International Journal of
Applied Mathematics,
Electronics and Computers
ISSN: 2147-8228 http://ijamec.atscience.org
Advanced Technology and Science
Original Research Paper

Service Oriented Mobile Wallets with NFC

M. Ali Erturk *[1], M. Ali Aydin [1], H. Ibrahim Ibali [1], Zeynep Gurkas Aydin [1], A. Halim Zaim [2]

Accepted 10th August 2015 **DOI: 10.18100/ijamec.39718**

Abstract: Near Field Communication (NFC) technology integration with mobile phones has extended the way we use mobile devices. Instead of voice and text communication mobile devices can be used as credit cards to replace our wallets. In this study we have developed an NFC based mobile wallet with using Alcatel Lucent Mobile Wallet web services with provided functionalities such as accounts, e-money, loyalty cards, etc. These services are consumed from NFC mobile phones and NFC device is used for payments and secure store to keep user credentials in SIM Secure Element.

Keywords: *NFC, Secure Element, SE, Mobile Wallet*

1. Introduction

World is getting more mobile day to day and technological improvements changes the way we use mobile devices. Instead of just communications, these devices can be capable of replacing our wallet with mobile phones.

Different e-wallet approaches proposed for different use cases with different schemes. [1] in the study author presents a client-server architecture for mobile payment system for public transportations. Security is handled by exchanging a key between client and server as encrypted and the systems security is based on the strength of the key. In the study it is aimed to have application specific model instead of general purpose usages. SIM Card only payment models and implementations are presented in the [2], [3] papers. The models use only Universal Integrated Circuit Card (UICC) to interact with mobile point of sale (POS) terminals for payment transactions. Since applications are limited to SIM card capabilities and the functionally such as payment history, card balance and money transfer from between parties either missing or can not be provided to the end user.

In this study, we developed a rich secure mobile wallet using RESTful [4] web services provided by Alcatel Mobile Wallet Services (MWS) [5]. Mobile application consumes web services to present end user wallet functionality. The application specifically developer for NFC based mobile phones to benefit all NFC functionalities available such as Secure Element and contactless payment.

This paper is organized as follows: Section 2 describes NFC technology. Section 3 presents developed solution and Section 4 concludes this paper and presents future work.

2. Near Field Communication

This section will briefly introduce NFC technology and its applications.

2.1. Near Field Communication (NFC)

NFC is a short-range wireless communication technology, which enables identification and data transfer within 4cm or less. NFC operates in 13.56 MHz with maximum 424kbps data rate.

A comparison of wireless technologies is shown in Figure 1. NFC communication standards are based on RFID ISO/IEC 14443 and FeliCa[6]. NFC devices can operate on three modes: card emulation, peer-to-peer and read/write mode. Card emulation can emulate an RFID tag which is useful for combining all RFID keys in a single mobile phone.

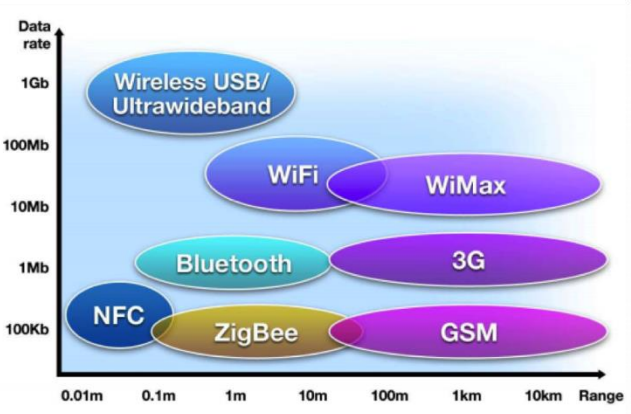

Figure 1. Wireless technologies.

Architecture's overview of NFC is shown in Figure 2. First bottom layer shows analog specifications of a NFC device e.g., RF fields and strengths. Digital protocol specifications are digital implementations of ISO/IEC 18092 and ISO/IEC 14443. NFC activity specifications describe required activities for communication [6].

In the architecture NFC Data Exchange Format (NDEF) defines message-coding formats for NFC applications. Also, Record Type Definition (RTD) describes how to construct records in NDEF messages [6].

Logical link protocol defines set of operations used in peer-to-peer mode of NFC device such as link activation, supervision, deactivation etc. Simple NDEF Exchange Protocol (SNEP) enables NDEF message exchange in peer-to-peer mode [6]. NFC can be used to communicate devices through directly reading device data or establishing a Bluetooth link to communicate. This This will enable NFC enabled medical devices to be communicating with our NFC mobile phones to exchange data[7].

