal, 6(2), 131–156
31. Siira, E., & Haikio, J. (2007). Experiences from near-field communication (NFC) in a meal service system. In Proceedings of 1st annual RFID Eurasia, Istanbul, Turkey, pp. 1–6.
32. Chang, Y., Chang, C., Hung, Y., & Tsai, C. (2010). NCASH: NFC phone-enabled personalized context awareness smart-home environment. Journal of Cybernetics and Systems, 41(2), 123–145.
33. Chang, Y., et al. (2009). Toward a NFC phone-driven context awareness smart environment. In Proceedings of symposia and workshops on ubiquitous, autonomic and trusted computing, Brisbane, QLD, pp. 298–303.
34. Payez Mobile. http://www.payezmobile.com
35. GSMA. (2007). Pay-buy mobile business opportunity analysis, version 1.0. White paper. Available at: http://www.gsmworld.com/documents/gsma_nfc_tech_guide_vs1.pdf.
36. Baldo, D., Benelli, G., & Pozzebon, A. (2010). The SIESTA project: Near Field Communication, based applications for tourism. In Proceedings of 7th international symposium on communication systems networks and digital signal processing, Newcastle upon Tyne, pp. 721–725.

37. Ghiron, S. L., Sposato, S., Medaglia, C. M. & Moroni, A. (2009). NFC ticketing: A prototype and usability test of an NFC-based virtual ticketing application. In Proceedings of the first international workshop on near field communication, Hagenberg, Austria, pp. 45–50.
38. Dominikus, S., & Aigner, M. (2007). mCoupons: An application for near field communication (NFC). In Proceedings of 21st international conference on advanced information networking and applications workshops, Niagara Falls, pp. 421–428.
39. Pasquet, M., et al. (2008). Secure payment with NFC mobile phones in the smart touch project. In Proceedings of international symposium on collaborative technologies and systems, Irvine, CA, pp. 121–126.
40. Baldo, D., Benelli, G., & Pozzebon, A. (2010). The SIESTA project: Near Field Communication, based applications for tourism. In Proceedings of 7th international symposium on communication systems networks and digital signal processing, Newcastle upon Tyne, pp. 721–725.
41. Benelli, G., & Pozzebon, A. (2010). An automated payment system for car parks based on near field communication technology. In Proceedings of international conference for internet technology and secured transactions (ICITST), London, pp. 1–6.
42. Lou, Z. (2010). NFC enabled smart postal system. In Proceedings of the 2nd international workshop on near field communication, Monaco, pp. 33–38.
43. Nepper, P., Konrad, N., & Sandner, U. (2007). Talking media. In Proceedings of 9th international conference on human computer interaction with mobile devices and services, Singapore.
44. Ok, K., Coskun, V., & Aydin, M. N. (2010). Usability of mobile voting with NFC technology. In Proceedings of IASTED international conference on software engineering, Innsbruck, Austria, pp.151–158.
45. Garrido, P. C., et al. (2011). Use of NFC-based pervasive games for encouraging learning and student motivation. In Proceedings of 3rd international workshop on near field communication, Hagenberg, Austria, pp. 33–37.
46. Ervasti, M., et al. (2009). Experiences from NFC supported school attendance supervision for children, In Proceedings of third international conference on mobile ubiquitous computing, systems, services and technologies, Sliema, pp. 22–30.

47. Sodor, B., Fordos, G., Doktor, T., & Benyo, B. (2011). Building a contactless university examination system using NFC. In Proceedings of 15th IEEE international conference on intelligent engineering systems (INES), pp. 57–61.

48. Broll, G., et al. (2010). Touch to play—mobile gaming with dynamic, NFC-based physical user interfaces. In Proceedings of the 12th international conference on human computer interaction with mobile devices and services, Lisboa.

49. Broll, G., et al. (2011). Touch to play—exploring touch-based mobile interaction with public displays. In Proceedings of 3rd international workshop on near field communication, Hagenberg, Austria, pp. 15–20.

