International Journal of u- and e- Service, Science and Technology
Vol.8, No.4 (2015), pp.233-246
http://dx.doi.org/10.14257/ijunesst.2015.8.4.22

A Secure NFC-based Electronic Voucher Solution

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

As the number of mobile Internet users grows rapidly, more and more service providers are distributing electronic vouchers to consumers via mobile phones, which eliminates the need to carry various plastic or paper-based vouchers. Currently, electronic vouchers are available mainly in the form of text message or QR code. However, these types of vouchers are usually stored in the mobile phone that lacks secure storage and trusted execution environment. In addition, it is not efficient enough to input voucher code manually or get voucher QR code scanned when the consumer redeems the voucher. Near Field Communication (NFC) is a short-range wireless communication technology that simplifies the way of interaction between the electronic devices and guarantees a fast and secure information exchange. In this paper, we propose an NFC-based electronic voucher solution, which provides capabilities of distributing, managing and redeeming vouchers in a secure manner. The security of the voucher is ensured by storing it in the Secure Element (SE). With the proposed system, the consumer is enabled to redeem the voucher just by touching the NFC reader at the point of sale with his/her NFC phone, which offers better user experience than traditional electronic voucher solutions.

Keywords: *Near Field Communication, Electronic Voucher, Secure Element, Mobile Phone*

1. Introduction

E-commerce has made it easier and faster for consumers to make purchases online while avoiding the hassles of going to the brick-and-mortar stores. However, in this way, the offline shopping experience is sacrificed. Meanwhile, the offline retailers wish to promote their products or services and guide consumers to their shops via the online platform. To bridge the gap between online and offline shopping, Online To Offline (O2O) commerce emerges and becomes a new opportunity for retailers to gain revenues. As a new business mode, O2O utilizes online efforts and methodologies to drive offline local sales. The key to O2O is that it finds consumers online and brings them into real-world stores [1]. The concept of O2O is best demonstrated by the success of Groupon [2] for local businesses. The consumer pays first and then receives the electronic voucher to be redeemed at the indicated shop via his/her mobile phone. Previously retailers had difficulty tracking the effect of their advertising. However, with O2O websites like Groupon, everything is quantified and tracked. The retailers can make fine-tuned changes to bring in more business.

The emergence of electronic vouchers eliminates the need to carry various plastic or paper-based vouchers. Currently, electronic vouchers are available mainly in the form of text message or QR code. The text voucher code is a character string sent to the mobile user usually via SMS. It is widely used as every mobile phone is text message capable, but its redemption process is slow, as the user has to input every

ISSN: 2005-4246 IJUNESST

character of the voucher code manually. In addition, it lacks security protection since it is usually sent in plain text. QR codes are two dimensional quick response codes that can be scanned by the camera phone equipped with a QR code reader. Although many businesses adopt this code to attract customers to the Internet for more information about their products or services, it has also been used as electronic voucher in recent years. Without customer's manual input, QR code voucher can be redeemed more quickly than text voucher. However, these types of vouchers are usually stored in the mobile phone that lacks secure storage and trusted execution environment. As a result, it is hard to prevent them from being duplicated and illegally redeemed. Moreover, it is not efficient enough to input voucher code manually or get voucher QR code scanned when the consumer redeems a voucher.

Near Field Communication (NFC) [3-4] is a short range wireless communication technology that simplifies the way of interaction between the electronic devices and guarantees a fast and secure information exchange. While RFID is capable of transmitting data beyond a few meters, as a subset of RFID, NFC limits the range of communication to within typically 4 centimeters. This is because long-range communication is not desirable in applications like mobile payment or ticketing, since malicious persons may sniff transmitted data. NFC devices may be active or passive. An NFC tag is a passive device that contains information other devices can read but does not read any information by itself. In contrast, an active NFC device, like a mobile phone, can not only collect information from NFC tags, but also exchange information with other compatible devices and even modify the information on the NFC tag. Depending on how the communication is established between NFC devices, three NFC operating modes are defined: reader/writer mode, peer-to-peer mode and card emulation mode. Reader/writer mode allows an NFC phone to write data to an NFC tag as well as read data from it. Peer-to-peer mode allows two NFC phones to exchange data like digital business cards. In card emulation mode, an NFC phone is enabled to be used as a substitute for smart card.

