Secure Electronic Transaction via NFC
NFC-SET

Hela Kaffel Ben Ayed
CRISTAL Lab., ENSI, University of Manouba
Tunis, Tunisia

Hajer Boujezza
CRISTAL LAB, ENSI, University Manouba,
Tunis, Tunisia

Arwa Ben Farhat
FST, University of Tunis AL- Manar
Tunis,Tunisia

Leila Saidane
CRISTAL LAB, ENSI, University Manouba,
Tunis, Tunisia

***Abstract*—Near Field Communication (NFC) is a wireless short range technology that aims to make applications faster with higher accuracy; improving productivity and eliminating costly errors that jeopardize the workplace, the safety of citizens and the business process. NFC security and privacy issues have to be addressed. In this paper, we focus on NFC mobile payment transactions and propose a new security solution, named Secure Electronic Transaction (NFC-SET). This solution aim to permits a legitimate cardholder and the rest of business ecosystem to achieve the NFC Electronic Transaction without leaking their private contents the merchant NFC equipment. For the m-payment transaction phase, we take advantages of shared secret NFC-SEC (Security) service and the SET to provide end-to-end security between the card holder and the payment gateway. We use the pattern checker Automated Validation of Internet Security Protocols and Applications (AVISPA) for the verification of our proposal.**

Keywords—NFC, Security, electronic transactions, Mobile-payment.

I. INTRODUCTION

NFC technology is the acronym of Near Field Communication [1] [2] [3]. NFC is a wireless communications technology. It emerged from the combination of contactless identification (Radio Frequency Identification - RFID) and Smartphones. NFC can be used with a large diversity of devices like mobile phones, notebooks, desktops, locks, printers, TVs, and consumer electronics. It provides users several kinds of services like payment, loyalty, transport, travel, culture, and infotainment. Around the world, many ongoing projects using this technology aim to emulate common tickets or coupons. Hence, Smart phones can be used as transport tickets, loyalty cards or even virtual vouchers etc. NFC technology provides three modes of operations: read/write mode, peer-to-peer mode, and card emulation mode. An NFC device can act as an NFC tag emulator or a tag reader [4]. NFC operates with a 13.56 MHz radio wave and at up to 424 Kbits/second data transfer speed. NFC is, at the same time, a “read” and “write” technology. The connection occurs among equipment when they touch. The maximum distance allowed for NFC well work is 10 centimeters. NFC application should be deployed on a secure element to make payment and ticketing operations more secure [5].

SET (Secure Electronic Standard) is an open encryption and security protocol that is designed for protecting credit card transactions on the Internet. Checking this protocol with Automated Validation of Internet Security Protocols and Applications, the protocol is declared as unsafe. Hence, we purpose to design and validate a new protocol named NFC-SET Protocol to enhance security for mobile contactless transaction [15].

In this paper we propose an approach named NFC-SET to provide end-to-end security for m-payment transactions using NFC.

The rest of the paper is organized as follows. Section II presents basic concepts. Section III presents NFC-SEC and SET protocols. NFC Mobile Payment is described on Section IV. Section V depicts the architecture of NFC-SET. Section VI portrays the formal validation of the proposed security solution and Section VII concludes this paper and outlines ongoing work.

II. BASIC NFC CONCEPTS

This section presents the concepts of NFC-SEC and SET.

A. NDEF

The data on a tag is structured in accordance with the NFC Data Exchange Format [6]. Therefore, NDEF is a standardized format for saving formatted and for exchanging data via a peer-to-peer link between two NFC devices [7]. The use cases for NDEF include the transporting of business cards, smart posters, and exploiting NFC as an enabler for other technologies [8]. An NDEF binary message encapsulates one or more payload fields of random type and size into one message. An NDEF message can contain one or various NDEF Records (an array of NDEF records). An NDEF record contains typed input information, like MIME-type media, a text, a URI, a Smart Poster, or a custom application payload. The first record has MB set and the last record has ME set. The NFC Data Exchange Format enables the “it’s all in a touch” principle: Over moving an NFC-enabled object near an NFC device, NDEF messages are exchanged, connection is established and an action is launched.

