Loyalty Systems over Near Field Communication (NFC)

Diogo Simões
IST - Technical University of Lisbon
Av. Prof. Cavaco Silva
Tagus Park
2780-990 Porto Salvo, Portugal
diogo.simoes@tagus.ist.utl.pt

Abstract. This work presents an integral and detailed alternative solution for creating and managing loyalty cards, through the NFC (Near Field Communication) technology. The concept of the solution is motivated by the fact that current loyalty solutions impose their users to always carry with them all the loyalty cards he possesses. The main objective is to allow users to keep their cards in a virtual and safe way, supported by Near Field Communication enabled mobile phones.
This solution states that if a user has access to his mobile phone, then he has access to any of his loyalty cards he may need and he also can consult the cards information.

Keywords: NFC (Near Field Communication), mobility, mobile communications, loyalty

1. Introduction

Customer Loyalty is when a product or service satisfies the expectation of the customer who becomes loyal to that satisfaction and to the company which provided the product or service, despite similar products may be sold cheaper by a competitor. Nowadays, most companies seek to get more and more loyal customers by creating almost a personal relationship between each of them. Identification documents (from now on will be called "cards") combined with CRM (Customer Relationship Management) solutions provide companies with useful structured information. This information gives the companies a possibility to define a profile for each user or groups of users, which is the necessary data for gaining customers loyalty.

As a result of the place Loyalty Programs take in companies' success, people have to carry a pile of cards in their purses every day, since they are given cards for almost every company where they are customers. This problem was the main driver for this work. The three main motivations of this work are:

- **Availability -** throughout our everyday lives, we never know when we will need one loyalty card from a specific company. Therefore, we have to carry all of them with us, just in case;
- **Comfort -** when the time to use a specific loyalty card comes, we have to search for that card in the pile we are carrying, which may become a very uncomfortable process;

- **Information Interaction** - currently, cards only allow customers to identify themselves, providing no information at all about their loyalty account. Those cards should provide real-time information such as budgets, promotions, discounts and transactions history.

The main objective of this work is to define and specify a flexible and enclosing modular architecture for loyalty programs. This architecture should be easy to integrate with the existing management systems of the companies. The main requirements, for achieving these objectives, are an enclosing structure of a loyalty card, regardless of the type of loyalty program; the availability of a NFC-enabled mobile device for storing several instances of a loyalty card; providing a GUI (Graphical User Interface) for managing the cards (i.e. information interaction); allowing use of the cards without the need to use the management GUI; being able to carry out a secure Peer-to-Peer transaction between two NFC-enabled mobile phones.

Nowadays, the current loyalty cards have few and limited technologies at their service. Technologies such as barcodes or magnetic stripes cannot compute data, and therefore are a bottleneck for innovative ideas. Smart Cards, despite being capable of computation, still present no interface for the user to manage the data in real-time. Taking these limitations into account, Near Field Communication (NFC) presents itself as the breakthrough technology that integrates the best of Smart Cards, RFID (Radio Frequency Identification) and mobile phones.

NFC is an emergent technology, allowing mobile phones to emulate cards (i.e. store cards data and work as conventional loyalty cards), to read cards or tags and to communicate via Peer-to-Peer. These capabilities and the fact that mobile phones provide an interface for managing the data which was received and sent by them, are the main reasons why NFC was the technology chosen for developing a solution that may accomplish the objectives and the requirements defined earlier.

2. Related Work

As stated in the previous chapter, there is more than one technology working at service of the loyalty programs, but none presents innovation. NFC technology may represent that innovation for loyalty and many other areas such as ticketing, payments and others. This technology, besides the specifications of its own, integrates the most powerful of the technologies referred above and RFID (Radio-Frequency Identification).

2.1. Barcodes

Easily identifiable, the barcodes are a set of parallel black and white stripes. The information is coded by a "never the same" pattern of stripes that vary in width, quantity and order. Despite its low costs, the ease of the creation process and the fact that it helps eliminating the human error, this technology is becoming obsolete. Being suitable to print or read errors, having low capacity for storing information or not being capable of any computation are some of the main reasons why barcodes are not a suitable solution for loyalty programs.

2.2. Magnetic Stripes

First in London, and afterwards in San Francisco, the magnetic stripe appeared for the first time in the 60's, in solutions for Public Transportation Networks [1]. Although still with heavy presence in the financial area, its functionalities did not evolve much the last decades. Magnetic Stripes are brown stripes, made of little magnetic particles that are placed in the back of the cards.