To ensure security, NFC often establishes a secure communication channel and encrypts transmitted data when sending sensitive information such as credit card numbers. In addition to its security, another advantage of NFC technology is its simplicity, as it enables users to quickly and easily transfer information between devices with a simple touch. Therefore, it is a good choice to provide secure and convenient electronic voucher services based on NFC technology. To redeem an NFC-based voucher, the customer does not need to line up phone camera with barcode or input the long voucher code manually. In order to secure the voucher, the secret voucher information is stored in the Secure Element (SE). A SE is a tamper-resistant platform (typically a one chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities [5]. SEs are used in multi-application environment and there are different form factors of SE: Plastic Smart Card, UICC (SIM), eSE, micro SD etc. [6]. Each form factor satisfies a different market need.

Nowadays more and more mobile phones are equipped with NFC, and many NFC applications have been developed, like mobile payment [7-8], smart tour guide [9-10], etc. In this paper, we propose an NFC-based electronic voucher solution, which provides capabilities of distributing, managing and redeeming vouchers in a secure manner. With the proposed system, the consumer can easily discover, download and manage NFC-based vouchers and is enabled to redeem the voucher just by touching the NFC reader at the point of sale with his/her NFC phone, which offers better user experience than traditional electronic voucher solutions, while the retailers will not have to issue various membership cards to consumers but can distribute electronic vouchers to the consumers' SEs in a simple but secure way.

The rest of the paper is organized as follows: Section 2 reviews the related works. Section 3 describes the requirements of the proposed system. In Section 4, we propose the system's architecture and describe its main components in detail. We conclude the paper in Section 5.

2. Related Works

As electronic vouchers always provide consumers with discounts on products or services and are so inexpensive to disseminate, they are very popular with not only consumers but also retailers. In the recent years, many mobile voucher or coupon applications have been developed.

Yan *et al.* [11] design and implement a restaurant coupon management system, which can serve as a mean for restaurant owners to publish coupons, as well as a portal for consumers to find restaurant deals via their mobile phones. Will *et al.* [12] describe a framework to exploit social network connections for targeted campaigns delivery and implement an application that allows the mobile user to browse for coupon offers based on the current location. Applications like Groupon, LetsBonus [13] also use QR code-based coupons. However, these applications do not provide an efficient way to redeem a voucher since either entering voucher code or getting voucher QR code scanned is not quick enough.

Borrego-Jaraba *et al.* [14] propose an NFC-based framework for the development of tailored marketing strategies, which is responsible for diffusion, distribution, sourcing, validation, redemption and managing of vouchers, loyalty cards and all kind of mobile coupons using NFC, as well as QR codes. Dominikus and Aigner [15] propose NFC-based coupons, so called mCoupons, which can be downloaded from a poster or a newspaper equipped with a passive NFC device to a mobile device. With this mobile device the user can then cash in the mCoupon at the cashier. However, on one hand, these applications use NFC peer-to-peer mode to exchange data, but peer-to-peer mode is still not supported by many NFC devices. On the other hand, these NFC-based vouchers or coupons are all stored in the mobile phone that lacks secure and trusted operating environment. Therefore, it is difficult for voucher applications to store sensitive data securely.

The SE is a tamper resistant smart card chip that facilitates the secure storage and transaction of payment and other sensitive credentials. As a technical organization, GlobalPlatform [16] is concerned with the management of multiple applications on the SE and has published a card specification [17] for standardization and interoperability of application management within a SE.

This paper presents a solution aimed to solve the aforementioned problems. The proposed system is NFC-based, which enables consumers to redeem the voucher just by a simple touch with their NFC phones. As the mobile phone platform is less secure than the SE, we store the sensitive voucher information in the SE and establish a secure communication channel when exchanging voucher information.

