International Journal of Smart Home
Vol. 9, No. 3 (2015), pp. 185-194
http://dx.doi.org/10.14257/ijsh.2015.9.3.17

A Common Data Storage Solution for SE-based Membership Card Applications

Jianchao Luo and Zhijie Qiu

School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, 611731, China
luojc@uestc.edu.cn, qzhijie@uestc.edu.cn

Abstract

In order to encourage customers to return, more and more retailers issue membership cards that offer certain exclusive benefits to the customers who own them. As it is not convenient for the customers to bring many plastic membership cards with them, electronic membership cards emerge. However, traditional electronic membership cards are stored in the mobile phone that usually lacks enough security protection. This paper presents a common data storage solution for SE-based membership card applications, which can enable retailers not only to deploy membership cards on secure area easily, but also to access membership cards in a fast and secure manner. Since the proposed solution provides common and simplified interfaces for managing membership card application information, the service providers will not have to know much about the complicated application management mechanism within a SE and thus the overhead of developing and deploying a SE-based membership card application is greatly reduced.

Keywords: *Electronic membership card, Secure element, Data storage, Mobile phone, Near Field Communication*

1. Introduction

Membership cards are very useful for building customer loyalty, since they provide customers with such benefits as discounts on future purchases or such privileges as notifications of sales. Customers usually apply for membership cards offered by retailers that offer products or services that they buy frequently. Because it is not convenient for the customers to bring many plastic membership cards with them, electronic membership cards emerge. However, as traditional electronic membership cards are stored in the mobile phone that usually lacks enough security protection, security of the membership card information cannot be well guaranteed.

Secure element (SE) is the place where membership card application information can be securely stored. A SE is a tamper proof micro controller that provides secure storage and execution environment for sensitive data and processing [1], which has different form factors for different market needs: plastic smart card, UICC, eSE, micro SD *etc.*, [2]. GlobalPlatform [3] offers a card specification [4] for standardization and interoperability of application management within a SE. Communication between the mobile phone operating system and the SE is done via the Application Protocol Data Unit (APDU). However, the development and deployment of a SE application are very complicated, as the developers have to learn about how to create application Supplementary Security Domain (SSD), how to install and personalize the application, how to allocate storage space on the SE for membership card data, *etc.*, Meanwhile, if

ISSN: 1975-4094 IJSH

different service providers (SP) develop different membership card applications to be deployed on the SEs, they will have to provide their own application data storage solutions. Therefore, how to simplify the development and deployment of a SE-based membership card application has become an important issue.

In this paper, a common data storage solution for SE-based membership card applications is proposed, which can enable SPs not only to deploy membership cards on secure area easily, but also to access membership cards in a fast and secure manner. During the membership card application service phase, the reader deployed at the retail store communicates with the mobile phone, which has built-in SE, based on Near Field Communication (NFC) [5, 6] technology, as NFC is compatible with the existing contactless infrastructure and enables a simple and safe two-way interaction between electronic devices. Many NFC applications have been put to use, like contactless payment [7, 8], ticketing [9], health care [10], access control [11], *etc.*, Since the proposed solution provides common and simplified APDU commands for adding, reading, updating and deleting membership card application information, as well as defines membership card data template for SPs to use directly, the SPs do not have to know much about the complicated application management mechanism within a SE any longer and thus the overhead of developing and deploying a SE-based membership card application can be greatly reduced.

2. Related Works

As electronic membership cards are very useful for retaining customers and can cut distribution costs, many electronic membership card applications have been developed and deployed on mobile phones.

Applications like CardStar [12] let users store all of their membership card information into the application, eliminating the need to carry plastic cards all the time. When the users choose a card, he can view the card's barcode that cashiers can scan. However, scanning barcode is less efficient than tapping the NFC phone to the touch point.

Borrego-Jaraba, *et al.*, [13] propose an NFC-based framework for the development of membership card applications as well as mobile coupon applications. However, the application uses NFC peer-to-peer mode to exchange data while peer-to-peer mode is still not supported by many NFC phones. More importantly, the membership card information or coupons are all stored in the mobile phone, which lacks secure and trusted operating environment.