B. SRTD

The Signature Record Type Definition [4] [9] adds digital signatures to NDEF. It offers a reliable method for giving information about the source of NDEF data and allows users to check the authenticity and integrity of records within

an NDEF message [10]. A signature record's payload comprises: (1) version information, (2) a digital signature, and (3) a certificate chain [4]. The Signature field includes either a signature or an URI to a signature onto the signed information. The certificate chain is a list of certificates pursued by an optional URI reference which points to a rest of the list. It begins with the certificate for the signing key and ends with a certificate that is published by one of the trusted root certificate authorities. Besides, every element in the certificate register approves the preceding and every signature record signs all previous NDEF.

C. Vulnerabilities

Vulnerabilities are defined as weakness or events causing perturbation to normal operations or entail transfer of financial resources to an unauthorized party, resulting in financial exposure to legitimate stakeholders in the mobile payments system. Multiple Vulnerabilities are detected in [11] to [14]. They include:

- Eavesdropping: The RF signal for the wireless data transfer can be "sniffed" with antennas. An attacker can typically eavesdrop within 10m and 1m for active devices and passive devices respectively.
- Vulnerabilities of NDEF applications [11] [12]: Manipulation/replacement of NFC tags and their content like a smart poster's URL (e.g. redirect to phishing site) or a phone number (e.g. redirect to premium rate service). Therefore, the common user cannot distinguish forged from genuine tags!
    - Defects in current NDEF developments: E.g. we can hide a smart poster's URI on the Nokia 6131 NFC.
- Vulnerabilities of SRTD applications [13]:
    - Joining Records: By changing the Length fields of the first record and removing the header byte and Length fields of subsequent records, multiple consecutive records can be joined into one record.
    - Moving Data between Type, ID and Payload Fields
    - Record Hiding: defining the TNF field as unknown.
    - Extraction Records and record composition.
- Vulnerability of mobile phone [14]:
    - Multiple vulnerabilities of overflow were founded: Tested phone crashes and resets: e.g. when the payload value's 0xFFFFFFFF or OxFFFFFFFE.
    - The combination of NFC and Bluetooth, enables to upload and install an application into the manufacturer domain where the applications have no access limitations and do not need any confirmation from the user to access advanced resources such as the securely stored information like the private address book [12].

III. NFC-SEC AND SET PROTOCOLS

A. NFC-SEC

NFC Security (NFC-SEC) standard [8] defines mutual NFC Security services and a protocol. This specification determines the NFC-SEC secure channel and shares secret services for NFCIP-1 and the Protocol Data Units (PDUs) and protocol for those services. This provision points out SSE (secret services for NFCIP-1) and SCH (the NFC-SEC secure channel). The SSE creates a shared secret between two NFC-SEC interlocutors. The appeal of SSE needs to establish a shared secret due to the key confirmation mechanisms and key agreement, depending on the NFC-SEC cryptography part that specifies the Protocol Identifier (PID).Whereas the SCH supplies a secure channel. Establishment of the SCH shall induct a link key, by derivation from a shared secret established by the key agreement and key confirmation mechanisms, and therefore must protect all packets of mutual conversation across the channel, in accordance with the NFC-SEC cryptography section.

B. SET

SET (Secure Electronic Transaction) [9] [10] is an open encryption and security standard proposed to ensure credit card transactions on the Internet. SET is in fact, a sequence of protocols for ensuring security.