3. System Requirements

The proposed system provides O2O services based on NFC technology. The main actors involved in the system include Service Provider (SP) and consumer.

The SPs are those who promote their products or services by issuing electronic vouchers online and/or via smart posters and validate them at the point of sale. In the proposed system, the SP's requirements can be described in Figure 1.

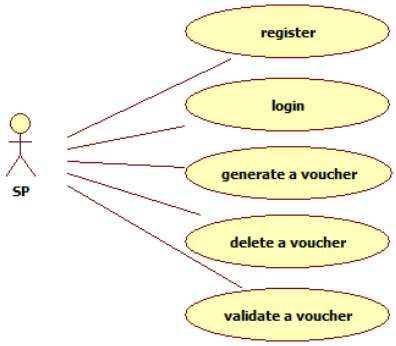


Figure 1. The SP's User Cases

Figure 1 shows the typical interaction between the SP and the system:

1. Registering for a SP ID: Before obtaining a SP ID for using the system, the SP has to send its company or personal information to the system and sign business agreement.
2. Logging into the system: The SP logins to the system using the SP ID and predefined password, before he can manage the vouchers on the system.
3. Generating a voucher: The SP fills in the basic information of the voucher, such as description of the product or service, location of the brick-and-mortar store, period of validity, etc. After the generation of the voucher, the SP can issue it online and/or via smart posters augmented with an NFC tag. For vouchers issued online, the consumer can browse and download them via his/her mobile phone. For vouchers issued via the smart poster, the SP has to download and write the voucher's URL information to the NFC tag and the consumer can acquire the voucher's URL by touching the NFC tag embedded in the poster with his/her NFC phone.
4. Deleting a voucher: The SP can delete a voucher if he does not want to promote the related product or service any longer.
5. Validating a voucher: The SP validates a voucher once the consumer requests to redeem it at the indicated store. The consumer touches the NFC reader deployed at the store with his/her NFC phone, and then the NFC reader transfers the voucher information to the system for validation and redemption.

The consumers are those who make purchase of the vouchers online and redeem them at the indicated brick-and-mortar store. In the proposed system, the consumer's requirements can be described in Figure 2.

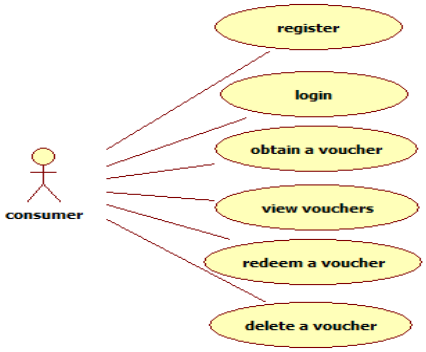


Figure 2. The Consumer's User Cases

Figure 2 shows the typical interaction between the consumer and the system:

1. Registering for a user ID: The consumer installs the Mobile eVoucher application that is the mobile client of the system and registers for a user ID. As the application needs to store vouchers into the SE, it consists of a mobile application and a SE applet.
2. Logging into the system: The consumer logins to the system using the user ID and predefined password, before he can buy and obtain the vouchers issued online.
3. Obtaining a voucher: The consumer can browse the vouchers online or get voucher's URL information by touching the smart poster distributed by the SP. He pays for a voucher online before it is downloaded to the mobile phone. The sensitive information of the voucher, i.e. the voucher code, is stored in the SE.
4. Viewing vouchers: The consumer can view the obtained vouchers directly on the mobile phone for their detail information.
5. Redeeming a voucher: The consumer requests to redeem a voucher at the indicated brick-and-mortar store by touching the NFC reader deployed by the SP with his/her NFC phone.
6. Deleting a voucher: The consumer can delete a voucher if the voucher has expired or been used.

In addition, as the vouchers contain sensitive data, security measures should be taken in order to prevent them from being counterfeited, duplicated or illegally redeemed.

