IDA-Pay: an innovative micro-payment system based on NFC technology for Android mobile devices

Luca Mainetti
Associate professor

Luigi Patrono
Assistant professor

Roberto Vergallo
Ph.D. student

Department of Engineering for Innovation
University of Salento
Lecce, Italy
E-mail: {luca.mainetti, luigi.patrono, roberto.vergallo}@unisalento.it

Abstract: **The evolution of modern mobile devices towards novel Radio Frequency (RF) capabilities, such as Near Field Communication (NFC), leads to a potential for delivering innovative mobile services which is still partially unexplored. Mobile NFC micro-payments systems can enhance the daily shopping experience, but the access to payment security resources of a mobile device (e.g. the "Secure Element") by third party applications is still blocked by smartphone and OS manufacturers. In this paper, the IDA-Pay system is presented, an innovative and secure NFC micro-payment system based on peer-to-peer NFC operating mode for Android mobile phones. It allows to guarantee mobile-to-POS micro-payment services, bypassing the need for special hardware. A validation scenario is also depicted in order to demonstrate the system effectiveness.**

1. INTRODUCTION

Recently, mobile devices are playing a very important linking role between humans and virtual worlds. Currently, a mobile phone can be used to update Facebook status, check-in to physical places, share digital music, and more yet to come. According to such trend, the adoption of Near Field Communication (NFC) technology in today's smartphones follows exactly the Internet of Things (IoT) paradigma. Cisco has designed an infographic [1] that offers a simple example of how IoT will affect our everyday life. It states that by 2020, there will be 50 billion 'things' connected to the Internet - everything from our body, car, alarm clock and even cows.

The special interest of Google's Android towards NFC is favoring the spread of smartphones with embedded NFC readers; such devices are becoming popular and they are going to play a fundamental role in people's life, as they allow to supply a wide range of ubiquitous applications such as: access control, consumer electronics, healthcare, information collection and exchange, loyalty and coupons, payments and transport.

Mobile phones create a lot of secure and convenient conditions for payment operations, e.g., battery, keyboard, screen, storage, and 3G network. In future, these smartphones will represent the personal electronic wallet (e-wallet) for most people replacing the current plastic credit cards.

However, as reported in [2], NFC payments are yet to attain to their market potential. This is mainly because only Google's Android [3] has reached a significant share of the NFC mobile market. Moreover, only the Google Wallet mobile application supports NFC micro-payments in the US for Android mobile phones. Third party applications cannot take advantage of the security resources embedded in Android devices because Google Wallet is the unique application having privileged access to such resource, namely the "Secure Element" (SE). The SE is a special memory area where trusted applications can store and retrieve sensitive user information, such as the credit card number and the CVV code. Furthermore, Google Wallet is limited to work with affiliated credit card issuers (e.g. MasterCard, Visa), so no chance is given to alternative payment ecosystems.

The research work summarized in this paper aims to develop an innovative mobile micro-payment system which can be easily used in alternative ecosystems to implement custom payment scenarios. Such system must ensure the same security level of traditional credit card payments, without the need of any hardware intervention (SIM or SD cards replacement) by smartphone's owners. That is, the user has only to download the application from the market and install it onto the smartphone. Multiple payment networks (e.g. credit cards, money transfer, couponing) must be easily configurable. Finally, the interaction between the user and the system must be bi-directional, so the system can return rich collectible feedbacks to the user.

To achieve the abovementioned goals, a security architecture based on both symmetric and asymmetric encryption has been designed. In our system, the end-user can securely access innovative and unlimited mobile services by waving his/her smartphone proximate to an ad-hoc NFC Point-Of-Sale (POS). We called our system IDA-Pay, as it has been designed and developed in the IDA-Lab (IDentification Automation Laboratory) of University of Salento (Italy). The system has been validated in our laboratory considering the raised requirements; an effective validation with real actors has not yet been performed as it represents a future work.

The paper is organized as follows. In section 2, an overview over NFC technology and standards is given. Section 3 reports the state of the art related to security issues in NFC mobile payments. Presentation and discussion about the IDA-Pay secure architecture are outlined in section 4. Section 5 discusses about implementation issues and strategies, as well as presenting a validation scenario. Finally, section 6 summarizes our key messages and sketches future research directions.