[1] *Computer Engineering Department, Engineering Faculty, Istanbul University, Istanbul/Turkey*
[2] *Information Technologies Application and Research Center, Istanbul Commerce University Istanbul, Turkey*
* *Corresponding Author: Email: mehmetali.erturk@istanbul.edu.tr*
Note: This paper has been presented at the International Conference on Advanced Technology&Sciences (ICAT'15) held in Antalya (Turkey), August 04-07, 2015

In our design, NFC enabled mobile phones are used to communicate web services, secure elements and mobile terminals for contactless payment operations.

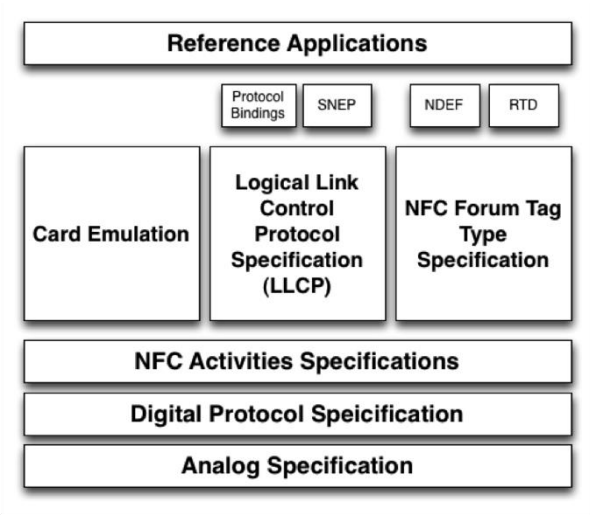

Figure 2. NFC architecture

2.2. NFC Applications

NFC technology provides benefits to its users and so far %40 of the research is the develop NFC-based applications [7]. In general NFC applications are evaluated in three common categories: smart environment, mobile wallets and data exchange application.

Smart environment applications usually work on read/write mode of the device and smart posters are the most common application types in this environment [8], [9], [10].

Mobile wallet applications are aimed to replace users credit card, tickets or reality cards with mobile phones. NFC based mobile phones store user credentials and capable of payment with contactless touches to NFC Pos terminals through card emulation mode [11], [12], [13].

Data exchange applications are mostly required peer-to- peer mode to operate and takes place whenever two NFC terminals touch each other to exchange information like business cards [13], [14].

NFC based mobile phones contain two main components; NFC modem and SE(Secure-Element). Secure Element is a component which is responsible for secure storage and execution environment in NFC devices [15]. There are two main approaches for SE implementations, one for embedded in mobile phones and other alternative is SIM based implementation. Mobile phone based embedded SE implementations contains SE chip inside mobile phones and called SE-NFC. SIM based implementations mobile phone doesn't contain SE native but embedded in GSM SIM (Subscriber Identity Module) cards.

Java Card technology is developed to develop Java based applets which run on smart cards. Java Card technology is a standard which is accepted most of the GSM SIM vendors and provides Java Card runtimes in SIM cards[17]. Java Cards are used to develop NFC-SE applications securely on both embedded and SIM based SE.

Java Card is a subset of Java programming languages and has the following features[17];

- Supports small data types, Boolean, byte, short
- Single dimension arrays
- Packages, classes, interfaces and exceptions
- Inheritance, virtual methods and dynamic objects.

Java Card virtual machine has;

- Card resource management
- Communication protocols (APDU)
- Applet execution
- Applet security

3. Developed System

Application environment consists of several components with different technology stacks. At the higher-level Alcatel-Lucent Mobile Wallet Services (MWS) provides necessary web services through http protocol. Our mobile clients consume RESTful services and add secure NFC functionality. These security is maintained SE, it is responsible for storing critical information securely on SIM.

RESTful services use SSL based secure connection and clients use OAuth to authenticate system [18].

In client side, Blackberry 9900 and Google Nexus S is selected as mobile NFC device. Blackberry has Blackberry OS 7.1 which is based on J2ME and set of tools developed by RIM. Nexus S runs on Android OS which is Java based platform runs on Dalvik JVM [19], [20].

For SE development purposes G&D SDK tool is used to develop, test and deploy SE applications with Java Card technology [21].

Developed system has two main parts: mobile user interface and SIM SE part.