An important feature of SET is that the merchant /seller never sees the credit card number; this is only provided to the issuing bank. Classic encryption using Data Encryption Standard is used to bear confidentiality. To grant the Integrity of Data: Payment information received by merchants from cardholders incorporates order information, personal information and payment payloads. But, ***"the cardholder cannot claim later that her credit card was misused by someone else"*** [13]. This is in fact what we look forward to a credit card payment protocol. Yet, there is an unsafe scenario in this model. The user would be convened responsible for any transaction (deal) made by the software SET on his computer. Hence, all transactions will have the user's certificate. If a malware exploits some vulnerability in the user's computer and corrupts the SET software, it could sign an erroneous transaction and consequently leads to financial losses to the customer.

In the next section we describe the basics of contactless mobile payment.

IV. HOW TO WORK NFC MOBILE PAYMENT ?

In spite of possible variations, the NFC payment process remains relatively generic:

• The customer has a "NFC equipped" mobile containing a payment application (credit card and / or electronic purse). The merchant has a NFC payment terminal.

• When setting a purchase, the customer places his mobile close the terminal, establishes a communication radio frequency with the mobile and reads the information supplied by the application (account credentials, ceilings, etc.);

• The transaction may be a confirmation and a client authentication on its mobile,

• The merchant's payment terminal communicates if necessary with a banking network (permissible transactions which may be given directly by the application Payment for smaller amounts).

Smartphones are expected to eliminate consumer's need for numerous cards, badges and tickets, and become complete electronic wallets. Hence NFC enabled mobile phones may result in great savings for issuers of all types of plastic cards and ID token, as they can be replaced by virtual cards integrated in software applications. M-payment via NFC is increasingly deployed and spread**,** given the multiple benefits it offers like speed and simplicity. Two ways are implemented on the mobile allowing contactless payment [5] [11] [12]:

- Two chips are integrated into the phone where the SIM card is devoted to the basic mobile use (to send and receive calls, SMS, MMS ...) and the chip (Secure Element) that includes an appropriate NFC requesting payment. These two chips are completely separated.
- One chip on which is added a payment application on an environment-SIM card, the NFC chip is dedicated to the exchange of RF. This implies a new type of multi-card applications by merging the two contexts (a SIM card and a credit card) into a single entity.

Communication between the smartphone and the Point of Sale (NFC reader) is based on ISO/IEC 7816 and ISO/IEC 14443 standards. ISO/IEC 14443 allows the reader and the NFC chip to set up the device parameters for NFC transaction. NFC-SEC is not used since its is designed to provide security services to Peer-to-Peer NFC communications and does not consider reader/writer and card emulation modes. Hence, several weaknesses and attacks may target NFC systems in these latter modes..

V. ARCHITECTURE NFC-SET AND STEPS

In this section we present our NFC-SET protocol providing security services. Thus, a good balance between security and performance should be established.

A. Architecture

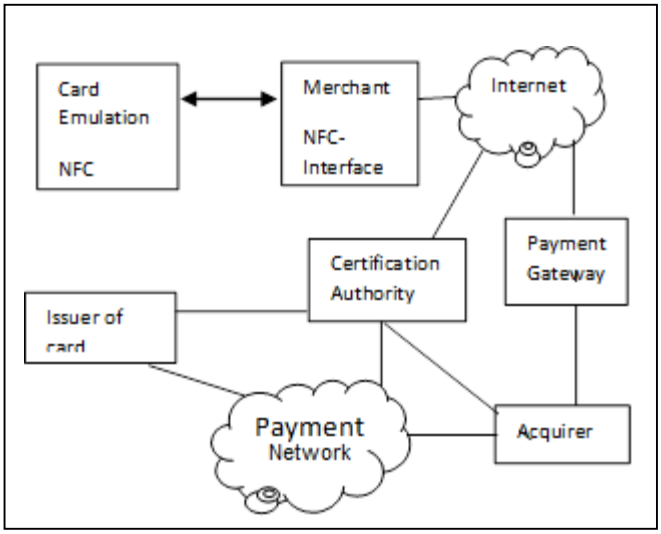


Fig. 1. NFC-SET Ecosystem

In our approach, we proposed a SET inspired Protocol to be compatible with NFC wireless technology. To ensure a secure payment transaction, several factors are taken into account i.e. response time and memory of the mobile, Secure Element and NFC radio interface. The Ecosystem of NFC Mobile Payment is respected. This Ecosystem contains the same actors/entities which were integrated in SET protocol. The difference is that the card-Emulation-Holder and the merchant communicate via NFC technology.