2. OVERVIEW ON NFC TECHNOLOGY

NFC is a short-range wireless technology derived from the Radio Frequency IDentification (RFID) family which, even if is widely diffused and adopted in applications even quite far from the canonical ones related to logistic [4 - 11], it is not adequate for micro-payments. NFC has been standardized and promoted by Sony, Philips and Nokia which founded the NFC Forum [12] in 2004. To date, the NFC Forum boasts more than 160 members.

NFC is based on inductive-coupling, where loosely coupled inductive circuits share power and data over a distance of a few centimeters (<5 cm). NFC devices inherit the basic technology of proximity such as RFID tags in High Frequency (HF) band (i.e., 13.56 MHz) and contactless smartcards, but have a number of key new features.

The specification for NFC is given by ISO/IEC 18092 NFC IP-1 [10] and ISO/IEC 14443 [14] contactless smartcard standards. According to such standards, NFC offer three different operating modes, illustrated in Fig.1:

1. Reader/Writer mode. The NFC device is capable of reading NFC Forum-mandated tag types. The reader/writer mode on the RF interface is compliant to the ISO 14443 and FeliCa schemes.
2. Card Emulation mode. The device can emulate an existing contactless card without adaptors in the existing payment infrastructure. A card and a tag are technically the same; however, contactless cards used in e-ticketing and payment today include additional technology to store secure data.
3. Peer-to-peer (P2P) mode. Two active NFC devices can exchange data, such as virtual business cards or digital photos. P2P mode is standardized on the ISO/IEC 18092 standard.

NFC always involves an initiator and a target; the initiator actively generates an RF field that can power a passive target (e.g. tags, stickers, cards) or an active target as well (i.e. a second NFC reader). Available bit rates for NFC are 106/216/414 Kbps.

Data stored into NFC passive targets follows the NFC Data Exhange Format (NDEF) Forum specification [15]. NDEF is a binary message format that can be used to encapsulate one or more application-defined payloads which may be of a variety of types and sizes. The format and the rules for

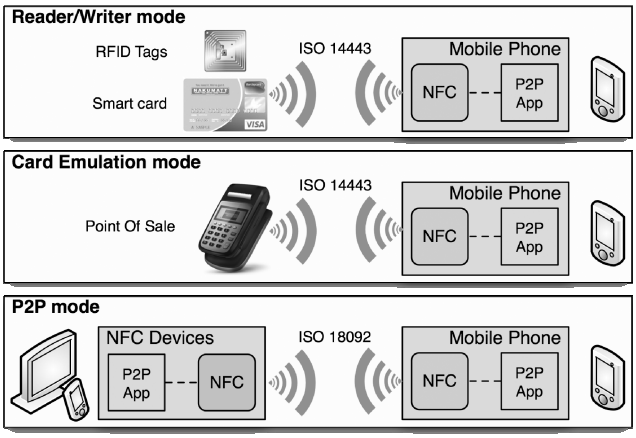

Figure 1 - NFC Operating modes and standards

building standard record types in NDEF messages are included in NFC Record Type Definition (RTD) Technical Specifications [16]. There are four specific RTDs: Text, URI, Smart Poster, and Generic Control.

The exchange of data between two active targets (P2P) takes place on top of the Logical Link Control Protocol (LLCP) [17]. LLCP is an OSI layer-2 compact protocol, based on the industry standard IEEE 802.2, designed to support either small applications or network protocols. Google released the Android NDEF Push Protocol (NPP) [18], a simple open protocol built on top of LLCP which is designed to push an NDEF message from a NPP client to a NPP server (one way). A device that supports NPP always run an NPP server, and may run a NPP client as well. This allows for bi-directional NDEF exchange between NPP devices.

3. RELATED WORKS

Working in card emulation mode implies to access the SE. It plays a key role in the security management, as it hosts the firewalled applications and user credentials, and controls security and cryptography using an onboard microprocessor and software.

There are three ways to implement the SE:

1. In the SIM. This has the advantage of portability, and is the preferred approach in GSM countries; the drawback is that the user must purchase a special purpose SIM.
2. Embedded SE component. This is a separate chipset in the handset. Its principal advantage is that it is convenient for handset manufacturers to implement quickly. The drawback is that handset and OS manufacturers rule the access to the SE.
3. A removable SE component. This is a theoretical approach to create a removable separate chipset in the handset; often it is implemented as a SD card. Again, the drawback is that the user must purchase special hardware.

