NFC Loyal for Enhancing Loyalty Services Through Near Field Communication

Busra Ozdenizci · Kerem Ok · Vedat Coskun

Citation:

Ozdenizci, B., Ok, K., & Coskun, V. (2013). NFC Loyal for Enhancing Loyalty Services Through Near Field Communication. *Wireless personal communications*, *68*(4), 1923-1942.

Abstract

Near Field Communication (NFC) as an emerging technology is currently leveraged by large standardization efforts and tries to find a suitable ecosystem. NFC enabled mobile devices with integrated smart cards introduce compelling opportunities and new business models. Development of new standards such as secure element (SE), smart card, secure channel, as well as JavaCard enables creating new ecosystems using a concurrent multi application platform which takes advantage of GlobalPlatform standards. We proposed NFC Loyal, which maintains storage, retrieval, and sharing among payment and loyalty applications through our proposed structure, called as Secure Common Domain Management (SCDM) system. SCDM as a centralized database management system on the SE stores valuable information provided by payment applications and shares them with loyalty applications through a secure channel. The direct outcome of using NFC Loyal is the increase in repeat purchases of customers; as well as being a beneficial business plan realized among the payment firms, loyalty firms, and the card owner, resulting in a win-win business model. In this study, we describe NFC Loyal model with its technical infrastructure, and present the NFC Loyal model's life cycle management on SE.

Keywords – NFC, loyalty, smart card, secure common domain management, NFC Loyal

1. Introduction

A smart card is an Integrated Circuit (IC) card with an embedded secure microcontroller consisting of internal memory which can process data as defined by Smart Card Alliance [1]. A mobile phone with a Near Field Communication (NFC) interface can further communicate with other NFC devices. Integration of contactless smart card technology with mobile phones increased the mobile service usage over the world especially for the applications that need to process fast and secure transactions. Sample applications are transit fare payment cards, government and corporate identification cards, electronic passports and visas, and financial payment cards. Moreover, integration of NFC technology with smart card technology on mobile devices allows centralizing various applications such as payment, ticketing, loyalty and access control on one central device [2].

It is true that development of smart card technology affects usage of mobile devices vastly. Service providers have introduced different secure applications on smart cards for end users. Smart cards enable secure storage of valuable information and provide secure area for the execution of applications on the smart card for this reason. In fact, smart cards' potential to increase its popularity depends on its ability to enable secure usage of multiple applications on one single card. Thus providing trusted, secure, interoperable, and multi-application platform became a crucial issue for those applications.

NFC technology is one emerging and promising technology that have adopted smart card as secure element (SE) to provide a secure area for the execution of multiple applications as well as storing sensitive data. NFC technology is a short-range, high frequency, and low bandwidth wireless technology which occurs between two devices within few centimeters, using 13.56 MHz frequency, with a bandwidth not more than 424 kbit/s [2, 3, 4]. NFC technology provides card emulation, reader/writer, and peer-to-peer operating modes where communication occurs between an NFC mobile on one side, and an NFC reader, an NFC tag (passive RFID tag) or an NFC mobile on the other side [2]. Reader/writer mode provides NFC mobiles to read and modify data stored in NFC compliant passive RFID tags. Card emulation mode enables embedding information of some traditional physical components, such as payment or door key cards, onto the smart card. Peer-to-peer mode enables two NFC mobiles to establish a device-to-device link-level communication to exchange any kind of data.

There are several SE alternatives that can be used as secure area for NFC enabled applications such as Universal Integrated Circuit Card (UICC), Embedded SE, and Secure Memory Card. These alternatives are supported by the architecture of mobile handsets as well [5, 6, 7]. Researchers acknowledge UICC as a promising, removable SE solution for NFC technology that is compliant with GlobalPlatform smart card standards and can securely host multiple applications. The usage of NFC technology with smart cards on mobile handsets definitely pushes the multi-application technologies towards a model that enables more and more valuable services on a typical SE [8].

It is currently a demanding area for researchers and practitioners to enable secure concurrent execution of multiple applications on the same smart card. Lots of cards such as credit cards, debit cards, membership cards, and loyalty cards can be stored in one single card. With the help of the payment (credit and debit card) applications the availability, mobility, and simplicity of using loyalty services can be increased to obtain more customer satisfaction and customer loyalty. So, advantages of loyalty cards can be enriched which act as an effective marketing tool.

For most companies, growth means increase in revenue, which is mainly caused by saving current customers and acquiring new customers as well as retaining old customers. Thus, analyzing the customer purchase behaviors is one important step to predict expected behaviors of individual customers and using this knowledge to perform efficient marketing activities. In traditional marketing activities, customer acquisition is mainly performed by mass marketing. In order to obtain new customers, a marketing manager selects the demographics properties of the target customers (e.g. age, gender, marital status) that the company is interested in, and then works with a data vendor to obtain lists of customers who matches those characteristics. The data vendor has large databases containing vast amount of prospective customers that can be segmented according to specific demographic measure, using traditional customer analysis methods. Hence the company can contact these customers with their marketing tools through different channels such as direct mailing, telemarketing, and mail.

However, in time the increase in customer data in warehouses caused complexity. Using traditional customer analysis methods to segment customers and manage that huge data became more and more difficult, and these methods started to meet the limited aspects of business needs [22], which was a headache for companies.

Currently, loyalty smart cards have a positive impact on the repeat purchase behavior of loyal customers through stimulating product or service usage as well as increasing switching costs. Customers receive a number of loyalty or membership cards from different companies and get benefits from each of them such as free miles, points, or coupons for each transaction, which can be defined as structured marketing efforts [9]. Hence, companies started to perform efficient analysis on complex customer databases using new advances in the technology such as Customer Relationship Management (CRM) software tools. However, big number of loyalty cards in the user's wallet also create unmanageable and problematic situation such as misuse of customer data.

At this point we believe that more attention on loyalty programs in terms of NFC technology is required [11] since NFC technology aims to integrate people's daily usage needs into their mobile phones securely and to eliminate the need for physical objects (i.e., identification, loyalty, debit and credit cards, keys as well as wallets) to be carried by the customer.

In this study, a new way of operating NFC enabled loyalty services on SEs is modeled as NFC Loyal which is based on today's promising smart card architecture standard of GlobalPlatform. NFC Loyal extends conventional understanding of loyalty card to a more efficient and secure usage by storing loyalty data on the SE which is embedded to a mobile phone, and by enabling secure data exchange between applications afterwards. According to our proposed model, loyalty and payment applications share and exchange valuable information to obtain mutual financial outcomes, to increase the repetition of purchase behavior of existing customers, and to start new purchase behavior if it already does not exist. Applications exchange required information as configured by the user. The payment applications send the data to the Secure Common Domain (SCD) which is maintained by the Secure Common Domain Management (SCDM) system on the smart card. Partners such as membership, loyalty, and payment applications can use the data appropriately afterwards if they are authorized to do so. Data exchanging between applications will be restricted and will be provided as it is configured by the user which will be explained in further sections. Some subset of the purchase information those are transferred to the SCD by the payment applications, can be used by loyalty applications, if it is classified as "sharable" by the user. At this time one important issue is that no loyalty application is able to modify information on the SCD. Such a model paves the way for other potential offers (i.e. gain coupons, discounts, free miles or free talks).