4. System Architecture

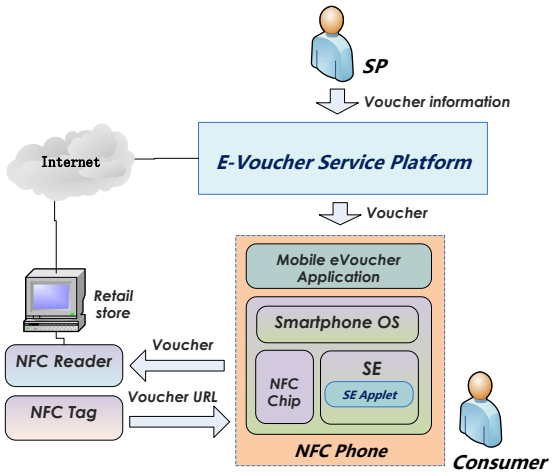


Figure 3. Architecture of the Proposed System

The proposed system is composed of two parts as shown in Figure 3:

- E-Voucher Service Platform: It is mainly responsible for managing various vouchers published by the SPs, providing vouchers for consumers to select, and validating the vouchers that the consumers request to redeem.
- Mobile eVoucher Application: It should be installed on the NFC phone beforehand and enables the consumers to purchase and download the desired vouchers by connecting to the E-Voucher Service Platform. As the mobile client of the system, it is delegated to establish secure channel sessions between the system and the SE in order to store the vouchers into

the SE. In addition, the application is in charge of sending the voucher to the E-Voucher Service Platform via the NFC reader for its redemption.

4.1 E-Voucher Service Platform

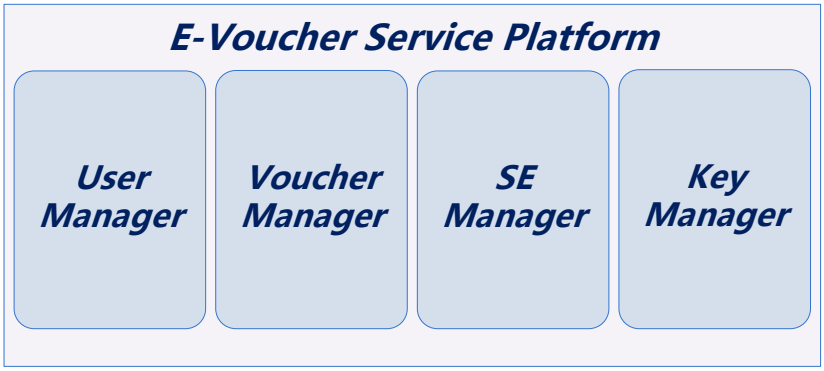


Figure 4. The Architecture of the E-Voucher Service Platform

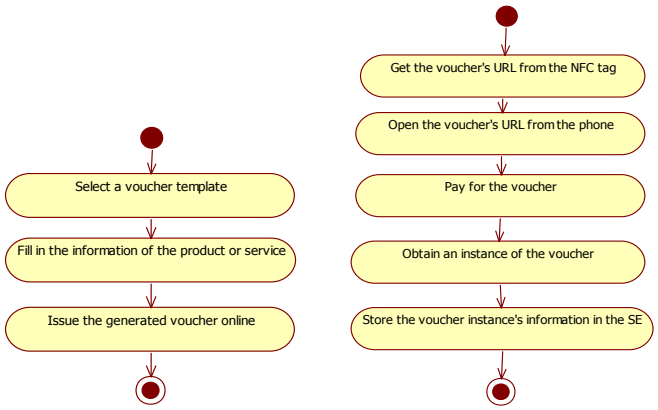
The E-Voucher Service Platform provides secure e-voucher services for SPs and consumers, which consists of four modules (See Figure 4):

- User Manager

  SPs and consumers are main users of the system. Each SP has to register for a user ID before it can issue vouchers on the system while each consumer has to register for a user ID in order to pay and download vouchers online. The User Manager provides user registration and management functionality. The user should send his basic information to the system and sign business agreement online before he can obtain a user ID to login to the system.