3.1. SE (Secure Element) Application

In the project Giesecke & Devrient (G&D) SDK and G&D UICC SIM cards used for development. G&D SDK has built-in tools for writing, compiling and debugging Java Card applications with simulator. Also, SDK includes additional devices and tools for on device deployment and debugging.

SE application is the responsible part for secure communication through mobile phone. Also it is capable of executing necessary operations. End users can perform following operations on SE:

- Update user credentials
- Update application PIN
- Make payment (without PIN) • Make payment with PIN

Table 1. APDU Command Structure

CLA	INS	P1	P2	Len	Data
Command Class	Instruction	Param1	Param2	Data Length	Payload Data

Whenever user touches his phone to NFC Pos for payment operation, NFC Terminal selects appropriate applet and communicates with SE through set of APDU commands. As illustrated in Figure 3. payment processes executed in the following order and if everything is OK, payment will be processed.

SE communications are performed by APDU commands, and data format is shown Table I.

As an example following sequences show simple payment scenario (for security reason this is example data, not applicable for real environment).

Host → Select applet
apdu:0;target=A0.00.00.00.90.00.00.01.02.03.04.05
Host → Payment APDU
SE ← 00019000
Operation succeeded.

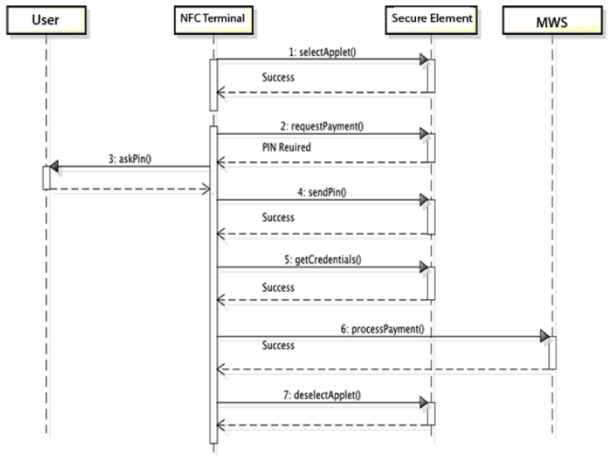

Figure 3. Payment sequence diagram.

3.2. Mobile Application

Developed mobile applications are able to communicate both SE and Alcatel-Lucent MWS services to provide end use mobile wallet functionalities. MWS services provide following operations;

- Money Card operations
  - o Query money balance
  - o Display transaction history
  - o Money transfer
  - o Money transfer via NFC touch
  - o Top-up money from credit card
- Loyalty Card Operations
  - o Query card balance
  - o Display card history
- Coupon Card Operations
  - o Query coupon balance
  - o Display coupon transactions
- Login
- Logout

All of these functionality is implemented by mobile clients so, users are able to perform money card, loyalty card or coupon card operations on their mobile phones. Whenever a user logs in to the system with mobile phone, user credentials are requested from server and securely stored in SE in the SIM.

Simple and minimal user interfaces design approach is selected for mobile clients. Blackberry application sample interfaces are shown in Figure 4, Figure 5 and Figure 6. In Figure 4 all accounts and balances are displayed.

If we summarize over all scenario;

- End user logins mobile application by using his/her username and password
- User information is retrieved from web services Important user credentials are stored in SE Whenever user wants to make a payment, he/she touches mobile phone to the NFC terminal
- NFC terminal request user credentials from SE
- If SE communication finishes successfully, NFC terminal request payment operation to MWS
- MWS authorizes NFC terminal makes payment operation
- End user can query transactions and payment history

These steps show example workflow of the application, which is tested in our labs. All RESTful operations were successful on both 3G and Wi-Fi networks.