As illustrated in Fig.1, six actors (participants) are involved in our secure electronic transaction. These actors are: Card-Emulation-Holder, Merchant equipped with NFC-reader, Issuer, Acquirer, Payment Gateway and Certification

Authority: The Card-Emulation-Holder is a licensed holder of a payment card which has been transmitted by an issuer and emulated in her or his own Smartphone. Merchant is an entity who has items to sell to the Card-Emulation-Holder and accepts credit cards or card emulation. Issuer is a financial

Establishment: such as a bank that lends the Card-Emulation-Holder with the payment card. Acquirer is a financial institution that creates an account with the merchant and processes credit card consents and payments. It provides authorizations to the merchants considering the cards accounts parameters. Payment gateway is viewed as a role that can be played by the *acquirer* or some third party that processes the merchant messages. The payment gateway interfaces between NFC-SET and the banking clearing networks for permission and payment settlement. Finally the Certification Authority (CA) is an entity who's empowered to distribute X.509v3 public-key certificates for Card-Emulation-Holder, merchants, and payment gateways.

B. The Steps

In the following we present the various stages designed for the deployment of this NFC-SET communication. The designed steps are:

1) Generation of virtual chip in the Smartphone:

For each physical credit card, we associate a virtual card on the mobile phone: vCard. It is constituted by the encrypted key information and assumes the fact that phone has the burden which allows it to make secure transactions. When configuring emulation, the user receives the software plug-in of its digital wallet on mobile's memory and code (from his bank) via SMS. the received code will replace the card number and the secret code avoiding the the credit card number and password exchange in a single message even encrypted.

2) Encryption and Storage of this virtual chip in a secure element (SIM / SD card):

The received code will be encrypted with the public key of the credit card provider (Visa, MasterCard, CarteBleu) in the SIM card for future electronic transactions. We propose that card emulation is possible only for one phone number.

3) Transaction:

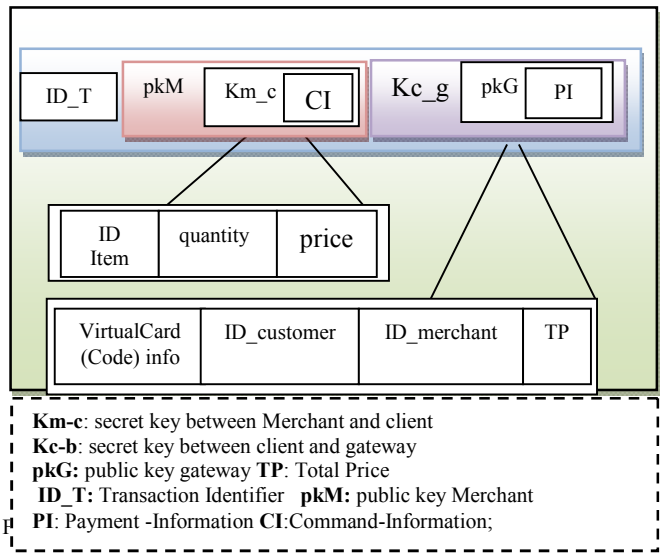
a) Phase1 : Initialization

This phase is similar to TLS handshake.

b) Phase2: Transaction

This phase uses the security parameters negotiated during phase 1, and sends message command information (CI) and payment information (PI). The purchase request is sent from the client to the merchant but the authorization and payment of seller settlement are sent to the payment gateway. During this phase, we keep the same treatment at the application level as in the SET protocol. All messages should be signed, hence, an the attacker can spoof an identity, he need to possess the certificate of one of the actors, which is obviously impossible to do, since certificates are issued by authorities that ensure the uniqueness of each certificate. Figure 3 illustrates different messages exchanged between the three actors during transaction step:

1) During this phase, the buyer sends a similar message to the message of requisition SET classic. The difference is that in NFC-SET, payment information (PI) is encrypted with the session key Kc-g (secret key shared between client and gateway), itself encrypted with the public key of the payment gateway (pkG): this is called digital envelope. The control information (CI) is encrypted with the session key Km-c (secret key shared between client and merchant), which will be transmitted in a digital envelope (public key of merchant: pkM) to the merchant.
2) When message (1) is received by Merchant, this latter sends a second message to the payment gateway. Message (2) contains payment request (pay-req) encrypted with secret key between the merchant and payment gateway (km-p), signature of merchant and "km-p " encrypted with public key of payment gateway.
3) Now, payment gateway sends payment response (pay-res) encrypted with shared secret key between itself and client (kg-c), its signature (sig-G) and "kg-c" encrypted with his public key.
4) Finally merchant returns response to Card-Emulation-Holder.



Once the transaction is completed, it is impossible to hack or produce replay attacks due to the identifier for the transaction.

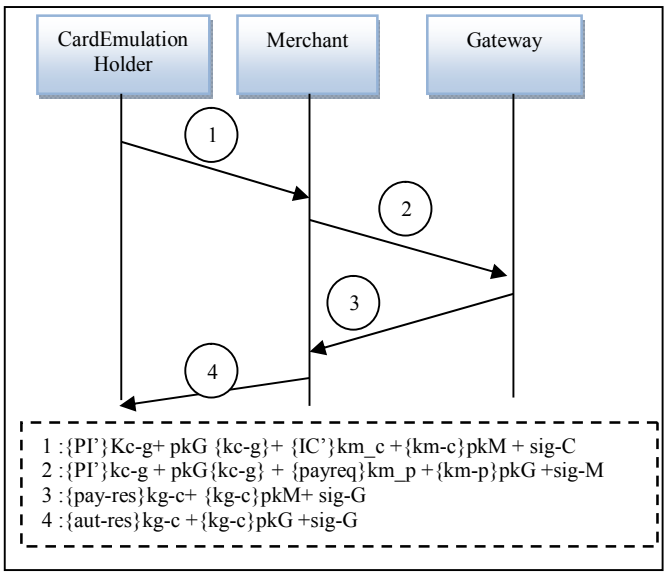


Fig. 3. Transaction

VI. FORMAL VALIDATION

Our goal here is to validate the targeted security services, i.e. confidentiality, authentication, no-replay, integrity and non-repudiation during NFC-SET transactions. To that end, we have chosen the model checker by AVISPA tool because it is powerful and open source.

A. AVISPA

AVISPA [14] stands for "Automated Validation of Internet Security Protocols and Applications". The AVISPA project gives a modular and semantic formal language for processing protocols and their security features, and includes different back-ends that deploy a variety of state-of-the-art automatic analysis techniques. These backend are:

- On-the-fly Model-Checker (OFMC):
- CL-AtSe (Constraint-Logic-based Attack Searcher)
- SAT-based Model-Checker (SATMC)
- TA4SP (Tree Automata based on Automatic Approximations for the Analysis of Security Protocols)

B. Validation

To prove the efficiency of our security design by AVISPA, we implement our 8 scenarios in High-Level Protocol Specification Language (HLPSL) code that can be processed by the tool. Thus every entity (Card_EmulationHolder, Merchant, and Payment_Gateway) is encoded into an HLPSL Agent code that describes the actions when sending or receiving messages. Then we build sessions by combining two or three entities together depending on the scenario we are validating. For example, in the scenario 1, a session « Session(C_em, M, P) » is composed of three agents. A hacker (intruder) can impersonate any agent just by intreducing the variable 'i' instead of the agent. So he can receive every message sent to

the hacked agent. The hacker knowledge describes several parameters such as the conversation and security. Those parameters are familiar to the hacker like channels, hash functions, participants' identities… etc. By mixing this knowledge with the data intercepted or received through the protocol checking, the intruder can build new messages and try to break the security specified in the section "Goals" of the HLPSL environment code (as far as he knows the required keys). After defining the sessions, we define the environment composed of sessions, intruder knowledge and the security goals. Once roles are defined, we proceed to the specifications.