- Voucher Manager

  There are so many offline retailers who wish to promote their products or services online by issuing electronic vouchers. The Voucher Manager enables them to generate vouchers in an easy manner by providing general voucher templates made by the system in advance. The process of issuing a voucher is described in Figure 5 (a):



(a) (b)

Figure 5. (a) The Process of Issuing a Voucher (b) The Process of Obtaining a Voucher

If the SP wants to publish the voucher information via the smart poster augmented with an NFC tag, he can get the URL of the online issued voucher from the platform and then write it to the NFC tag. As the NFC tags are deployed in the public area, the URL is digitally signed by the system in order for the Mobile eVoucher application to verify its integrality when opening it. The consumer can touch the NFC tag and obtain a voucher online after paying for it. The Voucher Manager is in charge of instantiating the voucher that the consumer selects and requesting the SE Manager to store its sensitive information (*i.e.* voucher code) into the SE. Figure 5 (b) shows the process of obtaining a voucher. Therefore, the Voucher Manager should manage and store not only the voucher templates but also the voucher instances. When the consumer requests to redeem a voucher, the Voucher Manager will verify its validity by comparing it to the corresponding one stored in the backend system.

- SE Manager

  As shown in Figure 5 (b), the voucher instance's sensitive information should be stored into the SE. As the storing work has to be performed by the Mobile eVoucher applet, the SE manager is responsible for installing and managing it through cooperating with the Mobile eVoucher application. The Security Domain of the SE acts as the on-card representatives of off-card authorities and is mainly in charge of installing the SE applets. The Issuer Security Domain (ISD) is the primary and mandatory on-card representative of the card administrator while the Supplementary Security Domain (SSD) is the additional and optional on-card representative of the SPs [17]. To isolate the proposed system's SE applet and confidential data, the SE Manager needs to create a SSD before installing the Mobile eVoucher applet (See Figure 6).

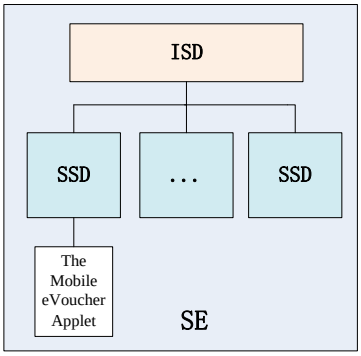


Figure 6. The SE Manager Creates a SSD for Deploying the Mobile eVoucher Applet on the SE

Before creating a SSD for the proposed system, the SE Manager needs to get the ISD keys for establishing secure communication channel with the ISD. The ISD keys include:

- Secure Channel Encryption Key: It is used for mutual authentication between the SE and the off-card entity.
- Secure Channel Message Authentication Code (MAC) Key: It is used for authenticating the integrity of the data transmitted over the secure channel.
- Data Encryption Key: It is used for encrypting the data transmitted over the secure channel.

The SE Manager sends APDU (Application Protocol Data Units) commands to the Mobile eVoucher application, which transfers them to the SE for execution. Figure 7 shows the installation and personalization process of the Mobile eVoucher applet.

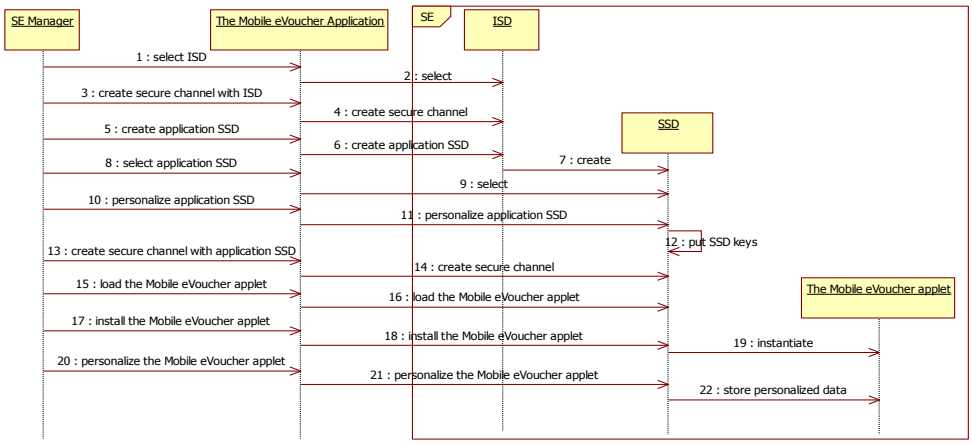


Figure 7. The Installation and Personalization Process of the Mobile eVoucher Applet