Despite providing modifiable data, higher data storage capacity than barcodes, additional security for not being humanly readable, robustness and low cost, this technology has few possibilities of lasting the next decades. Some of the reasons for that are the lack of computational power, the need for contact with readers and the data corruption when in proximity with magnetic fields.

2.3. Radio-Frequency Identification (RFID)

RFID increases convenience and productivity and can be applied to theft control, toll payment, stock management and monitoring and many other areas. The RFID concept consists of an antenna emitting radio waves to tags (with stored information) that modify and reflect - passive tags - the waves to antenna. There are also active tags, which are self-powered and can send waves by themselves. In an RFID based solution, we can tag each item with its unique information. This information can have access rights (read-only or read-write) and can be wirelessly transmitted to an antenna installed a few meters away. As long as in range of an antenna, RFID creates the possibility of letting us know were a specific object is, inside the system. On the other hand, problems can occur if too many tags are read in a small space.

2.4. Smart Cards

Being a recent technology (introduced in Europe about a decade ago), smartcards present advantages such as: convenience and security increase in transactions, sealed identification data storage, system security increase against badly stored data or attacks [2]. These consist of micro processing units with an internal memory chip controlled by an Operating System. Advantages such as computing power and elevated security and privacy levels have lead to an increasing use of Smart Cards. Another advantage is the fact that a single card can store several different applications, from different companies. Smart Cards can communicate through contact or contactless interfaces.

The main standards for Smart Cards are ISO/IEC 7816 and ISO/IEC 14443. Part 4 of ISO 7816 specifies the structure, the security and the commands (APDU – Application Protocol Data Units) for exchanging data between smart cards. ISO/IEC 14443 is an international standard for Identification Cards - Contactless ICCs (Integrated Circuit Cards) - Proximity Cards. This ISO operates at 13.56 MHz, supporting two types of communication protocols - Type A and Type B. ISO 14443 is backwards compatible with other ISOs and reuses ISO 7816 for the data format specification.

2.5. Near Field Communication (NFC)

Near Field Communication or NFC is an emergent technology which focuses on short range wireless connectivity for mobile devices. NFC evolved from other identification and communication wireless technologies, providing the better of each one: simple and safe Peer-to-Peer transactions between electronic devices, get digital content, connect devices with a simple touch and more [3]. NFC Forum is the non-profit industry association, with over 130 members, responsible for specifying NFC and advancing its use.

Operating at 13.56 MHz, NFC may work in three different modes, supported by ISO/IEC 14443 Type A & B, ISO/IEC 18092 NFC-IP1 and ISO/IEC 15693: emulation mode (i.e. the device works as a normal contactless Smart Card), reader or writer of RFID tags or Peer-to-Peer (i.e. two NFC devices can exchange data between them at a speed of 212 kbps or 424 kbps).

A NFC enabled device has an antenna (responsible for emitting the signal), a secure element (area where secure applications such as smartcards are stored) and a NFC chip (responsible for managing communication between the device processor, the secure element and the antenna).