- Knowledge of the intruder: here we assume the intruder knows all the security settings: hash function, the public keys of participants and their respective identities. This knowledge is given by "intruder-knowledge".
- Number of sessions: given by "composition".
- Referred Service: Privacy, given by "Secrecy of" in the GOAL section. We will check the secrecy of all the data that has been encrypted and transmitted: all session keys, payment information, those of the control, the number of the card dealer and finally the response of the bridge

Scenario 1) : One session is established with privacy check all encrypted messages. The result of the execution of this code indicates that the protocol is safe. The privacy service is guaranteed in mono session

Scenario 2) : The previous scenario was repeated but trying to see the impact of multi-session protocol security. As result we note that the number of visited nodes increases dramatically increasing the number of sessions. Unfortunately, AVISPA struggling to manage multi session and response time follows the exponential function of the number of sessions; it is merely a maximum of three sessions.

Scenario 3) :It is assumed that the attacker manages to open a session with the client. This is reflected in the composition part by establishing a new session or intruders "i" plays the role of merchant and uses its public key "Kpub-i" instead of the merchant's key

Scenario 4) :It is assumed that the attacker manages to open a session with the merchant. This is reflected in the composition part by establishing a new session or intruders "i" plays the role of client and uses its public key "Kpub-i" instead of the client's key. Here also, AVISPA validate our protocol as safe.

Scenario5): The client and merchant should certainly agree on the value of the exchanged key. In particular, client wishes to be sure that this value was indeed created by merchant…, that it was created for her/she for the aim of being used as a shared key, and that it was not replayed from a previous session. Even requiring authentication services on messages and no-replay, the output indicates that our protocol is safe.

Scenario 6): We repeat the same fifth scenario but with legitimate multi session.

Scenario 7) : We repeat the sixth scenario and adding an intruder session as a legitimate client.

Scenario8): We repeat the fifth scenario and adding an intruder session as a legitimate merchant.

All results are summarized in the three followings tables. Table I, Table II and Table III depict the validation results of our 8 scenarios with ATSE, OFCM and SATMC (respectively) backend. They show that the previously defined security goals are respected and validated in each scenario.

TABLE I. F ORMAL AVISPA VALIDATION TOOL OF NFC-SET PROTOCOL USING OFCM BACKEND

		Attack Found	Upper Bound Reached	Encoding Time	if2sate Compilation Time
Auth + Not replay	mono-session	false	True	0.01	1.43
	multi-session	false	True	0.02	1.39
	hack-client	false	True	0.02	1.5
	Hack-marchent	false	True	0.02	1.42
Conf	mono-session	false	True	0.01	1.43
	multi-session	false	True	0.02	1.42
	hack-client	false	True	0.01	0.37
	hack-marchent	false	True	0.02	1.54

TABLE II. FORMAL AVISPA VALIDATION TOOL OF NFC-SET PROTOCOL USING ATSEBACKEND

		Time (s)	Visited node	Plies
Auth + Not replay	mono-session	0,08	6	5
	multi-session	9,74	1254	10
	hack-client + multi-session	0,26	24	8
	hack-marchent	3,74	861	5
Conf	mono-session	0,1	6	5
	multi-session	15,05	1254	10
	hack-client	1,19	119	8
	hack-marchent	0,05	4	3