The embedded SE solution is adopted in Android NFC mobile phones. Samsung's Nexus S, Galaxy Nexus, and Galaxy S III have this feature implemented in the PN65N NFC chipset which includes the SE. However the Android NFC APIs do not provide SE software interfaces, except for the Google Wallet application, that can work in card emulation mode and take advantages of the existing payment infrastructure.

In literature, some attempts to address such limits exist. In [19], the first experiment of a NFC-based payment application fully supporting the EMV (Europay, MasterCard and VISA) international standard [120] is described. In this solution the SE is embedded within a special SIM card. The same approach is used in [21], where Nokia NFC mobile phones use special SIM cards to guarantee privacy and security in car parking payment transactions in Italy. Other interesting SIM-based solutions are proposed in [22 -25].

In [26], the pros and cons of combining NFC with the SIM card in the handsets are described. Although the technology itself is already working properly, the authors admit that the processes and concepts for integration of both into one mobile device still needs time. At present, the user should replace his SIM card with a new one. Moreover, SE itself is not completely threat-safe, as its centralized logic may be object of Denial of Service and Relay attacks [27, 28].

4. SYSTEM ARCHITECTURE

In IDA-Pay, P2P operating mode is used to transfer payment information between the Android NFC smartphone and the POS. The forced choice to use P2P has the unavoidable drawback of not being compatible with the existing NFC POS infrastructure; nevertheless, EMV virtual POS services are offered almost by every bank. Moreover, the choice to use P2P mode instead of card emulation leads to several benefits, e.g. the user can receive customizable confirmations onto his/her smartphone, so he or she can keep tracks of the payments at any time (even when off-line).

In Fig. 2 the high level IDA-Pay system architecture is shown. In particular:

1. The client is an Android NFC smartphone with the IDA-Pay App installed on. In IDA-Pay client, there is no need for a SE, as the sensitive information for every configured credit card is stored in a secure file placed in the smathphone memory and called Credit Card File (CCF).
2. The IDA-Pay POS is a desktop client connected to the Internet. It has also an NFC interface and runs the IDA-Pay POS application, in order to exchange payments data with the buyer.
3. The IDA-Pay Gateway (GW) is a Web server which forwards the payment request incoming from the IDA-Pay POS to the right credit card network endpoint (e.g. an EMV compliant virtual POS).

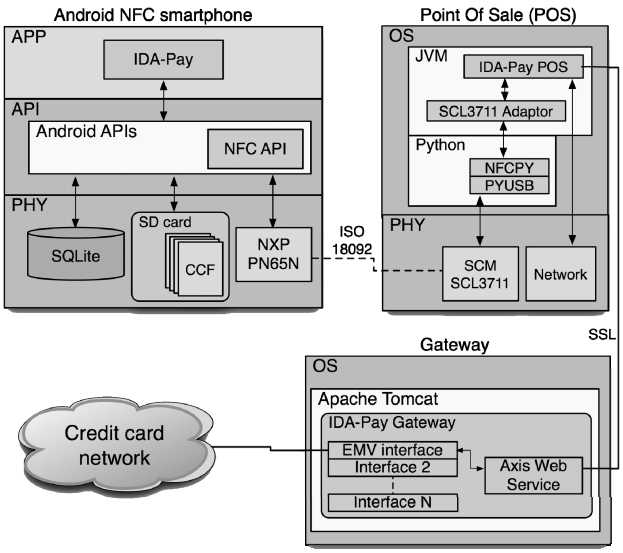

Figure 2. The IDA-Pay architecture

The security architecture designed for IDA-Pay follows in Dominikus's footsteps [26].

When a payment is requested, the user inserts a PIN and the CCF is passed to the IDA-Pay POS through a NFC P2P link. The CCF encrypts a plain text credit card file M containing the device ID, the credit card number, the month/year of expiration and the CVV. The device ID is the phone's fingerprint; it is used to hard-link the CCF with the smartphone, so the CCF, if stolen, cannot be used by any different device. It is calculated by combining various hardware information such as the smartphone's CPU serial number and the Bluetooth card MAC address.