3. Architecture

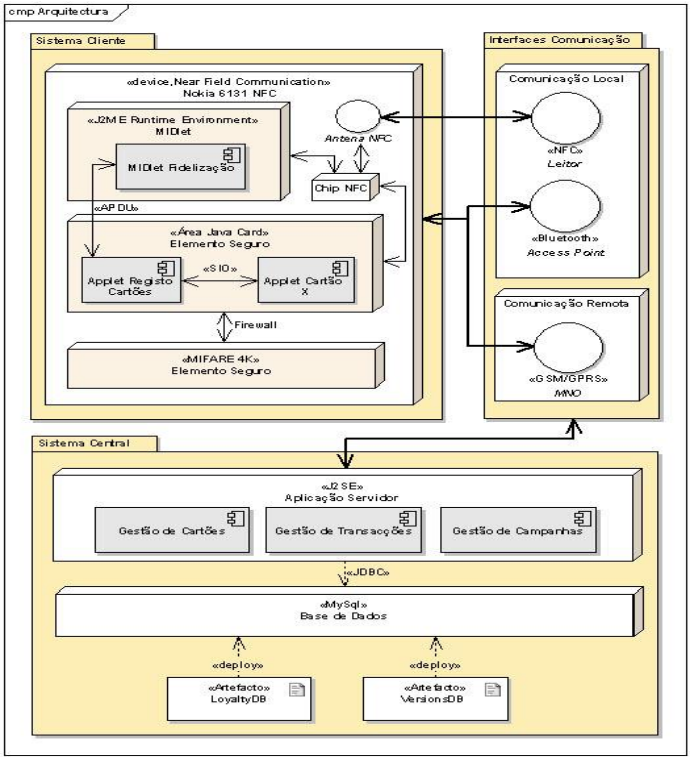

Figure 3-1 - Modular Representation of the Architecture

As stated above, the objectives for this work are to "define and specify a flexible and enclosing modular architecture". The process of designing the architecture began with an analysis of the major types of loyalty programs: points based programs, discounts and promotions bases programs and claim based programs. This analysis allowed identifying a set of main security fields and consequently defining a general data model which provides the flexibility and enclosing required by this solution.

The architecture is mainly divided into three distinct groups of components: the Client System, the Central System and the Communication Interfaces group, as shown in Figure 3-1.

3.1. Client System

The Client System is mainly responsible for the storage, management and access to the customer's loyalty programs data. This system is composed by a J2ME MIDlet and a pair of Java Card applets.

3.1.1. J2ME MIDlet

The J2ME MIDlet serves the system as an interface so the user can consult and manage data stored in the Secure Element of his mobile phone. Communication with other mobile devices (either NFC enabled mobile phones or the readers used by the loyalty companies) is also a responsibility of the J2ME MIDlet. Basically, the MIDlet reads or writes data in the Java Card component, in the Record Stores or in an external system (such as other MIDlet installed in another different mobile phone or a Central System). After being processed, that data is presented to the user through the screen of the mobile phone.

This component is modular and is divided into the Communication Layer, the Data Persistence Layer and the Presentation and Business Logic Layer.

The Communication Layer allows data to arrive or leave the MIDlet through GPRS (General Packet Radio Service), GSM (Global System for Mobile communications), Bluetooth, ISO/IEC 18092 NFC-IP1 and ISO/IEC 14443-A. The Data Persistence Layer is responsible for storing data with non-critical security requirement, such as transaction history. The third layer defines all the possible interactions of the system both internally (other components) and externally (the user, other mobile phones or readers). The Presentation and Business Logic Layer fully supports the business logic for all the non-secure data (Data Persistence Layer). On the other hand and for secure data, the logic is mostly implemented by the Java Card component.

3.1.2. Java Card Component

This component may be named the "heart" of the solution. It is in this area that all the loyalty cards are installed in order to be emulated. When speaking of several cards emulation, a question arises: How can these be managed in order to know which card is supposed to be emulated? For instance, if user has two cards from the same company, how can the system know which card to select?

The Java Card component consists of two Java Card applications (applets): the Card applet defines the structure, the objects and methods for a loyalty card, while the Card Register Management registers each instance of the loyalty cards installed. This second applet is responsible for mapping each card's AID (Application Identifier) and for manipulating the card data accordingly to the methods invoked by the MIDlet.

The Card applet stores data with critical security requirements, like, for instance, points or money budgets. The information stored in this applet can be accessed or manipulated only through the methods shared by this applet with the Card Register Management applet.

The management applet stores the data which allows obtaining the cards instance AIDs. This AIDs grant access to the Card applet instances. Besides providing access to every card installed in the Java Card area, this applet also stores data for each card. Fields such as the card number, company, card type and the card's creation and limit dates.

This architecture protects the data requiring high security: all the access to that data is made inside the JCRE (Java Card Runtime Environment). Also, the rest of the data is stored in a persistent and safe way. Reference data, such as the main password, are also stored persistently inside Card Register Management applet. This password guarantees that data is only accessed by valid users.

3.1.3. Mifare Component

The Secure Element may also have a Mifare area. This area could be used for storing the data of the cards and their registers. Besides the extra security provided by the firewall which separates it from the Java Card, Mifare could also increase interoperability, due to its backwards compatibility.