The proposed NFC Loyal model provides more efficient storage of valuable information on SE by integrating NFC enabled loyalty and payment applications. In contrast to the limitations and problems mentioned above, NFC Loyal provides secure storage and management of the sensitive data on the NFC mobile on user's side; whereas easy collection and analysis of valuable customer data by simple data mining techniques on service provider's side. So, service providers can provide benefits to their customers and reach more customers easily by taking advantage of improvements made by the NFC technology and smart cards.

In this section, we introduced the features of the NFC technology and loyalty card programs together with early and brief definition of NFC Loyal. The remainder of the study is organized as follows. In the second section, the technical background for NFC Loyal is provided. In the third section, we explain NFC Loyal Card details, some scenarios, NFC Loyal architecture, and its life cycle management on SE with a promising ecosystem model. In the fourth section, we provide a short discussion of the NFC Loyal model and finally, a conclusion on the topic is given in the last chapter.

2. Technical Background

2.1 GlobalPlatform Specifications

The most promising standards for management of multiple applications on the UICC based SEs that is also acceptable by the financial industry appears to be developed by the GlobalPlatform [6]. GlobalPlatform is a cross-industry membership organization comprising over 50 organizations, responsible for specifically providing and promoting interoperable technical specifications necessary to support SEs (i.e. UICC, Embedded SE, and Secure Memory Card) selected for NFC enabled mobile handsets [5, 6].

We also agree that GlobalPlatform specification is a proper card specification which offers secure, and flexible multi-application card content management functionality during a card's life cycle [13, 14]. GlobalPlatform card specification is comprised of a number of logical and physical components that aim to provide application interoperability and security in an issuer controlled environment.

The main entities of GlobalPlatform card specification are Card Manager as central administrator of the card, Card Issuer, and Service Providers which are the companies (banks, mobile network operators etc.) those have a business relationship with the Issuer. Card Manager can be viewed as a composition of three entities which assume multiple responsibilities; The GlobalPlatform Environment (OPEN), The Issuer Security Domain, and Cardholder Verification Method Services [5, 14].

Each entity has its own security domain. Security domains of GlobalPlatform act as on-card representatives of off-card authorities and have their own security architecture. They are responsible for performing cryptographic functions, generating and handling keys, and implementing secure channel protocols. In accordance with GlobalPlatform

Card Specification 2.2 [5], security domains will be the critical components in our SCD specification to store keys, and control access to the SCD database. Other required security domains in the GlobalPlatform Card are the Issuer Security Domain (ISD), Application Provider Security Domain (APSD) and Controlling Authorities' Security Domain (CASD). As stated in [5, 14], ISD is the first application installed on a card and performs all issuer related card content management. APSD or Supplementary Security Domain (SSD) maintains a secured environment where application providers are allowed to download, install, and maintain applications following their own life cycle. CASD is a special type of APSD or SSD which enforce the security policy on all application code loaded to the card.

GlobalPlatform is designed to provide maximum flexibility to the Card Issuer as well as its business partners regarding card content management which includes loading, installation, extradition, registry update, and removal of card content. Due to this flexibility, Card Issuer can delegate card content management functions to an Application/Service Provider - delegated management content loading - with or without authorization. At this point, appropriate content management policy on smart cards becomes a fundamental concern; flexible, easy, safe and dynamic structure of a policy is required, rather than closed or open multi-application smart card policies [8].

Another important issue is that a SE platform needs to be managed and controlled by platform manager preferably via Over the Air (OTA) technology [13, 15]. OTA technology enables secure wireless communication between the OTA provider and the client, also providing remote download, installation, and management of NFC services to mobile devices through wireless communication. Providing flexible and interoperable OTA solution is a key requirement in proper NFC ecosystem.

2.2 JavaCard Technology

JavaCard is one of the available supporting architectures that enable secure coexistence of multi applications on the same smart card [8]. JavaCard technology is indeed the leading significant smart card operating system standard for multi-application platforms. Researchers often express JavaCard technology as the biggest innovation that can store and manage dynamically multiple applications [8]. Efficient content management and need for clear separation among applications are the most cited issues up to now. In JavaCard technology, isolation between the operating system and the applications, as well as the isolation of each applet (application on the mobile device, that is written using Java programming language) on the card are provided through a firewall mechanism which is added on JavaCard Runtime Environment (JCRE). Such a mechanism ensures the privacy of the user as no service provider is able to see other applications data on the SE. In cases when applets need to share data, collaborate directly with each other, or to access services JCRE, the Java Virtual Machine (JVM) (i.e. JVM has number of cryptographic services, key repositories) allows such possibilities through a secure mechanism [8]. Integration of GlobalPlatform Card Specification with JavaCard technology provides the necessary functionality for our proposed model in terms of secure storage of keys, key management system, and distinct security domains of GlobalPlatform Card Architecture.

2.3 Secure Channel Protocols

Security vulnerabilities of a SE increase in multi-application environments due to sharing data and resources. Similar case is valid for NFC Loyal, because of sharing sensitive data among payment and loyalty applications. Establishment of a secure channel via secure channel initiation, operation and termination [16] between the SCDM applications and the service applications reduces the risk.

In GlobalPlatform Card Specification, two important secure channel protocols are defined which are SP01 and SP02. Both of them focus on integrity, data origin authentication, and confidentiality. The difference among them is that SP01 provides mutual authentication between the card and off-card entity; while SP02 provides entity authentication, means that the card authenticates the off-card entity initially and the off-card entity may further authenticate the card [5].

SE's multi-application environment can benefit from the use of public key cryptography, and this cryptography can be beneficial for the establishment of a secure channel and higher levels of confidence when two unknown parties want to establish keys, and protect subsequent communications.

3. NFC Loyal Model

3.1 NFC Loyal Model Definition

NFC Loyal is a beneficial model to share the payment data among payment and loyalty applications according to the filters as configured by the mobile user. NFC Loyal model includes several phases; OTA transfer of the required applications to the smart card, installation and configuration of the applications by the user, storage of transaction data by the payment applications, and retrieval and proper usage of the data by the loyalty applications as authorized by the smart card owner.