In order to ensure confidentiality, only the IDA-Pay GW should be able to understand the CCF; so it is obtained by encripting the M file using a Public Key Infrastructure (PKI). When a new credit card is configured in the IDA-Pay App, the M file is encripted using the IDA-Pay public key (ePub) and the CCF is created. The used encryption algorithm is the RSA with a key length of 2048 bits.

$$M_{Pub} = e_{Pub}(M) \tag{1}$$

The encrypted message resides on the smartphone memory, so it may be object of spoofing attacks. The user authentication is necessary when the access to M_{Pub} is requested. For this reason it has been used an additional level of encryption based on the symmetric key algorithm AES, where the 128 bits key k_{PIN} is computed on the basis of a 5 digits seed (PIN) inserted by the user at the moment of card configuration. So:

$$CCF = k_{PIN}(e_{Pub}(M)) \tag{2}$$

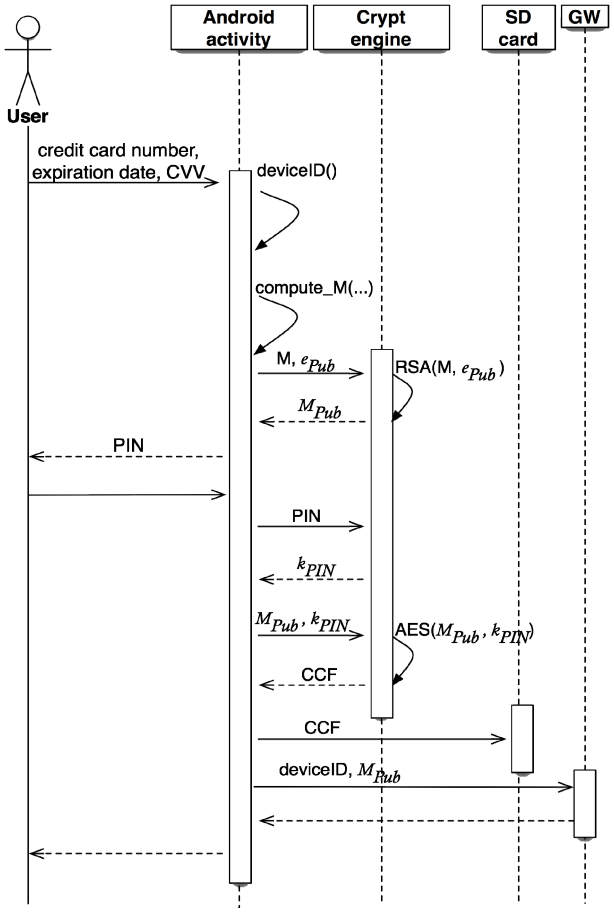

Figure 3. The card configuration interaction scenario

Such process is schematized in the card configuration interaction scenario shown in Fig. 3. In Fig. 4 the payment interaction scenario is reported. When a new payment is requested, the user selects a configured credit card on its Android smartphone and the IDA-Pay App prompts the user to re-type the PIN. The k_{PIN} symmetric key is re-computed, so it can be used to try to decrypt the CCF. If the PIN is right, M_{Pub} is obtained and it is ready to be transferred to the requesting POS through the NFC P2P link, along with the recomputed device ID. The IDA-Pay POS works as a relayer, as it forwards the CCF, the device ID and the payment amount to the IDA-Pay GW in the POST body of a SOAP message. The SOAP request is transferred by using a Secure Socket Layer (SSL) tunnel. After the device ID has been validated, the gateway can extract the M plain file using the IDA-Pay private key e_{Priv} and it forwards the payment request to the right credit network (e.g. a virtual EMV POS).