As SE can provide secure storage space for sensitive data, some solutions like NFC Loyal [14] are proposed to store membership card data in the SE that is embedded to a mobile phone and enable secure data exchange between the NFC reader and the mobile membership card application. However, these solutions do not provide simple and common interfaces for SPs to deploy membership card applications.

In order to solve the above problems, this paper presents a common data storage solution for SE-based membership card applications, which can provide secure storage and simplify the development and deployment of membership card applications.

3. The Proposed System

The proposed system is implemented as a SE applet, which is called Membership Card Applet, and installed on the SE. The Membership Card Applet is a Java Card [15] application that runs on the SE and controls access to the membership card information stored in the SE. It receives different membership card information from different SPs through the mobile membership card application deployed on the customer's mobile phone, and stores the information of each membership card in the secure area respectively. In addition, the system can provide secure membership card information exchange service between retailers and customers.

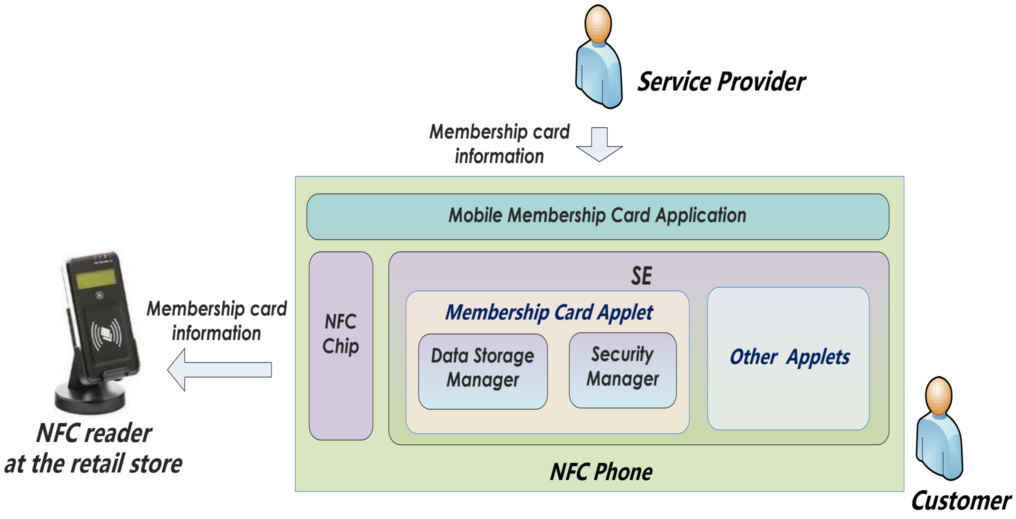

Service Provider
Membership card information
Mobile Membership Card Application
SE
Membership Card Applet
NFC Chip
Data Storage Manager
Security Manager
Other Applets
Membership card information
NFC reader at the retail store
NFC Phone
Customer

Figure 1. Architecture of the Proposed System

The proposed system mainly consists of two parts as shown in Figure 1:

- Data Storage Manager

It provides the off-card entity with the capability to access membership card information stored in the predefined storage space, which includes adding or removing a membership card and reading or updating information of a membership card. The off-card entity performs these operations by sending the provided APDU commands to the Membership Card Applet.

- Security Manager

The Security Manager provides security mechanism for membership card information access services in order to ensure that both the membership card holder and the off-card entity are trusted and the transmitted data has not been illegally tampered with. Services given by the module include membership card identity verification, APDU command data integrity verification, *etc*.

3.1 Data Storage Manager

In order to store various membership card information, a secure storage space is allocated during the proposed system's initialization phase. As the size of the storage space is limited, it can save a fixed quantity of membership cards.

The structure of the membership card storage space is depicted in Figure 2. Each data record corresponds to a membership card, which contains two parts: membership card data and key data that are used for controlling secure access to membership card data. The information of one membership card can be found if its record number is given. The size of each membership card record is fixed, however, the content of its card data can be determined by the retailers. In the meantime, the data length of the card record key is also fixed. When the proposed system is initialized, the key of each card record is assigned an initial value, which can be altered later on.