Usage of NFC Loyal provides different benefits to each actor in the ecosystem. The primary actor in this model is obviously the user as the owner of the NFC enabled mobile device. She is the one who should be motivated to use NFC Loyal, and thus to install SCDM system, and make use of it by the payment and loyalty applications installed on the SE. Sample benefits of the NFC Loyal user are earned coupons, discounts, free miles and free talks. On the service providers' side, loyalty card issuers will face with increase in repeat purchase of the offered product or service and will hopefully acquire more loyal customers. Individual gains of each party will increase, as users and payment services agree to share more information with the loyalty services. The barrier on increasing the exchanged information is of course the pessimism about the risk of leaked data usage for malicious purposes. Hence, there is a tradeoff between increase on the benefit, and the amount of the shared data that might be subject to privacy misuse.

Several challenging NFC Loyal scenarios on smart card can be given. Applications on SE can send/forward information onto the SCD, or receive / retrieve the information those are previously sent/forwarded by a payment application. In this study, we focus on some scenarios which ensure the interaction between payment and loyalty applications installed on the SE:

Scenario 1: A customer purchases gasoline from a gas station (Gaseous) using her NFC enabled device, where payment is performed using the credit card application on the smart card. The transaction information (id, gasoline as the category, date, time, price, company and location etc.) is stored on the SCD immediately. A loyalty application of another gas station that is already installed onto the smart card may obtain that transaction information from the SCDM system and may give an immediate offer to the customer for her next possible gas purchase. The service provider of credit card application can prefer not to store the earlier company's name (Gaseous) to satisfy privacy. To sustain this issue, a setting mechanism is to be implemented prior to the purchase.

Scenario 2: Loyalty cards can also be used to collect shopping habits of people. In return, service providers such as retailers can gain from that valuable information. A customer makes a purchase from a supermarket (ACME Market) using her debit card application which is installed on the NFC mobile. This transaction is stored on the SCD. A loyalty application of a famous cosmetic brand in that supermarket (My Cosmo) can propose an immediate offer (e.g. buy two My Silk Cream, and earn %30 discount) to the customer.

Scenario 3: The customer purchases a ticket to a destination, from Flier Airlines with debit card application on his/her mobile phone. This transaction information (id, airline, date, time, price, company, location etc.) is stored on the SCD by the loyalty application. Other information includes the ticketing details. Loyalty application of a local arrangement company on her mobile phone can give immediate, different offers such as hotel, exciting trips in that certain place, entertainments, concerts etc. We can extend this scenario and use an alarm mechanism on the SCDM system. This mechanism's goal is to activate customer's repeat purchase behavior if customer did not make any purchase for a long time from a specific company (e.g. Flier Airlines). To achieve this functionality, time will be the trigger condition of such a mechanism.

3.2 NFC Loyal Model Architecture

Payment and loyalty programs are to be OTA downloaded to the SE, and installed and configured by the user as already explained before. We use GlobalPlatform card specification that provides appropriate framework including all of the ingredients to enable NFC Loyal model. According to that specification, the smart card architecture is comprised of a number of logical and physical components such as microprocessors, OPEN and GP Trusted Framework as the communication component, RTE as the run time environment, security domains to store information such as keys and files, and several application slots to install applications by the Card Issuer, Application Provider, and Global Services [5, 14]. In our proposed model, we use this architecture to satisfy NFC Loyal requirements, and demonstrate our model on GlobalPlatform card architecture in Figure 1:

- SCDM application is to be installed to the application cluster, and SCD be created on the security domain cluster.
- Payment and loyalty applications are to be installed on the applications cluster, and they create their security domains as expected on the security domain cluster.

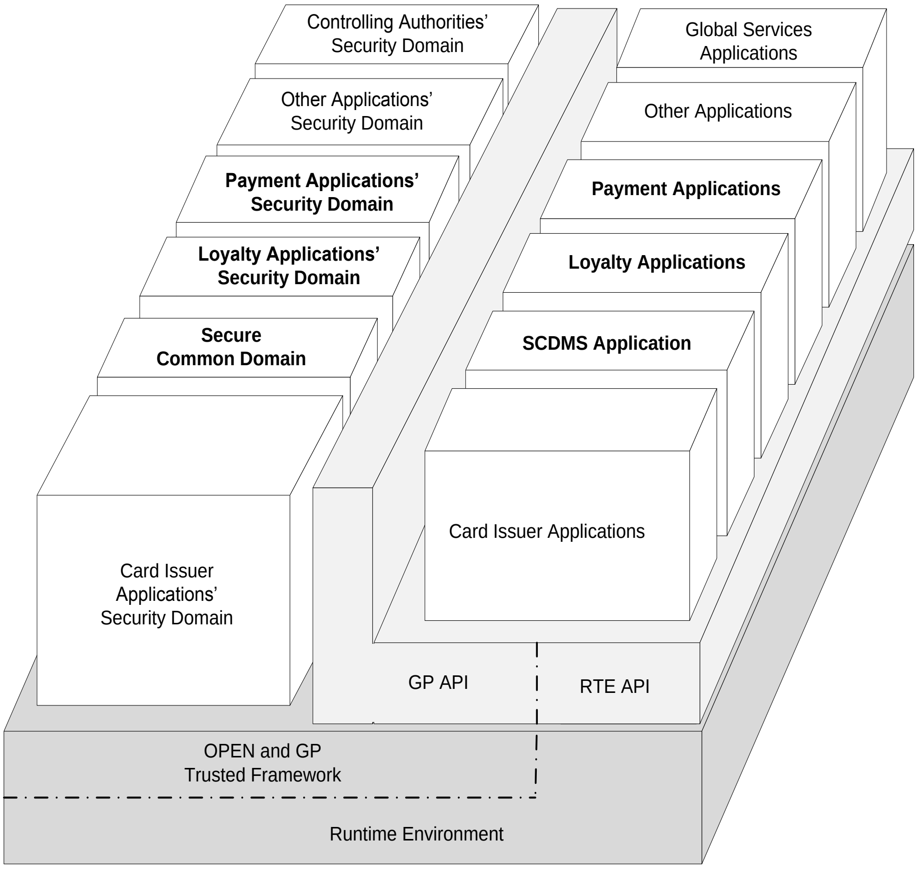

Controlling Authorities' Security Domain
Global Services Applications
Other Applications' Security Domain
Other Applications
Payment Applications' Security Domain
Payment Applications
Loyalty Applications' Security Domain
Loyalty Applications
Secure Common Domain
SCDMS Application
Card Issuer Applications' Security Domain
Card Issuer Applications
GP API
RTE API
OPEN and GP Trusted Framework
Runtime Environment

Figure 1. NFC Loyal Architecture

SCD can be viewed as a centralized secure database storage cluster which aims to enable secure data storage and data sharing by the payment and loyalty applications. SCD is managed by the SCDM system which acts as the interface between the SCD and the applications. Please remember that sample related scenarios are already given in Section 3.1. SCDM system is responsible for storing the data that is sent by the payment applications, as well as from responding to queries made by the loyalty applications. SCDM system provides following services to the payment and loyalty applications:

- Secure data insertion by the payment applications, so that only authorized actors can insert data,
- Secure data storage, so that only authorized actors can access data,
- Secure data retrieval by the loyalty applications, so that no eavesdropping or similar attack can succeed to reveal the content, and no active attack is possible against other security concerns such as integrity,
- Availability of secure data for all types of authorized requests,
- Database design requirements (e.g., durability, consistency, and integrity) usage,
- Configuration by user, so that only the intended data will be transferred to specified applications.