5. VALIDATION

The IDA-Pay App prototype has been implemented and validated by using a Samsung Nexus S mounting Android 4.1.1 (i.e., Jelly Bean version). We chose this smartphone model because the Nexus S was the first Android device to

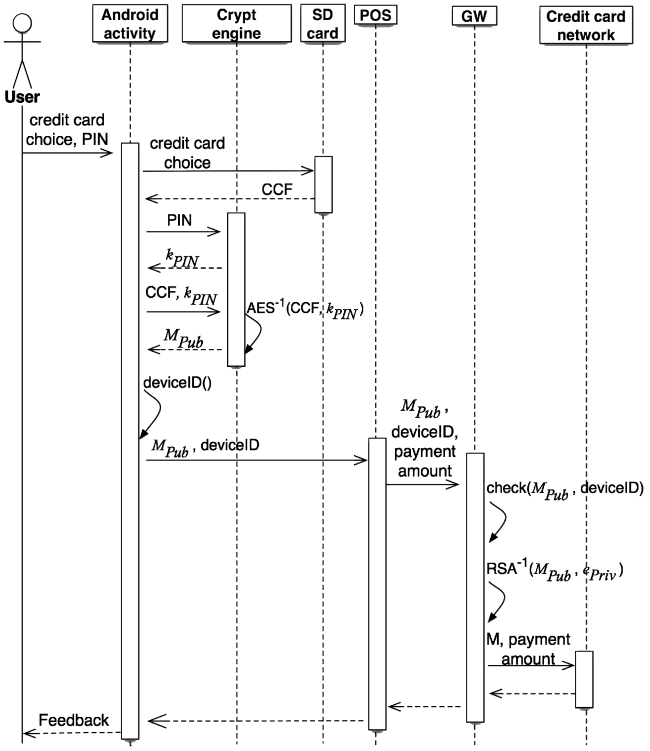

Figure 4. The payment interaction scenario

support NFC in both hardware and software. It represents the best trade-off between performances and cost; the double-level encryption process is almost instantaneous on the Nexus S' ARM Cortex A8 CPU. The package javax.crypto from Android SDK has been used in order to produce the CCF.

The IDA-Pay POS prototype uses a SCM Microsystems SCL3711 USB Dongle NFC reader, as it is the best supported reader by NFCPY libraries [27]. Such libraries have been used as they were the most evoluted NFC P2P desktop libraries at the time of implementation (Jan. 2012). NFCPY libraries are written in Python and implement the Google's NPP specifications.

However, NFCPY are still a work in progress and the latest release (1.0 at the time of implementation) was still buggy. In particular, we had to solve a problem occurring when switching NPP client and server roles between the smartphone and the SCL3711. Such switching was needed for receiving feedbacks from the POS, as at the first phase of the payment the communication flows from smartphone to SCL3711, while at the second phase it flows from SCL3711 to smartphone. The SCL3711 could not switch from server to client role because it remained pending, waiting for other NDEF messages incoming from the smartphone. Our fix let the connections be closed when data exchange between the two NFC devices is terminated

In the IDA-Pay POS implementation, NFCPY are wrapped in a Java standalone program, in order to follow the Android philosophy. However, the Python runtime environment must be installed on the POS machine.

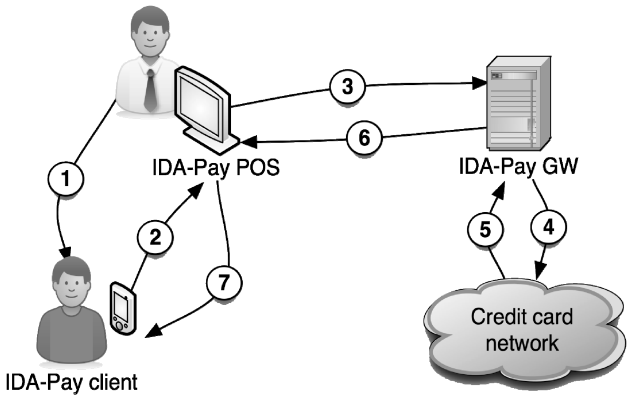

Figure 5. Validation scenario

The IDA-Pay GW exposes a set of web services through the Tomcat servlet container. In order to support multiple credit card networks, the Abstract Factory design pattern [28] has been used, thus it is simple to implement multiple concrete adaptors for different credit card networks, with no effort in re-engineering the code.