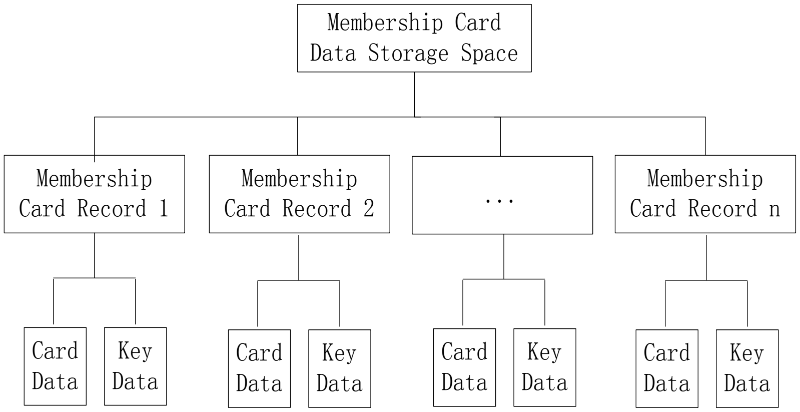


Figure 2. Structure of Membership Card Storage Space

To access the membership card storage space, the system defines a series of APDU commands for off-card entities to add, remove, read and update membership card information.

- ADD RECORD

The "ADD RECORD" command is used for adding a new membership card record to the storage space by providing card data and key data. If currently there is no empty record, the operation shall fail. As the structure of the card data can be defined by the SPs, to simplify the development of membership card applications, we provide SPs with membership card data template. The SPs can also define the data template they need by themselves. Table 1 shows the data attributes of the membership card application data template that the system provides.

Table 1. Data attributes of Membership Card Application Data Template

Data attribute	Description
CardName	Name of the membership card
SPID	Identifier of the SP that issues the membership card
CardID	Identifier of the membership card
CardHolderName	Name of the membership card holder
MembershipLevel	Level of the membership
IssueDate	Issue date of the membership card
ExpirationDate	Expiration date of the membership card

The data field of the APDU command consists of card data, key data and message authentication code (MAC) value of the command itself. Therefore, besides setting card data, setting key data of the new membership card record is needed. To ensure confidentiality of the key, the key data is encrypted by the initial key of the record before being written into the record.

- READ RECORD

The "READ RECORD" command is used for getting information of one membership card record, excluding the key data of the card record. Usually, the NFC reader needs to perform mutual entity authentication before it starts to exchange data with the SE. However, as the membership card data does not include confidential information, in order to accelerate the card reading speed and improve user experience, the system does not require identity authentication for the NFC reader but only require identity authentication for the membership card when reading a membership card record. The process of reading membership card information is shown in Figure 3.

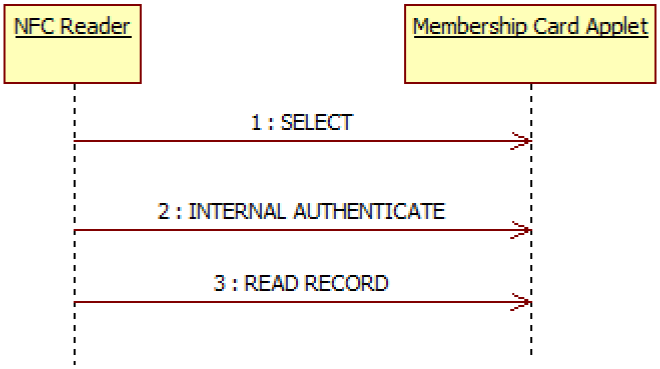


Figure 3. The Process of Reading Membership Card Information

As shown in Figure 3, the NFC reader deployed at the retail store sends the "SELECT" command for selecting the Membership Card Applet, and then sends the "INTERNAL AUTHENTICATE" command for authenticating the membership card to be accessed. After successful authentication, the NFC reader will send the "READ RECORD" command for getting the membership card information.