50. Hardy, R., et al. (2010). MyState: Using NFC to share social and contextual information in a quick and personalized way. In Proceedings of the 12th ACM international conference adjunct papers on ubiquitous computing, Copenhagen, Denmark, pp. 447–448.

51. Siira, E., & Törmänen, V. (2010). The impact of NFC on multimodal social media application. In Proceedings of the 2nd international workshop on near field communication, Monaco, pp. 51–56.

52. http://en.wikipedia.org/wiki/Near_field_communication

53. The Mobile Payments and NFC Landscape.: A U.S. Perspective A Smart Card Alliance Payments Council White Paper Publication Date: September 2011

54. Hasoo Eun, Hoonjung Lee, Heekuck Oh, "Conditional Privacy Preserving Security Protocol for NFC Applications", In: Consumer Electronics (ICCE), IEEE International Conference Volume 59, 4 April, 2013.

55. Emir Husni, Kuspriyanto, Noor Basjaruddin, Tito Purboyo, Sugeng Purwantoro, Huda Ubaya, "Efficient Tag-to-Tag Near Field Communication (NFC) Protocol for Secure Mobile Payment", In: Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME), 2011 2nd International Conference, 8-9 Nov, 2011.

56. Ugo Biader Ceipidor, Carlo Maria Medaglia, Antonella Marino, Serena Sposato, Alice Moroni, "KerNeeS A protocol for mutual authentication between NFC phones and POS terminals for secure payment transactions", In: Information Security and Cryptology (ISCISC), 2012 9th International ISC Conference, 13-14 Sept, 2012.

57. Ali T , Awal M.A, “Secure Mobile Communication in m-payment system using NFC Technology”, In: Informatics, Electronics & Vision (ICIEV), 2012 International Conference, 18-19 May 2012.
58. Constantinos Markantonakis, Konstantinos Rantos, “On the life cycle of the certification authority key pair in emv 96”, In: Proceedings of Euromedia99, 1999.
59. A Smart Card Alliance Payments Council White Paper Publication/Update Date: January 2013 Publication Number: PC-12001
60. Fikrul Arif Nadra, Heri Kurniawan, and Muhammad Hilman, “Proposed architecture and the development of nfcafe: an nfc-based android mobile application for trading transaction system in cafeteria
61. http://www.google.com.pk/wallet/faq.html#tab=faq-security. Accessed on 27th June 2014.
62. Nelenkov, http://nelenkov.blogspot.com/2012/08/exploring-google-wallet-using-secure.html?q=google+wallet. Accessed on 27th June 2014.
63. Omkar Ghag, Saket Hegde, “A Comprehensive Study of Google Wallet as an NFC Application”, In: International Journal of Computer Applications, Volume 58, November 2012.
64. Mainetti L , Patrono L , Vergallo R, “IDA-Pay: an innovative micro-payment system based on NFC technology for Android mobile devices”, In: Software, Telecommunications and Computer Networks (SoftCOM), 2012 20th International Conference, 11-13 Sept, 2012.
65. Urien P, Piramuthu S, “LLCPS and SISO: A TLS-Based Framework with RFID for NFC P2P Retail Transaction Processing”, In: RFID (RFID), 2013 IEEE International Conference, April 30 2013-May 2 2013.
66. NFC Forum, http://members.nfc-forum.org/specs/spec_list/. Accessed on 27th June 2014.
67. Byungrae Cha , Jongwon Kim, “Design of NFC based Micro payment to support MD authentication and privacy for trade safety in NFC application”, In: Complex, Intelligent, and Software Intensive Systems (CISIS), 2013 Seventh International Conference, 3-5 July 2013.

68. Pasquet Marc , Reynaud J, Rosenberger C, “Secure payment with NFC mobile phone in the smart touch project”, In: Collaborative Technologies and Systems, 2008. CTS 2008. International Symposium, 19-23 May, 2008.

69. http://www.drburney.net/INDUCTIVE%20&%20DEDUCTIVE%20RESEARCH%20APPROACH%2006032008.pdf