3.3 NFC Loyal Actors

Main actors of NFC Loyal are users, card issuers, SCDM providers, payment service providers, loyalty service providers, certificate authority, and trusted service manager. The role of each actor is described below:

- **User** is the card holder, who currently owns and makes use of the smart card and maintains the contents of the SE with the authorization of the card issuer.
- **Card Issuer** is the issuer of the smart card and holds ultimate responsibility of the smart card by keeping the master key of the smart card, so that it can further be used by the Trusted Service Manager.
- **SCDM Provider** provides SCDM application.
- **Payment Service Provider (PSP)** provides the payment services via the applications. Banks and other financial institutions can provide payment services in form of debit payment and credit payment applications.
- **Loyalty Service Provider (LSP)** develops the loyalty services via the applications. Every firm can provide loyalty services such as rewards, points, or some other advantages.
- **Certificate Authority (CA)** is a trusted entity such as government agency or a certified financial institution who issues digital certificate. These digital certificates will be further used by the NFC Loyal actors (i.e., SCDM provider, PSPs and LSPs). We use these certificates for authentication and non-repudiation purposes. SCDM as well as payment and loyalty applications need to receive a valid certificate from the CA, and use it to prove its identity before the installation.
- **Trusted Service Manager (TSM)** is a neutral and trusted party from both users' and service providers' perspectives. It handles all security and privacy issues of NFC Loyal model and manages security credentials and public keys for message encryption.

In NFC Loyal model, TSM indeed has the most strategic importance. TSM is independent and possibly government related party serving to all other actors. Its main responsibility is to create and manage a trusted environment and also to provide a network among Mobile Network Operators (MNOs), CAs, LSPs, PSPs and users. TSM is mainly responsible for securely provisioning and managing the life cycle of the NFC based applications and services, and providing a flexible OTA solution for NFC application life cycle management [13, 17]. It authorizes applications before it is downloaded to mobile phones. Also TSM is able to manage (delete, update, lock, unlock) the applications installed to SE on behalf of users and SPs. Its trustworthiness enables managing and controlling multiple applications on the same SE.

In accordance with the NFC ecosystem study of [18], TSM can provide a central location called as "application pool" for housing applications. Applications can be uploaded by SPs to the application pool, and users that intend to use any of those applications will be able to OTA download it from TSM's application pool. Such an application pool under control of TSM provides easy searching and updating of applications, preventing spam-like applications as well as checking the needs of applications in terms of convenience and security [18]. In user's perspective, host application on the SE has ability to deny any application from outside of the application pool.

3.4 NFC Loyal Model Installation

The user who wishes to use NFC Loyal needs to initially download the SCDM system, one or more payment applications, and one or more loyalty application to her mobile phone, from the application pool of the TSM. The pre-installation and installation [18] of SCDM, payment and loyalty applications on SE is explained in the following section. The numbers of each activity represents its legend on Figure 2 which covers the steps 1 through 3, and Figure 3 which covers the steps 4 through 8.

3.4.1 Pre-Installation and Installation of SCDM, Payment, and Loyalty Applications

Step 1: Obtaining a Signed Certificate from CA

1a. SCDM provider requests and obtains digital certificate from CA.
1b. PSP requests and obtains digital certificate from CA.
1c. LSP requests and obtains digital certificate from CA.
1d. User obtains gets her digital certificate from CA.

Step 2: Upload of applications to TSM's Application Pool

2a. SCDM provider needs to sign a business agreement with TSM in order to be able to deploy SCDM application to a SE. In this step, SCDM provider signs a business agreement with TSM, and sends to TSM together with SCDM's certificate. TSM can validate the business agreement using the certificate. Since there is only one SCDM application provider, this business agreement step between SCDM provider and TSM is performed only once for each SCDM application.

2aa. SCDM provider signs a service agreement with TSM, and TSM validates the service agreement and SCDM application. TSM uploads SCDM application to its application pool as it receives. So, SCDM application is ready to be requested and downloaded by users. Since SCDM application is unique and provided by only one service provider, this step also occurs only once.

2b. PSP needs to sign a business agreement with TSM in order to be able to deploy a payment service to SE. Payment SP signs a business agreement with TSM, and sends it to TSM together with PSP's certificate. So, TSM validates the business agreement. Each PSP must sign business agreement with TSM only once.

2bb. PSP signs the service agreement with TSM, and TSM validates the service agreement and service application. TSM uploads the payment application to its own application pool as it receives. So, payment application is ready to be requested and downloaded by users. This step is performed for each application (e.g. PSP may provide more than one payment services) of PSP.

2c. LSP needs to sign a business agreement with TSM in order to be able to deploy a loyalty service to SE. LSP signs a business agreement with TSM, and sends it to TSM together with LSP's certificate. So, TSM validates the business agreement. Each LSP must sign business agreement with TSM only once.