- UPDATE RECORD

The "UPDATE RECORD" command is used for modifying the data or the key of a membership card record. The command should carry the record number as a command parameter for locating the record. Since membership card information modification needs security control, the system will verify the MAC value of the command before it can be executed, no matter it modifies card data or key data.

- DELETE RECORD

The "DELETE RECORD" command is used for deleting a membership card record. After the deletion, the deleted record will be marked as an unoccupied one and its record key will be set to initial value. Similarly, the system will verify the MAC value of the command before it can be executed.

3.2 Security Manager

In order to ensure the security of the proposed system, the Security Manager is responsible for authenticating identities of membership cards and NFC readers.

- Membership card identity authentication

To prevent the usage of counterfeit membership cards, the retailer is enabled to verify the authenticity of the membership card every time he reads it. The authentication process is described as follow:

1. The NFC reader generates random data, puts it into the "INTERNAL AUTHENTICATE" command and sends the command to the Membership Card Applet.
2. The Membership Card Applet encrypts the received random data by using the record key and then returns the cipher text to the NFC reader.
3. The NFC reader decrypts the received cipher text and gets the plaintext. If the plaintext is the same as the random data it sends to the applet previously, identity of the membership card is authenticated.

- Off-card entity identity authentication

In order to guarantee that membership cards are accessed in a secure manner and completely isolated from each other, each membership card holds a different record key. The record key is set when its corresponding membership card is added, and is used for verifying the identity of the off-card entity when it updates or deletes a membership card record. The process of updating membership card information is depicted in Figure 4.

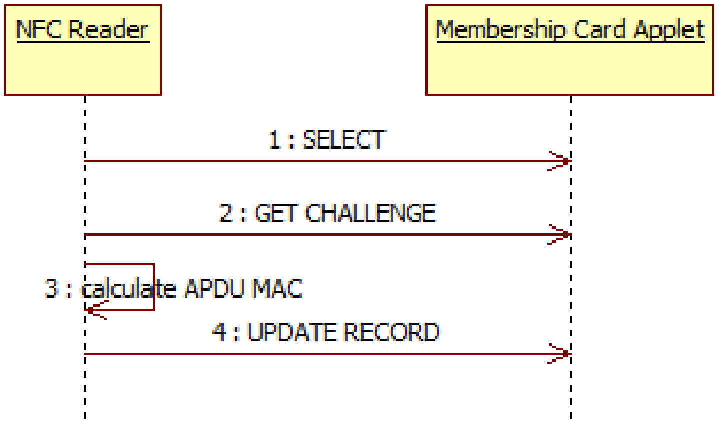


Figure 4. The Process of Updating Membership Card Information

As shown in Figure 4, the MAC value of the "UPDATE RECORD" command should be calculated before the command is sent to the applet. The MAC value is calculated by using the record key of the membership card to be updated and appended at the end of the command message. The initial vector used for the MAC calculation is the random data generated by executing the "GET CHALLENGE" command. Once receiving the command, the applet will verify the MAC value to determine whether it is sent by a valid entity or is tampered with by any unauthorized party. Only if identity of the off-card entity is authenticated, the command can be executed by the applet.

4. Sample Application

To validate the proposed solution, one membership card Android application for a restaurant is developed and its membership card information is stored in the SE of an NFC phone via the proposed system. The NFC phone for the test is a Galaxy S4 smartphone, which is equipped with a micro SD card that has built-in SE.

As the proposed system has already provided a membership card data template, we use it directly to simplify the development process. Table 2 shows the information of a new membership card of the restaurant.

Table 2. Card Information of a New Membership Card of the Restaurant

Data attribute	Data value
CardName	Capricciosa Restaurant
SPID	REST_00000001
CardID	000198
CardHolderName	John Smith
MembershipLevel	A
IssueDate	01022014
ExpirationDate	01022019

To add the membership card information to the customer's SE, the membership card Android application developed for the restaurant needs to communicate with the proposed system (*i.e.*, The Membership Card Applet, which is installed on the SE in advance) as shown in Figure 5.