TABLE III. FORMAL AVISPA VALIDATION TOOL OF NFC-SET PROTOCOL USING SATMC BACKEND

		Analysed states	Reachable	Translation (s)	Computa-tion (s)
Auth + not replay		3	2	0.02	0.0
		216	208	0.06	5.08
	mono-session	3	2	0.04	0.0
	hack-marchent	5	3	0.02	0.01
Conf	mono-session	5	3	0.02	0.02
	multi-session	216	208	0.06	5.24
	hack-client (mono-session)	216	208	0.05	0.58
	hack-marchent	0	0	0.01	0.0

VII. CONCLUSION

In this work, we proposed a security solution for secure NFC transactions. We have explored the capabilities of the novel NFC technology for enabling secure mobile applications and validated the achievement of the security goals using the AVISPA tool. Verification of our solution shows the efficiency of our approach in terms of confidentiality, authentication, non-replay, non-repudiation and transaction integrity.

TABLE IV. TAXONOMY OF NFC SECURITY AND COUNTERMEASURE

	attack	Countermeasure deployed in NFC-SET
Application Layer	skimming	Cryptography
	replay	DES
	tracking	Shared secret
	Resynchronisation	Hash-based Authentication
Communication Layer	Man in the middle	Certificates X509.3
	Collision	Dual signature
Physical Layer	eavesdropping	Digital key envelop
	jamming	
	cloning	

REFERENCES

[1] Ali Alshehri and Johann A. Briffa, "Formal Security Analysis of NFC", M- coupon Protocols using Casper/FDR .23 Septembre 2013, 6pages.
[2] Collin Mulliner and Fraunhofer SIT (Darmstadt, Germany), "Vulnerability Analysis and Attacks on NFC enabled Mobile Phones", 1st International Workshop on Sensor Security March 2009 Fukuoka, Japan.
[3] (Near Field Communication in the real world – part II Using the right NFC tag type for the right NFC application), [paper of NFC FORUM].
[4] Michael Roland. Security Vulnerabilities of the NDEF Signature Record Type. Ieee 2011 Third International Workshop on Near Field Communication.
[5] Princeton Junction, Security of Proximity Mobile Payments, A Smart Card Alliance Contactless and Mobile Payments Council White Paper, Publication Date: May 2009 Publication Number: CPMC-09001.
[6] G. Madlmayr, J. Langer, C. Kantner, and J. Scharinger, "NFC Devices: Security and Privacy," in Proceedings of the Third International Conference on Availability, Reliability and Security (ARES '08), Barcelona,Spain, Mar. 2008, pp. 642–647.
[7] Michael Roland, FH OÖ Forschungs Entwicklungs GmbH, Security & Privacy Issues of the Signature RTD *NFC Research Lab Hagenberg* 2012-01-30
[8] Ecma International, NFCIP-1 Security Services and Protocol Cryptography Standard using ECDH and AES, 2008, Ecma/TC47/2008/089.
[9] MasterCard Inc., (1997), "SET Secure Electronic Transaction Specification, Book 1: Business Description, MasterCard Inc., http://www.win.tue.nl/~ecss/2IF30/set_bk1.pdf.
[10] A. Fourati, H.K.B. Ayed, F. Kamoun, A. Benzekri, (2002), A SET Based Approach to Secure the Payment in Mobile Commerce, In Proceedings of 27th Annual IEEE Conference on Local Computer Networks, pp. 136 – 140.
[11] *Alex Cheng and Andrew Pouleson,* "MOBILE PAYMENT SECURITY ANALYSIS AND SOLUTIONS". University of Pittsburgh Swanson School of Engineering, April 13, 2013
[12] David M. Monteiro1. A Secure NFC Application for Credit Transfer Among Mobile Phones. 2012; 5 pages
[13] http://www.indicthreads.com/1496/security-and-threat-models-secure electronic-transaction-set-protocol/
[14] http://www.avispa-project.org
[15] France BelangerJournal, Janine S. Hiller, Wanda J. Smith, "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes", Journal of Strategic Information Systems 11 (2002) 245–270.