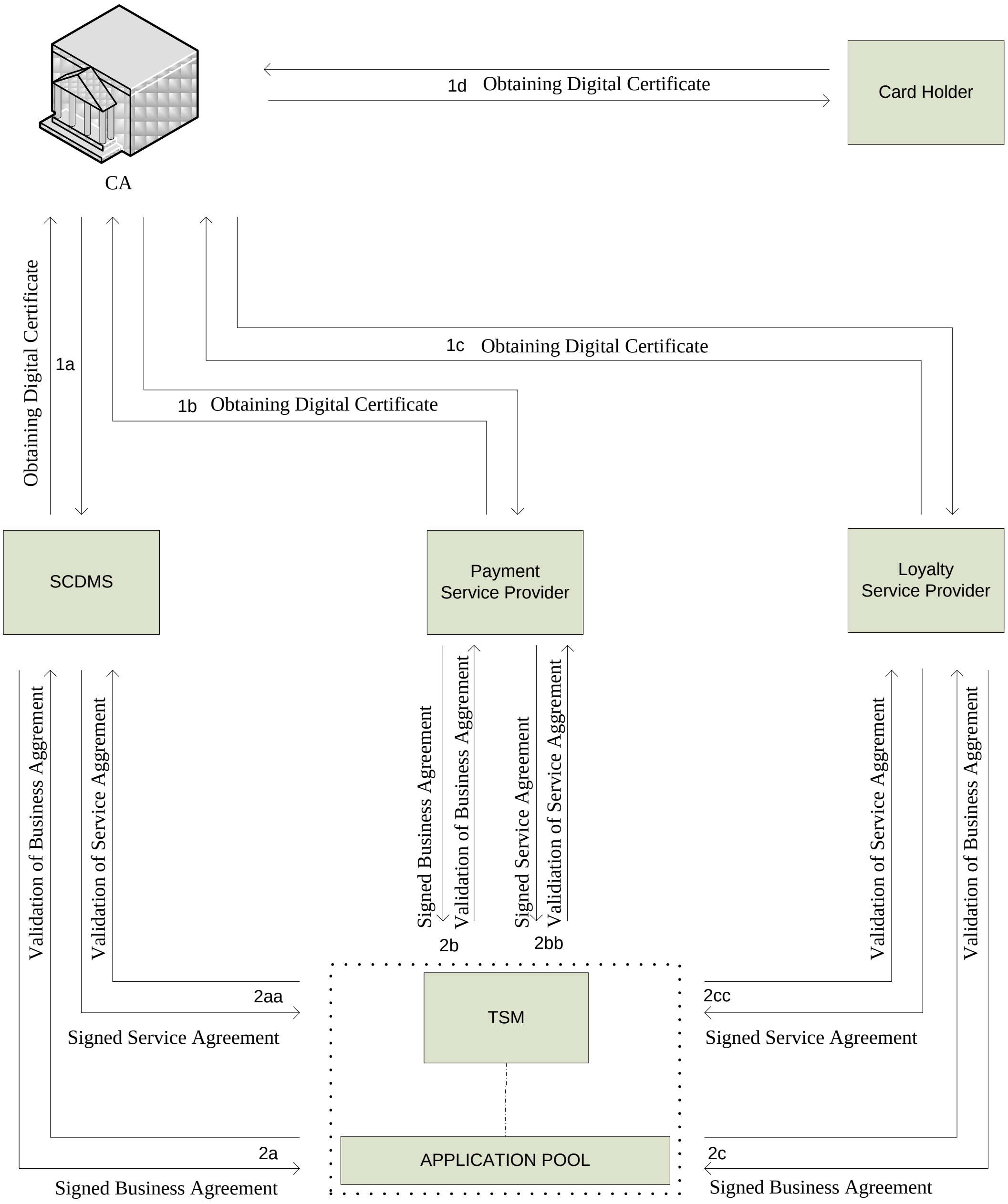
2cc. LSP signs the service agreement with TSM, and TSM validates the service agreement and service application. TSM uploads the payment application to the application pool as it receives. So, loyalty application is ready to be requested and downloaded by users. This step is performed for each application (e.g. LSP may provide more than one loyalty services) of LSP.

Step 3: Requesting SCDM, Payment and Loyalty Application from TSM

3a. User requests SCDM application from TSM's application pool database. Then user is requested to sign SCDM application's service usage agreement by host application on the SE.

3b. Similarly, user requests a payment application from TSM's application pool database. Then user is requested to sign payment application's service usage agreement by host application on the SE.

3c. User requests a loyalty application from TSM's application pool database. Again, user is requested to sign loyalty application's service usage agreement by host application on the SE.



CA
Card Holder
1d Obtaining Digital Certificate
1a
Obtaining Digital Certificate
1b Obtaining Digital Certificate
1c Obtaining Digital Certificate
SCDMS
Payment Service Provider
Loyalty Service Provider
Validation of Business Aggrement
Validation of Service Aggrement
Signed Business Agreement
Validation of Business Aggrement
Signed Service Agreement
Validiation of Service Aggrement
2b
2bb
Validation of Service Aggrement
Validation of Business Aggrement
2aa
Signed Service Agreement
TSM
2cc
Signed Service Agreement
APPLICATION POOL
2a
Signed Business Agreement
2c
Signed Business Agreement

Figure 2. Pre-Installation of SCDM, Payment and Loyalty Applications (Step 1 and Step 2)

Step 4: Taking Control over User's SE

Master key is a unique key and exists in all SEs and the actor who has the master key has control over SE. Master key enables owner to create security domains in SE, control each security domain and install applications to SE [18]. TSM requests user's SE's master key (if it did not receive before) from card issuer in order to take control over user’s SE, and TSM requests this master key at first application installation to the user’s SE (Figure 4). This step is performed only once for each SE.

Step 5: Getting Approval for Installation from User

5a. TSM gets approval for requested SCDM application from user to install them on the SE and personalize them.
5b. TSM gets approval for requested payment application(s) from user to install them on the SE and personalize them.
5c. TSM gets approval for requested loyalty application(s) from user for same purposes.

Step 6: Download of Applications via OTA on User’s SE

6a. After user’s approval for installation, the requested SCDM application is securely OTA downloaded together with SCDM application’s certificate to user’s SE.
6b. Again, after user’s approval for installation, the requested payment application is securely OTA downloaded together with payment application’s certificate to user’s SE.
6c. Similarly, with user’s approval for installation, the requested loyalty application is securely OTA downloaded together with loyalty application’s certificate to user’s SE.

Step 7: Generation of Security Domains, Installation and Personalization of Applications via OTA on User’s SE

7a. With the download of SCDM application, SCD is created on the SE’s security domain cluster.
7b. In case of a payment application, the SE receives a “CREATE SSD” command and Supplementary Security Domain (SSD) is created by the Issuer Security Domain (ISD). Loading and personalization of all service applications are performed by using GlobalPlatform content loading commands [11]. After creation of security domain and personalization of a payment application, payment application is installed and personalized on the SE.
7c. Also, for loyalty application, creation of a security domain and personalization of application are performed.

Step 8: Confirmation

8a. Once the requested operations are performed and the required data are loaded onto the SE; SCDM provider receives a confirmation response, and (optionally) specific keys from the TSM to access the security domain.
8b. Once the requested operations are performed and the required data are loaded onto the SE, PSP receives a confirmation response, and (optionally) specific keys from the TSM to access the security domain.
8c. Also, LSP receives a confirmation response, and (optionally) specific keys from the TSM for same purposes.

3.4.2 Configuration of SCDM Application

After loading phase, user as the owner of the card, configures the SCDM application, loyalty and payment applications. In NFC Loyal, the payment applications can share either partial or all information with loyalty applications, according to the presetting made by the user. To share partial information, a setting mechanism is required that provides marking the transaction tags those will be sent to SCDM system. Such a mechanism is beneficial for users who prefer more privacy to more profit. The amount of the shared information can be low or high, depending on the user's sharing preferences. A user who prefers more privacy may configure the system accordingly, but will gain less than the user who prefers high profit and configures the system to exchange more data among the payment and loyalty applications. This configuration includes the setting mechanism that has been mentioned in case scenarios.

Also, that user needs to decide on which payment applications installed on her smart card will be used for NFC Loyal model, and make necessary configurations on SCDM application. User can select all or some of the payment applications which refers to the credit cards or debit cards, so the transactions that are done by only the selected ones will be stored on SCD. On the other side, the similar configurations for loyalty applications need to be performed by the user. The selected loyalty or membership applications will benefit from user's SCD.