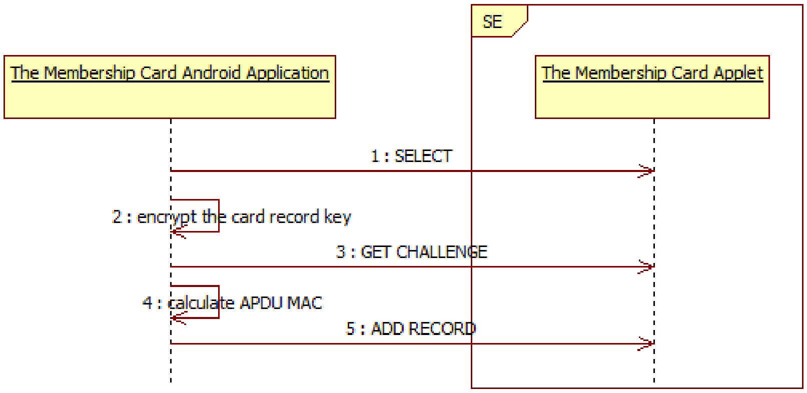

SE
The Membership Card Android Application
The Membership Card Applet
1 : SELECT
2 : encrypt the card record key
3 : GET CHALLENGE
4 : calculate APDU MAC
5 : ADD RECORD

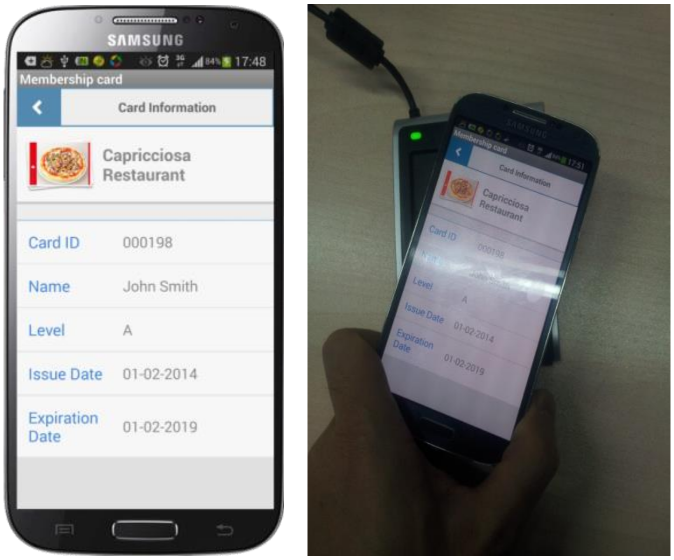
Figure 5. The Process of Adding the Membership Card information to the Customer's SE

Figure 5 shows the process of adding a new membership card to the SE:

1. The membership card Android application sends the "SELECT" APDU command for selecting the Membership Card Applet.
2. The membership card Android application encrypts the key data of the new membership card by using the initial record key of the proposed system for ensuring its confidentiality.
3. The membership card Android application sends the "GET CHALLENGE" APDU command to the Membership Card Applet for getting a newly generated 4-byte random data.
4. The membership card Android application calculates the MAC value of the "ADD RECORD" command message by using the initial record key of the proposed system and the generated 4-byte random data at step 3, and then appends it at the end of the command message.
5. The membership card Android application sends the "ADD RECORD" APDU command to the Membership Card Applet for adding a new membership card record to the storage space in the SE, which is allocated during the proposed system's initialization phase.

In this way, only three simple APDU commands are used in order to create a new membership card on the SE. And the membership card application developers do not have to learn about how to create application SSD on the SE, how to install and personalize a SE-based membership card application as well as how to allocate storage space on the SE for membership card data.

After the new membership card of the restaurant is added to the SE, its card information can be read by the membership card Android application and the NFC reader respectively as shown in Figure 6.