In Fig. 5 the validation scenario is reported. Here we assume that a credit card (at least) has been configured by the buyer into his smartphone. In particular:

1. The cashier inserts and confirms the amount into the IDA-Pay POS application (Fig. 6.a) and tells the buyer to touch his NFC Android smartphone to the POS NFC reader.
2. The buyer starts the IDA-Pay App and taps a credit card from the configured credit card list (Fig. 6.b). The App prompts the buyer to insert the correspondant PIN, then tell the buyer to touch the smartphone to the POS NFC reader (Fig. 6.c).
3. Payment details are transferred to the IDA-Pay GW.
4. The IDA-Pay GW instantiates a payment transaction with the right credit card network.
5. The GW receives the result from the credit card network.
6. The result is formatted and returned to the IDA-Pay POS, where it is shown to the cashier.
7. A plain text response is created and sent back to the buyer's smartphone through the NFC P2P link. A process dialog notifies the buyer that the payment has been sent successfully and that he can move the smartphone away from the POS NFC reader. The payment response is stored into the payments archive (Fig. 6.d).

During the entire transaction, the buyer's smartphone must remain in touch with the POS NFC reader in order to receive the response from the system. During the payment process, it is not necessary for the buyer to be connected to the Internet.

6. CONCLUSION

In this paper, an innovative NFC-based mobile micro-payment system architecture and prototype for Android smartphones has been proposed and discussed. In literature, several NFC-based micro-payment systems have already

Figure 6. The IDA-Pay prototype

been presented; in order to avoid the security limitations imposed by smartphone and OS manufacturers, such works force the user to install addictional hardware (special SIM or SD cards). Our system, called IDA-Pay, is SE-agnostic as it uses NFC P2P mode and can be easily used in alternative micro-payments ecosystems. Nevertheless, the same security level of traditional credit card payments is ensured, and the compatibility with popular credit card networks is preserved. Moreover, in IDA-Pay the data flow between the smartphone and the system is bi-directional, so the user can read and collect textual or binary feedbacks.

Nevertheless, only NFC-enabled smartphones can be used in IDA-Pay. Alternative solutions based on NFC stickers or QR codes could be considered in order to retro-fit the system.

Our effort has been spent to validate the system with a set of predefined test beds through the "living laboratory" approach. The next step is to validate our system in a pilot project with real users using the system in real scenarios; moreover, biometric techniques to identify the cardholder will be also taken into account in order to avoid the need of a PIN, which can be easily forgotten, lost or stolen.

ACKNOWLEDGMENTS

We want to thank the student Marco Schito for his valuable help in developing the system during his first level degree stage at the IDA-Lab.

REFERENCES

[1] Cisco, “The Internet of Things [INFOGRAPHIC],” http://blogs.cisco.com/news/the-internet-of-things-infographic/.

[2] Gartner, “Hype Cycle for Emerging Technologies 2011,” http://www.gartner.com/DisplayDocument?doc_cd=215650.

[3] Android, http://www.android.com/.

[4] L. Catarinucci, R. Colella, M. De Blasi, L. Patrono, L. Tarricone: “Enhanced UHF RFID Tags for Drug Tracing,” Journal of Medical Systems (JOMS), Springer, 2011.

[5] M. Maffia, L. Mainetti, L. Patrono, E. Urso: “Evaluation of potential effects of RFID-based item-level tracing systems on the integrity of biological pharmaceutical products,” International Journal of RF Technologies: Research and Applications, vol. 3, Issue 2, pp. 101-118, 2012.

[6] L. Catarinucci, R. Colella, M. De Blasi, L. Patrono, and L. Tarricone: “Experimental Performance Evaluation of Passive UHF RFID Tags in Electromagnetically Critical Supply Chains,” Journal of Communications Software and Systems, Vol. 7, No. 2, pp. 59-70, 2011.

[7] L. Catarinucci, S. Tedesco, L. Tarricone, “On the Use of UHF RFID Antenna Systems Customized for Robotic Applications,” in Proc. IEEE International Symposium on Antennas and Propagation, APSURSI, Chicago, IL, 2012.

[8] G. Calcagnini, F. Censi, M. Maffia, L. Mainetti, E. Mattei, L. Patrono, E. Urso: “Evaluation of Thermal and Non-thermal Effects of UHF RFID Exposure on Biological Drugs,” IEEE Transactions on Information Technology in Biomedicine, Volume: PP , Issue: 99, 2012.

[9] L. Catarinucci, R. Colella, M. De Blasi, L. Patrono, and L. Tarricone, “Improving Item-Level Tracing Systems Through ad Hoc UHF RFID Tags,” Proc. IEEE Radio and Wireless Symposium, RWW 2010, pp. 160-163, 2010.