At the beginning of establishing a secure channel, the SE Manager sends the "INITIALIZE UPDATE" command to the ISD of the SE to authenticate the identity of the SE, and then it sends the "EXTERNAL AUTHENTICATION" command to enable the ISD to authenticate the identity of the off-card entity, i.e. the SE Manager. During the secure channel initiation, both the SE and the SE Manager send the challenge (random data unique to this secure channel session) encrypted by using the secure channel encryption key to the other entity, and the other entity validates the cryptogram by performing a comparison.

After the SSD is created by the ISD, it should be personalized by storing cryptographic keys (Secure Channel Encryption Key, Secure Channel MAC Key and Data Encryption Key) because the SSD can provide the applet with cryptographic services to ensure confidentiality and integrity during installation and personalization. The SE Manager puts keys into the newly created SSD by sending the "PUT KEY" command. To protect data confidentiality, the cryptographic keys to be loaded to the SSD are encrypted using the data encryption key of the ISD.

To perform applet installation operation, the SE Manager should also establish a secure channel session with the SSD, after which the Mobile eVoucher applet can be loaded by executing the "INSTALL [for load]" command and multiple "LOAD" commands. Then the SE Manager sends the "INSTALL [for install and make selectable]" command to the SSD for installing the applet.

After the installation, the applet can be selected by the off-card entity such as an NFC reader for exchanging data. To ensure secure communication, the Mobile eVoucher applet should hold secret keys for entity authentication, data integrity authentication and data confidentiality protection respectively. Therefore, the SE Manager should personalize the applet by sending the "INSTALL [for personalization]" command and consecutive "STORE DATA" commands to the SSD. The Mobile eVoucher applet's personalization data, *i.e.* the secret keys, is generated by the Key Manager of the proposed system.

During the voucher storage process, the SE Manager sends the "WRITE VOUCHER" APDU command to the SE over the established secure communication channel. The data field of the command contains the voucher's sensitive information (i.e. voucher code) to be stored into the SE. The SE Manager uses the applet's data

encryption key for encrypting the data field of the command in order to protect voucher data confidentiality, while it uses the applet's secure channel MAC key for generating the MAC value of the command to ensure the integrality of the command data. Correspondingly, during the voucher redemption process, the NFC reader, which connects to the E-Voucher Service Platform, sends the "READ VOUCHER" APDU command to the SE over the established secure communication channel for obtaining the voucher to be redeemed, and the voucher information will be returned in the response message in a secure manner. If the voucher is successfully redeemed, its status will be changed from "unused" to "used". Both the "WRITE VOUCHER" and the "READ VOUCHER" APDU command are defined by the proposed system conforming to the ISO/IEC 7816-4 specification.

- Key Manager

The Key Manager is mainly in charge of generating and storing the SSD key set as well as the Mobile eVoucher applet key set.

The SSD key set are generated using the ISD key set provided by the SE issuer (The SE contains the same ISD key set initially) and the triple DES algorithm. The input seed data is limited to 8 bytes for the computation. Both the ISD key set and the SSD key set contain three 16-byte DES keys: secure channel encryption key, secure channel MAC key and data encryption key.

The Mobile eVoucher applet key set also includes three 16-byte DES keys generated by the Key Manager. They are used for ensuring secure communication when the SE Manager stores the voucher information into the SE and when the applet exchanges voucher information with the NFC reader and the E-Voucher Service Platform during the voucher redemption phase.

4.2 Mobile eVoucher Application

Before obtaining an electronic voucher, the consumer has to download and install the Mobile eVoucher application on his/her NFC phone. As the mobile agent of the proposed system, it allows the consumers to select, download and manage various vouchers issued by different SPs in an easy and secure way, removing the need of carrying plastic or paper-based vouchers. As the SE provides secure storage and trusted execution environment, the application stores the sensitive information of the vouchers into the SE in order to prevent their being read in an unauthorized way.