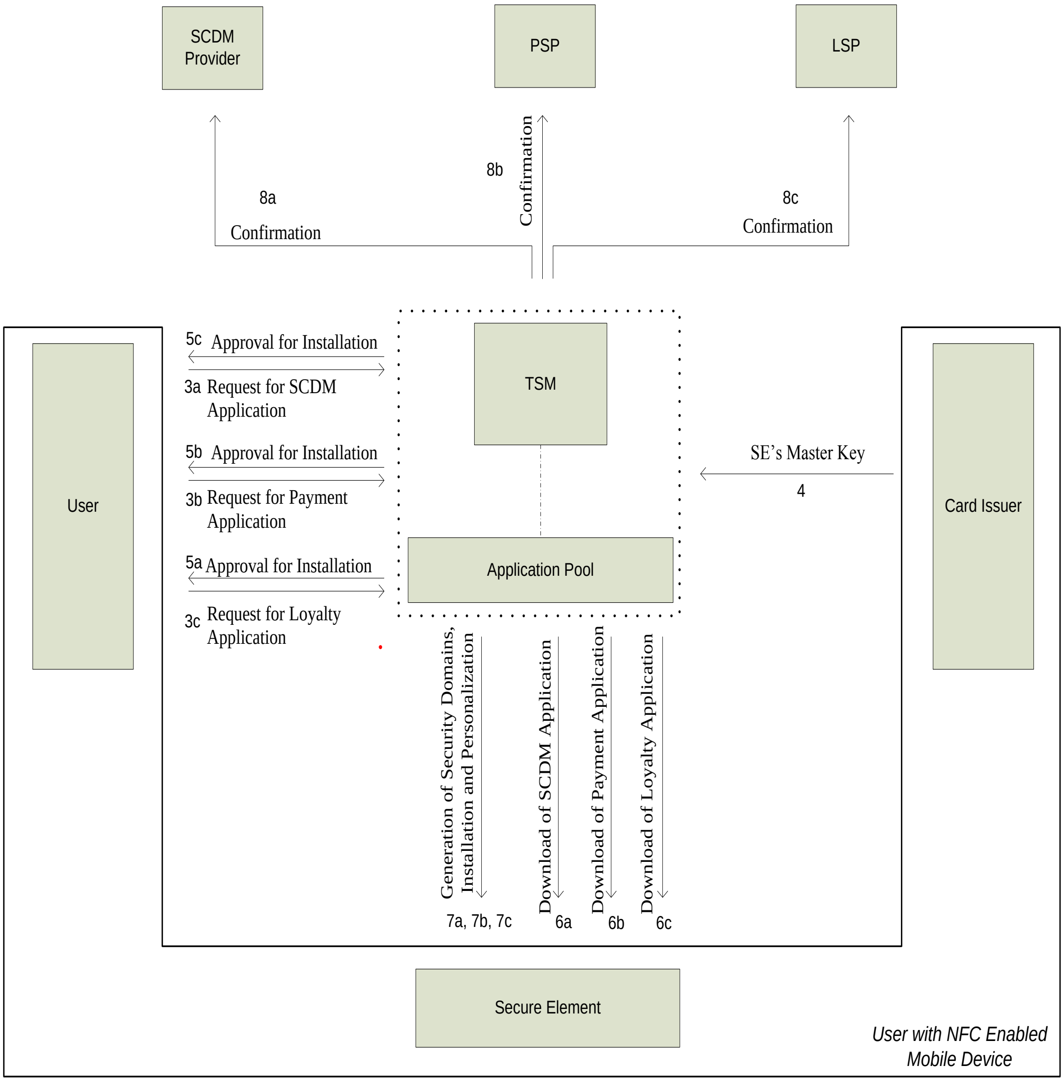

SCDM Provider
PSP
LSP
8b
Confirmation
8a
Confirmation
8c
Confirmation
5c Approval for Installation
3a Request for SCDM Application
5b Approval for Installation
3b Request for Payment Application
5a Approval for Installation
3c Request for Loyalty Application
TSM
Application Pool
SE's Master Key
4
User
Card Issuer
Generation of Security Domains, Installation and Personalization
Download of SCDM Application
Download of Payment Application
Download of Loyalty Application
7a, 7b, 7c
6a
6b
6c
Secure Element
User with NFC Enabled Mobile Device

Figure 3. Installation of SCDM and Payment, Loyalty Applications (Step 3 to 8)

3.5 NFC Loyal Service Usage Model

Through appropriate key management and security mechanism, applications and SCD can interact with each other. Payment applications can send information to the SCD and loyalty applications can receive information from the same database securely. Figure 4 shows the interactions between service applications and SCDM application. After each transaction, the related payment application creates an XML file containing the required information (Figure 6). Then loyalty applications can perform queries and request transaction information that is saved to the SCD those has happened so far from SCDM system. After the request is processed, SCDM application sends the resultant data to the requesting loyalty application (Figure 8). So, loyalty application can benefit from this valuable data and can provide new offers to user.

As a note, secure channel establishment is essential for enabling secure data communication between the SCDM application and the service applications. To achieve a secure channel protocol between them, one of the available public key encryption schemes such as RSA may be used. Secure channel allows a smart card and an off-card entity to authenticate each other and to establish session keys in order to protect the integrity and confidentiality of subsequent communications [16]. For the establishment of secure channel, initiation of secure channel protocol through appropriate Application Programming Data Units (APDU) commands is required by an off-card entity or by an on-card entity (e.g. secures domains, SCD). Secure Channel Protocol initiation phase also involves the authentication of off-card entity by the card. After the secure channel protocol initiation, payment applications and loyalty applications can interact with the SCDM securely.

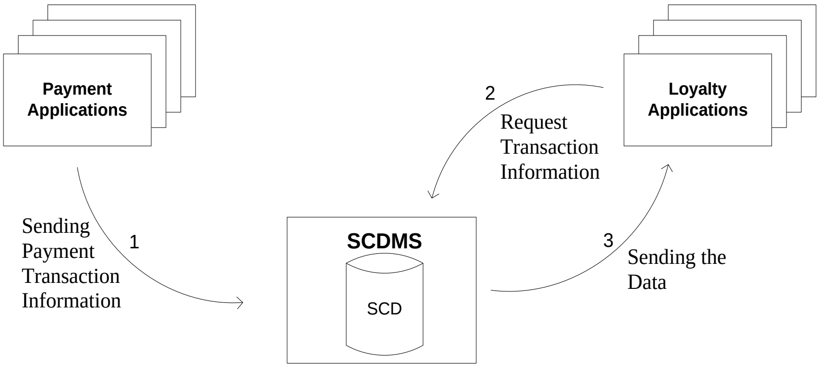

Payment Applications
2
Request Transaction Information
Loyalty Applications
Sending Payment Transaction Information
1
SCDMS
SCD
3
Sending the Data

Figure 4. Interaction with Secure Common Domain

3.5.1 XML Language for NFC Loyal Interactions

In order to provide data exchange between loyalty applications, payment applications, and SCDM system, an interface to access the SE at the application layer is necessary [19]. Thus, the Java Community Process Program has already standardized an Application Programming Interface (API) for using the features of a SE. One of the optional packages of API specifications is the data exchange format to exchange data between a reader and smart card chips, allowing communication with SE through APDU. Currently, SE communicates with phone using APDU. Indeed, the ISO 7816 standards define only a set of low level APDU commands, which perform writing orders, reading orders, or cryptographic functions invocation.