3.2. Central System

The Central System is a set of components that allow the creation of new cards, their local (compatible reader) or remote (OTA Provisioning) installation and personalization, the management of Clients data, its update and the transaction of information by APDU commands (accordingly to the Card Register Management applet specification). This information transaction can only be done locally, through ISO/IEC 14443 or ISO/IEC 18092 NFC-IP1 compliant readers. The system is divided into the Server Component and the Databases.

3.2.1. Server Component

The Server Component is nothing more than a set of applications that provide functionalities related with Customer Relationship Management (CRM), Point-of-Sale (POS) or installation balconies. Cards Management, Transactions Management and Campaigns Management are the three applications which compose the Server component.

The Cards Management application provides the following functionalities:

- Manage, create and delete customer cards;

- Locally or Remotely (OTA Provisioning) install and personalize new cards;
- Install the Loyalty MIDlet locally or remotely (wap-push).

The Transactions Management application provides the following functionalities:

- Add money to a card;
- Transactions at POS balconies (credit/debit of points or money);
- Data processing before delivering it to the Campaigns Management.

The functionalities provided by the Campaigns Management application are:

- Create, edit or remove promotional campaigns;
- Record promotional coupons in NFC tags;
- Create and edit products catalogues;
- Local or remote distribution of catalogues, promotions or coupons.

The Server Component's architecture was designed seeking to reach the most real-like possible loyalty solution, but with cards emulated by NFC enabled mobile phones.

3.2.2. Databases

For the architecture designed, and serving the Central System, two databases were installed: the Client Database (LoyaltyDB) and the Campaigns Database (VersionsDB). The Clients Database stores and relates information of every client, their cards, their contacts and each transaction of each card. The Campaigns Database stores and relates every product, the catalogues where they appear and the discounts and promotions associated to them.

4. Implementation

By implementing a solution compliant with the defined requisites, the main objectives were met. The implementation was divided in development and testing of all the components described in the architecture.

4.1. Hardware

In spite of developing a solution that could be tested, some of the used hardware had to be chosen before the implementation. Regarding the NFC technology, some variations in the hardware could become the bottleneck for a complete development of the solution. So, the Nokia 6131 NFC mobile phone and the NXP/Philips PEGODA CL RD 701 reader were the two hardware components chosen for testing the components of the system.

4.2. Java Card Applets

Due to the Java Card applets importance to the final result of the solution and to the limitations Of the Java Card subset, the applets were previously designed and detailed. This helped to achieve in a more quick and efficient way the expected result.

For each applet, the steps taken were: describe their functionalities, analyze their security aspects, implementation and design, definition of their protocols, implementation of authentication mechanisms and defining the applets' lifecycles. These steps were concluded with a few iterations of testing and corrections.

The Card applet implementation process was simpler than the Card Register Management applet, since it communicates only through Shareable Interface Objects (SIO), and has no authentication mechanism. Despite being the applet responsible for storing and modifying the most security critical data, these applets were designed in a way so that they can only be accessed through an authenticated Card Register Management applet.

4.3. Loyalty MIDlet

Before implementation, this component was also designed and specified before being implemented. The Loyalty MIDlet has two main layers: the presentation layer draws the screens with the information for display, and the communication layer which provides the methods for establishing communication with the Java Cards (APDU commands), the external readers (APDU commands) and the other NFC-IP1 capable devices (Peer-to-Peer). In order to guarantee successful Peer-to-Peer transactions, the messages exchanged were defined before the implementation of the protocol.

After completely tested, the MIDlet was then integrated with the Java Card applets and both components were submitted to integration tests.

4.4. Server Component

The implementation phase of this component began with the creation and population of the databases, accordingly with the data model defined in the architecture phase.

The next step was to design the Transactions and Cards Managers in way that future work could be done over them without the necessity to change the whole applications. Having a modular design for each Manager, the next step was to implement them.

The Transactions Management component consists of a single application which works as a POS, where all the credit or debits of points or money are dealt with. On the other hand, the Cards Management component consists of two applications: the central application and the installation counter application. The first one is mainly responsible for creating, installing and personalizing the cards. The central application allows consulting the databases and is also responsible for every remote process (i.e. OTA provisioning).

Generally, the whole three applications described above share the same layered structure: a presentation layer, a business logic layer and a communication layer for communicating not only with the databases, but also with any interface it requires (for instance, creating and sending APDU commands in the POS application).