[10] L. Catarinucci, S. Tedesco, D. De Donno, L. Tarricone: "Platform-Robust Passive UHF RFID Tags: a Case-Study in Robotics," Progress In Electromagnetics Research C, Vol. 30, 27-39, 2012.

[11] L. Catarinucci, R. Colella, L. Tarricone, “A Cost-Effective UHF RFID Tag for Transmission of Generic Sensor Data in Wireless Sensor Networks,” IEEE Transaction on Microwave Theory and Techniques, Vol. 57, Issue 5, pp. 1291-1296, 2009.

[12] NFC Forum, http://www.nfc-forum.org/home/.

[13] International Standard ISO/IEC 18092, Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1), 2010-04-20, ISO/IEC 2010.

[14] International Standard ISO/IEC 14443-1-2-3-4, Identification cards - Contactless integrated circuit cards - Proximity cards, 2008-07-15, ISO/IEC 2008, Switzerland.

[15] NFC Data Exchange Format (NDEF) Technical Specification (NDEF 1.0), 2006-07-24, NFC Forum, Inc., Wakefield (MA), USA.

[16] NFC Record Type Definition (RTD) Technical Specification (RTD 1.0), 2006-07-24, NFC Forum, Inc., Wakefield (MA), USA.

[17] NFC Logical Link Control Protocol (LLCP) Technical Specification (LLCP 1.1), 2011-06-20, NFC Forum, Inc., Wakefield (MA), USA.

[18] Android NDEF Push Protocol Specification, version 1, 2011-02-22.

[19] Pasquet M., Reynaud J., Rosenberger, C.: "Secure payment with NFC mobile phone in the SmartTouch project," International Symposium on Collaborative Technologies and Systems, 2008 (CTS 2008), pp.121-126, 19-23 May 2008.

[20] EMVCo., http://www.emvco.com/ .

[21] Benelli G., Pozzebon, A.: "An automated payment system for car parks based on Near Field Communication technology," Int. Conference for Internet Technology and Secured Transactions (ICITST), pp.1-6, 2010.

[22] Xiong Yu-ning: "Research on NFC and SIMpass Based Application," International Conference on Management and Service Science, 2009. MASS '09., pp.1-4, 20-22 Sept. 2009.

[23] Hao Zhao, Muftic S.: "The concept of Secure Mobile Wallet," World Congress on Internet Security (WorldCIS), 2011, pp.54-58, 21-23 Feb. 2011.

[24] Steffens E.-J., Nennker A, Zhiyun Ren, Ming Yin, Schneider L.: "The SIM-based mobile wallet," 13th International Conference on Intelligence in Next Generation Networks, 2009. ICIN 2009, pp.1-6, 26-29 Oct. 2009.

[25] Wei-Dar Chen, Mayes K.E., Yuan-Hung Lien, Jung-Hui Chiu: "NFC mobile payment with Citizen Digital Certificate," The 2nd International Conference on Next Generation Information Technology (ICNIT), pp.120-126, 2011.

[26] Madlmayr G, Dillinger O., Langer J., Schaffer C., Kantner C, Scharinger J.: "The benefit of using SIM application toolkit in the context of near field communication applications," International Conference on the Management of Mobile Business, 2007. ICMB 2007., pp.5, July 2007.

[27] Roland M., Langer J., Scharinger J.: "Practical Attack Scenarios on Secure Element-Enabled Mobile Devices," 4th International Workshop on Near Field Communication (NFC), 2012, pp.19-24, 13-13 March 2012.

[28] Jara Antonio J., Alcolea Alberto F., Zamora Miguel A., Skarmeta Antonio F. G.: "Evaluation of the security capabilities on NFC-powered devices," European Workshop on Smart Objects: Systems, Technologies and Applications (RFID Sys Tech), 2010, pp.1-9, 15-16 June 2010.

[29] Dominikus S., Aigner M.: "mCoupons: An Application for Near Field Communication (NFC)," 21st International Conference on Advanced Information Networking and Applications Workshops, AINAW '07, pp.421-428, 2007.

[30] Python module for near field communication, https://launchpad.net/nfcpy.

[31] Gamma, E. et al, 2007. Design Patterns: Elements of Reusable Object-Oriented Software. Addison-Wesley Professional, Redwood City, USA