We propose using a high-level language, namely Extensible Markup Language (XML) [20], for the interaction between the SCDM system and the payment as well as loyalty applications. In accordance with [13], XML is the language of choice for structuring messages, and it provides flexibility, interoperability, and a standards-based approach, so that created XML documents will be unambiguous. Moreover it supports different versions of messages as they evolve and be conducive to ease of information parsing and maintenance. Actually, XML is easily adaptable by actors involved in our SCDM model and facilitates future changes in the content model. Thus, XML is a choice to represent communication among applications and SCDM system which should be conceivable to everyone involved in smart card implementations.

XML documents must be both well formed and valid [16] in order to be used. In being a well formed document, the tags within the XML document must not violate XML guidelines. A well formed XML document conforms to the provided DTD document (i.e. Document Type Definition, a context-free grammar for describing XML tags and their nesting). After configuring an application, one separate DTD document must be prepared by the SCDM system. After a DTD document is prepared, each exchanged XML document can be checked against its validity. DTD content can either be embedded into the related XML document, or can be prepared as a separate document. In our proposed model, DTD document is written and saved as a separate document for each transaction, as shown in Figure 5.

In NFC Loyal, payment applications on a single, dynamic smart card stores partial information of occurred transaction to SCD, as defined by the users' filtering configuration. The transaction table has to be created in the database of SCDM. The transaction table typically consists of id, date, time, price, company, location and category columns. Figure 5 shows a sample XML DTD file. ID refers to the transaction id, which is the primary key value and makes that transaction unique. Date and time refer to the occurred transaction's date and time information. Price information is related with the cost of the purchase. The company is where the customer or user makes the purchase and this information is the most critical option. The location is where the company is placed, in which city or country. Company and location information can be concealed by the user configuration. The last tag as category of the transaction is the categorization of the purchased item that can be described as market, gasoline, cosmetics, book, music etc. Furthermore, we can add other category for getting more detailed information about the transaction; such a category will be useful for companies providing valuable offers which were discussed especially in our third scenario in Section 3.1 . Please note that we describe the complete data structure in here, but each payment application will store only the appropriate parts of this definition, and each loyalty application will also be able to request data; both of which is defined by the previous configuration made by the user.

```
<! - -TRANSACTIONS.DTD document - - >
<!DOCTYPE Transactions [
<!ELEMENT Transaction (ID, date, time, price, company, category)>
     <!ELEMENT ID (#PCDATA)>
     <!ELEMENT date (#PCDATA)>
     <!ELEMENT time (#PCDATA)>
     <!ELEMENT price (#PCDATA)>
     <!ELEMENT company (#PCDATA)>
     <!ELEMENT category (#PCDATA)>
     <!ELEMENT other (#PCDATA)>
]>
```

Figure 5. A Sample Transaction DTD document of Payment Application

```
<! - - TRANSACTIONS.XML document - - >
<? XML VERSION = “1.0” ENCODING=“ISO-8859-1” STANDALONE = “no”?>
<Transactions>
<Transaction category= ”Gasoline”>
    <ID> 101 </ID>
    <date> 15 October 2010 </ date>
    <time> 14:00 </ time>
    <price> 45.00 </ price>
    <company> GASEOUS </ company>
    <location> Istanbul </location>
<Transaction>
<Transaction category= ”Market”>
    <ID> 103 </ID>
    <date> 15 October 2010 </ date>
    <time> 17:00 </ time>
    <price> 50.00 </ price>
    <company> VIMJA </ company>
    <location> Istanbul </location>
<Transaction>
<Transaction category= “Gasoline”>
    <ID> 102 </ID>
    <date> 16 October 2010 </ date>
    <time> 14:15 </ time>
    <price> 55.00 </ price>
    <company> GASEOUS </ company>
    <location> Istanbul </location>
</Transaction>
</Transactions>
```

Figure 6. Sample Transactions XML Document from Payment Application

Let’s consider a simple case on NFC Loyal interactions. A user started to use NFC Loyal model on October 14 and started to make purchases using her NFC enabled mobile phone. The payment application on user’s smart card creates an XML document as a record of the transactions done after October 14 as seen in Figure 6. These three transactions (two of them are gasoline purchases, one of them is market purchase) are prepared according to the DTD document which was formed at the beginning of XML record. All category, id, date, time, price and company information was explicitly given by the company and by the user. This sample XML document is sent from Payment Application to SCDM system securely, and accepted and stored on SCD in transaction.xml document, by SCDM application. On the other hand, a loyalty application can receive information from SCD by making queries to SCDM application and SCDM application responds these queries. To provide this interaction, a query language for XML called XQuery [21] is used in our model. XQuery provides selection of information based on specified criteria by loyalty application and filtering out unwanted information, sorts, and groups and aggregates the data [21]. FLWOR expression is the basic structure of many queries according to the literature, thus we propose to use this expression. After a time, a loyalty application of a gasoline company called GASPOWER on user’s SE makes a request from SCDM system through XQuery language principles. As seen in Figure 7, the request from GASPOWER Loyalty application is about getting price information of the gasoline purchases done up to now. This XML query is sent to SCDM application securely, and SCDM application decrypts and processes the query. The query result is formed (Figure 8), and sent to GASPOWER loyalty application securely.

```
for $transaction in doc(“transaction.xml”)/transactions/transaction
let $price := $transaction/price
where $transaction/@category=”Gasoline”
return $price
```

Figure 7. A Sample XML Query Document from Loyalty Application

```
<result>
    <price> 100.00 </price>
    <price> 50.00 </price>
</result>
```

Figure 8. A Sample XML Query Result Document from SCDM

4. Discussion

NFC Loyal model is supposed to enable an alternative complementary way to improve technical and business opportunities drastically which is based on NFC technology and GlobalPlatform compatible smart cards. NFC Loyal model on user’s SE allows companies to provide loyalty services in a new mechanism. User earns money or some goods by sharing some of her purchase information and gets valuable offers from the SCDM application stored on the smart card. Through SCDM application the companies can easily suggest value added offers or perform advertising. According to the NFC Loyal model’s life cycle management, the user needs to download the SCDM application, payment and loyalty applications from TSM’s Application Pool [18], and install them on her SE’s application domain via OTA platform. Actually, the user as well as providers of SCDM and service applications must sign required agreements by TSM to ensure proper uses of data and acceptance of the financial and legal issues. After installation process, user configures her SCDM application to obtain offers from the loyalty applications of companies already installed on her mobile phone.