5. Qualitative and Quantitative Evaluation

In order to validate the main functionalities of the implemented solution, integration tests were defined. The activities defined were the insertion and deletion of database records, local installation of new cards, utilization of a card (i.e. transaction) and transaction of points between two NFC mobile phones.

From a qualitative point-of-view, the integration tests had the following results:

- Insertion and deletion of database records – the requirements for this test were a normal authenticated access to the database and a successful record modification. The induced errors in the format of the records defined what validations had to be done in the Cards and Transactions Management applications;
- Local installation of new cards – the tasks for this test were to obtain the most recent version of the Card applet from the Central Application, to upload the Card applet into the phone, instantiate a card and personalize it. All tasks were always succeeded, except for the personalization that sometimes failed due to communication problems with the reader. The correct Status Word was received when trying to install the applet in a Java Card area which was out of memory;
- Utilization of a card – This test followed the detailed specification of each command provided by the Register Card Management applet. All the commands returned correctly in every supposed situations, whether they were induced errors or successful commands;
- Transaction of points between two NFC mobile phones – Accordingly to the defined flow of these transactions, this test was easily validated the Peer-to-Peer functionality.

Next to the qualitative evaluation, a quantitative one took place. The first activity was not tested in this phase, since the amount of transactions is always small, so the time would not have any variation.

The installation of a card for the first time takes 8.5 seconds. However, notice that the process of installing the Card applet happens only the first time. The future installations of new cards would not require the upload of the applets. So the activity would only take 805 milliseconds after the first time.

After successfully installing and personalizing a card, the client may then use it. Suppose that the client goes to a fuel station for gas, and decides to use the card of that gas station company, where he happens to be a loyalty customer. He can use his card to pay for the gas and have the points credited at the same time. Because the card will be used to pay something, the client has to insert his security code in the POS interface. The whole execution of these tasks takes approximately 7 seconds to complete. Being one of the most common activities, 7 seconds might seem too much. However, 5 of those 7 seconds were the time spent by the client to insert his security code. Therefore, the time directly related with the system was 2 seconds, which is a good result.

The last activity was see how much time would it take two users to enter the Loyalty MIDlet, authenticating themselves, selecting the card for the transaction, and: a) choosing the “Send Points” option, inserting the amount of points and initiating the transaction; b) initiating the receive points transaction by choosing the “Receive

Points" option. This activity took 9.3 seconds to complete, but the transaction task by itself, took only 4 seconds. Then, the time spent justifies the use of such an innovative feature in this solution.

6. Conclusions

In the first chapter, the motivation for this work was explained and contextualized into the negative aspects that come from Loyalty Programs. At the end of that chapter, the proposed solution was clearly described.

In chapter 2, the technologies which related with the existing Loyalty Programs were thoroughly analyzed. Then NFC, the emergent technology, was properly described and its advantages and innovations presented.

The third chapter describes each component of the defined architecture for supporting the proposed solution. The architecture's chapter defines each component necessary for implementing the solution.

After presenting the implementation details, the solution which resulted from implementation is then evaluated. The fact that all the main functionalities were validated and their execution times are short validates the whole solution. From the conceptualization, passing by the architecture's design and ending in the validation of the implemented solution, this work proves that NFC can indeed be positively applied to Loyalty Programs.

6.1. Future Work

The main aspect which should be taken into account is the fact that a solution like this one has to be supported by an Over-the-Air Provisioning System that enables the remote installation of applets without compromising the Secure Element. For that, there are some Trusted Service Managers providing that kind of services.

The specific solution implemented misses one layer that could also improve security. That is the Cipher layer and would be one of the main components to add to the solution

References

[1]. **Global, Aim.** Magnetic Stripe. *Card Technology: Magnetic Stripe.* [Online] [Cited: Novembro 15, 2007.] http://www.didyouknow.cd/creditcards.htm.

[2]. **Cross, Richard.** Smart cards for the intelligent shopper. *Allbusiness.com.* [Online] Direct Marketing, Abril 1, 1996. [Cited: Dezembro 10, 2007.] http://www.allbusiness.com/marketing/direct-marketing/554240-1.html.

[3]. **Cassidy, Ruth.** Call For Entries Touching the Future: NFC Forum Global Competition. *NFC Forum.* [Online] 2007. [Cited: 1 18, 2008.] http://www.nfc-forum.org/news/pr/view?item_key=ffc0422bbc6504e4915ae500e4c19629dde0e5e9.