Figure 4. All accounts and balanced are listed in application

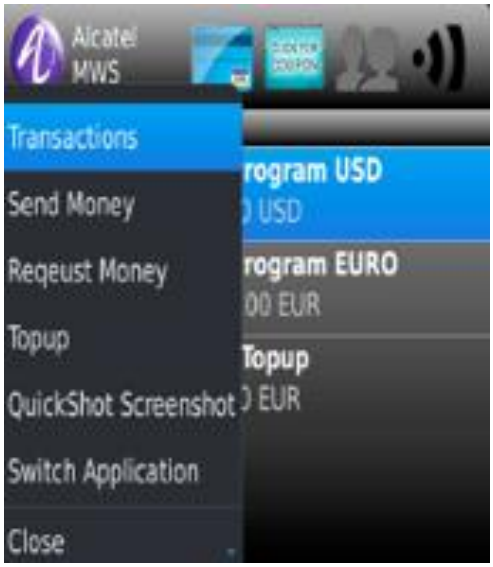

Figure 5. User operations for a selected account

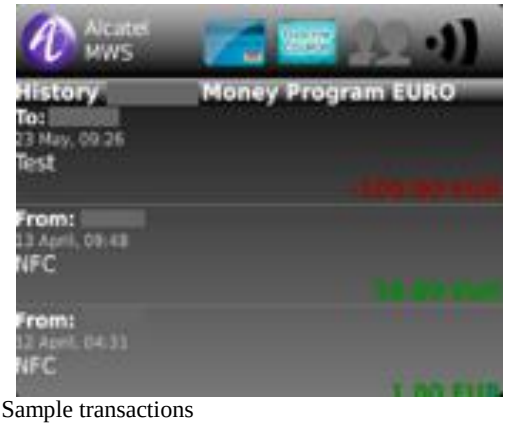

Figure 6. Sample transactions

4. Conclusion

Improvement in the mobile technology changed the way we used our phones and added more functionality. NFC enabled mobile devices can be used for mobile payment systems to replace our credit cards with our mobile phones.

In this paper, we have developed two core applications and a test

terminal application for NFC based mobile wallet system. First part of the application involves SE development, which took place in SIM card with Java Card technology. Second part contains end user interfaces and MWS communication layers. Both sections are developed and tested in real life scenarios and use cases.

Our study is focused to develop solid secure NFC based mobile wallet with REST based web services. User data is protected by SIM-SE securely with user defined PIN code. Critical user credentials and payment secrets are kept in SIM- SE, mobile phone itself doesn't store any sensitive information. This design is successfully implemented and tested in several cases.

As future work, we will integrate our application for new released NFC supported mobile phones also, we will test SE based application on different SIM vendors to increase application availability.

Acknowledgements

This study is supported by Republic of Turkey, Ministry of Science, Industry and Technology by reference code 00810.STZ.2011-1.

References

[1] H. Su, X. Wen, and D. Zou, "A secure credit recharge scheme for mobile payment system in public transport," {IERI} Procedia, vol. 4, no. 0, 2013, pp. 303 – 308, 2013 International Conference on Electronic Engineering and Computer Science (EECS 2013). [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2212667813000464.

[2] E.-J. Steffens, A. Nennker, Z. Ren, M. Yin, and L. Schneider, "The sim-based mobile wallet," in Intelligence in Next Generation Networks, 2009. ICIN 2009. 13th International Conference on, Oct 2009, pp. 1–6.

[3] H. Zhao and S. Muftic, "The concept of secure mobile wallet," in Internet Security (WorldCIS), 2011 World Congress on, Feb 2011, pp. 54–58.

[4] R. T. Fielding, "Architectural Styles and the Design of Network-based Software Architectures," Ph.D. dissertation, University of California, Irvine, 2000.

[5] "Alcatel mobile wallet services," 2011, URL: http://www.lucent.com/wps/DocumentStreamerServlet?LMSG CABINET=Docs and Resource CtrLMSG CONTENT FILE=Other/MobileWalletService intro leaflet December 2011.pdf [accessed: 2014-05-30].

[6] "Nfc architecture," URL: http://nfc-forum.org/our-work/specifications- and-application-documents/specifications/ [accessed: 2014-05-30].

[7] S. Ghiron, S. Sposato, C. Medaglia, and A. Moroni, "Nfc ticketing: A prototype and usability test of an nfc-based virtual ticketing applica- tion," in Near Field Communication, 2009. NFC '09. First International Workshop on, Feb 2009, pp. 45–50.

[8] J. Morak, V. Schwetz, D. Hayn, F. Fruhwald, and G. Schreier, "Elec- tronic data capture platform for clinical research based on mobile phones and near field communication technology," in Engineering in Medicine and Biology Society, 2008. EMBS 2008. 30th Annual International Conference of the IEEE, Aug 2008, pp. 5334–5337.

[9] I. Cappiello, S. Puglia, and A. Vitaletti, "Design and initial evaluation of a ubiquitous touch-based remote grocery shopping process," in Near Field Communication, 2009. NFC '09. First International Workshop on, Feb 2009, pp. 9–14.

[10] E. Siira and J. Haikio, "Experiences from near-field communication (nfc) in a meal service system," in RFID Eurasia, 2007 1st Annual, Sept 2007, pp. 1–6.