Card ID 000198
Name John Smith
Level A
Issue Date 01-02-2014
Expiration Date 01-02-2019

(a) (b)

Figure 6. Reading the Membership Card Information Stored in the SE (a) The Android Application Displays the Information of a Membership Card (b) The NFC Reader Reads the Membership Card Information by a Simple Souch

Through adding and reading the membership card information based on the proposed system, we can find that the proposed solution is very simple to use for SPs.

5. Conclusions

The proposed solution provides secure storage space for storing electronic membership cards. Meanwhile, it enables retailers to access membership cards in a fast and secure manner based on NFC technology. As it provides common and simplified interfaces for adding, reading, updating and deleting membership card application information, the SPs can develop and deploy SE-based membership card applications much faster than before. They will not need to know much about the complicated application management mechanism within a SE any longer and thus the overhead of developing and deploying a SE-based membership card application is greatly reduced.

Currently we are working on adding to the proposed system new features like supporting loyalty cards and electronic tickets in order to widen its application range.

References

[1] http://www.globalplatform.org/mediaguideSE.asp.

[2] M. Reveilhac and M. Pasquet, "Promising Secure Element Alternatives for NFC Technology", In Proceedings of the 1st International Workshop on Near Field Communication, **(2009)**, pp. 75-80.

[3] http://www.globalplatform.org/.

[4] http://www.globalplatform.org/specificationscard.asp.

[5] ECMA, Near Field Communication White paper. ECMA/TC32-TG19/2005/012, **(2005)**.

[6] http://nfc-forum.org/what-is-nfc/.

[7] M. Pasquet, J. Reynaud and C. Rosenberger, "Secure payment with NFC mobile phone in the SmartTouch project", In Proceedings of 2008 International Symposium on Collaborative Technologies and Systems, **(2008)**, pp. 121-126.

[8] U. B. Ceipidor, C. M. Medaglia, A. Marino, S. Sposato and A. Moroni, "KerNeeS: A protocol for mutual authentication between NFC phones and POS terminals for secure payment transactions", In Proceedings of 2012 9th International ISC Conference on Information Security and Cryptology, **(2012)**, pp. 115-120.

[9] R. Widmann, S. Grunberger, B. Stadlmann and J. Langer, "System Integration of NFC Ticketing into an Existing Public Transport Infrastructure", In Proceedings of 4th International Workshop on Near Field Communication, **(2012)**, pp. 13-18.

[10] A. J. Jara, P. López, D. Fernández, B. Úbeda, M. A. Zamora and A. F. G. Skarmeta, "Interaction of Patients with Breathing Problems through NFC in Ambient Assisted Living Environments", In Proceedings of 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, **(2012)**, pp. 892-897.

[11] A. Dmitrienko, A. R. Sadeghi, S. Tamrakar and C. Wachsmann, "SmartTokens: Delegable Access Control with NFC-Enabled Smartphones", In Proceedings of Trust and Trustworthy Computing - 5th International Conference, **(2012)**, pp. 219-238.

[12] http://www.cardstar.com/.

[13] F. Borrego-Jaraba, I. Luque Ruiz, and M. A. Gómez-Nieto, "A NFC-based pervasive solution for city touristic surfing", Personal and Ubiquitous Computing, vol. 15, **(2011)**, pp. 731-742.

[14] B. Ozdenizci, V. Coskun, and K. Ok, "NFC Loyal for Enhancing Loyalty Services Through Near Field Communication", Wireless Personal Communications, vol. 68, **(2013)**, pp. 1923-1942.

[15] http://www.oracle.com/us/technologies/java/embedded/card/overview/index.html.

Authors

Jianchao Luo, He is a Ph.D. candidate in Computer Science at University of Electronic Science and Technology of China. He has been a lecturer in School of Computer Science and Engineering, University of Electronic Science and Technology of China. His research interests include mobile computing, context-aware systems and e-commerce security.

Zhijie Qiu, He received his B.S. and M.S. degrees in Computer Science and Engineering from University of Electronic Science and Technology of China, in 2001 and 2004, respectively. He has been an associate professor in School of Computer Science and Engineering, University of Electronic Science and Technology of China. His research interests include wireless communication, e-commerce security and ubiquitous computing.