It is important that the SCDM application keeps all stored data securely, do not transfer the information to any other party (application) not installed on the smart card and configured properly, and not to any other remote server such as company database as well. This conforms to the current situation where DBMS applications are trusted parties in this sense. The information that is stored on the SCD after each transaction is under the control and responsibility of the user, so that user can store partial or all information (i.e. date, time, price, category, location, company information etc.) of each payment transaction that she performs.

The stored information is comparable to the information on credit card statements that we receive from banks at the end of each month. But in our model, the transaction of each payment performed by NFC enabled mobile device will be stored on smart card’s SCD after each transaction immediately. This difference actually will have so huge impact on the loyalty schemes. In current situation the transaction information can be processed in live fashion only by the bank, since the transaction information is saved only in the bank’s database in real time. In our model, each authorized loyalty application can use the transaction information online. The impact is so big. One loyalty application can offer a discount meal to the user immediately after the purchase information in some location is stored in the SCD. Another loyalty company can offer a discount on the gas price, after the driving direction of the user can be guessed after a couple purchases on the way.

The company, whose loyalty application is installed on the user’s smart card, can request information to be transferred to the company server via OTA transfer according to configurations made on the SCDM application. So the company can use the received information to provide more value added services to that user. Also the company can perform same request at any time to all of or partial of his customers who uses SCDM application on their NFC mobiles. So on the background, the company can perform data mining techniques on this large data in classical way, and according to the analysis results it can provide offers to this target group via SMS.

5. Conclusion

In this study, NFC Loyal model is discussed with its complete architectural design, its life cycle management on SE, and its implications. NFC Loyal model provides sharing transaction data among payment and loyalty applications those are installed and configured on the SE by the NFC mobile owner. This model enables more efficient and secure storage of sensitive data on SEs of user’s mobile through a database management system. Hence, service providers can easily collect and perform analysis on these data by simple data mining methods.

NFC Loyal model creates a win-win model on business side by using the benefits of NFC technology as well as facilitates the adoption and development of more card emulation mode NFC services on user side. However, there are some important limitations that should be highlighted within the scope of this study. Up to now, most of the performed trials in NFC context usually include limited number of services without the possibility of removal or insertion of any new or unused NFC service on SEs. Although NFC technology and GlobalPlatform specifications warrants the separation of various NFC applications on the same smart card with high security and minimal risk of corruption, some certain security specifications prohibits this coexistence of multiple applications on the same smart card [6, 17]. However, users would prefer a dynamic multi-application environment within NFC mobiles where they can download or remove NFC services easily. Problems with dynamic multi-application card content management and OTA service provisioning issues should be solved as soon as possible to remove restrictions in front of service providers and MNOs, and allow them to develop innovative NFC applications on a single SE.

This model will create a new market and research area for secure database management solutions in NFC applications context with different performance, quality, data mining techniques as well as features for user friendliness.

References

[1] Smart Card Alliance. About smart cards, frequently asked questions. http://www.smartcardalliance.org/pages/smart-cards-faq. Accessed 10 January 2011.

[2] Coskun, V., Ok, Kerem and Ozdenizci, B. (2012) Near Field Communication: From Theory to Practice. John Wiley and Sons (under publication).

[3] Chang, Y., Chang, C., Hung, Y., and Tsai, C. (2010). NCASH: NFC Phone-Enabled Personalized Context Awareness Smart-Home Environment. Cybernetics and Systems, 41 (2), 123 – 145.

[4] Sixto Ortiz Jr. (2006). Is near-field communication close to success? Computer, 39 (3), 18-20.

[5] GlobalPlatform, GlobalPlatform Card Specification, Ver. 2.2. http://www.globalplatform.org. Accessed 10 January 2011.

[6] Mobey Forum, ‘Best Practice for Mobile Financial Services – Enrolment Business Model Analysis’ (2008). White Paper. Available at: http://www.mobeyforum.org/Press-Documents/White-papers. Accessed 10 December 2011.

[7] Choudhary, B. and Risikko, J. (2005). Mobile device security element: key findings from technical analysis v. 1.0. Mobey Forum.

[8] Sauveron, D. (2009). Multi-application smart card: towards an open smart card? Information Security Technical Report, 14 (2), 70-78.

[9] Sharp, B. and Sharp, A. (1997). Loyalty programs and their impact on repeat-purchase loyalty patterns. International Journal of Research in Marketing, 14 (5), 473-486.

[10] Meyer-Waarden, L. (2007). The effects of loyalty programs on customer lifetime duration and share of wallet. Journal of Retailing, 83 (2), 223-236.

[11] Ozdenizci, B., Coskun, V., Aydin, M. N. and Ok, K. (2010). NFC Loyal: A beneficial model to promote loyalty services on smart cards of NFC-enabled mobile devices. IEEE International Conference for Internet Technology and Secured Transactions, London, 134-139.

[12] Wiechert, Thomas J. P., et al. (2009). NFC Based Service Innovation in Retail: An Explorative Study. 17th European Conference on Information Systems, ECIS, Verona.

[13] GlobalPlatform (2009). GlobalPlatform's Proposition for NFC Mobile: Secure Element Management and Messaging. http://www.globalplatform.org/. Accessed 10 January 2011.

[14] Markantonakis, K. and Mayes, K. (2003). An overview of the GlobalPlatform smart card specification. Information Security Technical Report, 8 (1), 17-29.

[15] Reveilhac, M. and Pasquet M. (2009). Promising secure element alternatives for NFC Technology. First International Workshop on Near Field Communication, Hagenberg, 75-80.

[16] Markantonakis, K. and Mayes, K. A Secure Channel Protocol for Multi-Application Smart Cards Based On Public Key Cryptography. Information Security Group Smart Card Centre.

[17] StoLPaN. (2011). Description of the Life-cycle management of NFC Applications. Resource document. StoLPaN. http://www.nfc-forum.org/resources/white_papers/Stolpan_White_Paper_08.pdf, Accessed 10 Aug 2011.

[18] Ok, K., Coskun, V., Ozdenizci, B., and Aydın, M.N. (2012). A Role based Service Level NFC Ecosystem Model, Journal of Wireless Personal Communications (under publication).

[19] Madlmayr, G., Dillinger, O., Langer, J., and Schaffer, C. (2007). The Benefit of Using SIM Application Toolkit in the Context of Near Field Communication Applications. International Conference on the Management of Mobile Business, 5.

[20] W3C Recommendation, Extensible Markup Language (XML) 1.0. http://www.w3.org/TR/REC-xml/. Accesssed 10 January 2011

[21] XML Query Language. http://www.xquery.com/. Accessed 10 January 2011.

[22] Srivastava, J. Data mining for customer relationship management. http://www.dtc.umn.edu/ddmc/resources/crm.pdf. Accessed 10 January 2011.