The Mobile eVoucher application contains a mobile application and a SE applet. The SE applet is a Java Card [18] application that runs on the SE and controls access to the voucher data stored in the SE. The mobile application on one hand transfers the APDU commands sent by the SE Manager to the SE for installing and personalizing the SE applet as described in Figure 7, and on the other hand enables the consumers to get the voucher's URL from the smart poster, obtain the vouchers online, manage the obtained vouchers on the phone, as well as redeem the vouchers quickly and securely.

As shown in Figure 8, the typical usage scenario of the Mobile eVoucher application includes the following steps:

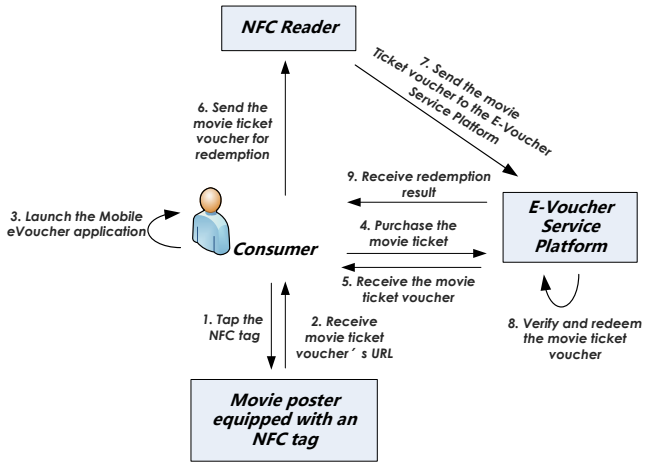


Figure 8. The Typical Usage Scenario of the Mobile eVoucher Application

1. Tapping the NFC tag: The consumer taps the NFC tag attached to the movie poster using the NFC phone (See Figure 9 (a)).
2. Receiving movie ticket voucher's URL: The movie ticket voucher's URL as well as its digital signature that are stored in the NFC tag are read by the phone.
3. Launching the Mobile eVoucher application: The Mobile eVoucher application that can process the tag information runs automatically and verifies the validity of the voucher URL's signature in order to prevent accessing illegal websites. If the URL is valid, the application will display the movie's ticket information like show times, length, pictures, etc. (See Figure 9 (b))
4. Purchasing the movie ticket: The consumer purchases the movie ticket online by using the payment service the application offers.
5. Receiving the movie ticket voucher: Upon successful payment of the ticket fee, the E-Voucher Service Platform sends the ticket voucher to the phone (See Figure 9 (c)). After that, the application transfers the voucher's sensitive data, *i.e.* voucher code, to the SE applet for secure storage through sending the "WRITE VOUCHER" APDU command over the established secure communication channel. The sensitive information of the voucher is encrypted using the the application's data encryption key and its integrity is ensured by using the application's secure channel MAC key.
6. Requesting to redeem the movie ticket voucher: When the consumer arrives at the cinema, he/she touches the NFC reader deployed by the SP with the NFC phone (See Figure 9 (d)). The reader sends the "READ VOUCHER" command to the SE over the secure communication channel, after which the SE applet returns the voucher data to the reader.
7. Transferring the movie ticket voucher to the system: The NFC reader transfers the received ticket voucher data to the E-Voucher Service Platform for redemption.
8. Redeeming the movie ticket voucher: The E-Voucher Service Platform verifies and redeems the voucher.
9. Receiving the redemption result: Upon successful redemption, the consumer can get through the entrance and the status of the ticket voucher is changed from "unused" to "used" and cannot be used any longer (See Figure 9 (e)).

The Mobile eVoucher application is an Android application that runs on the Samsung Galaxy S4 smartphone, which is an NFC phone equipped with a micro SD card that has built-in SE and NFC antenna and is compatible with GlobalPlatform

card specification. Two NFC operating modes are used in the application: reader/writer mode and card emulation mode.

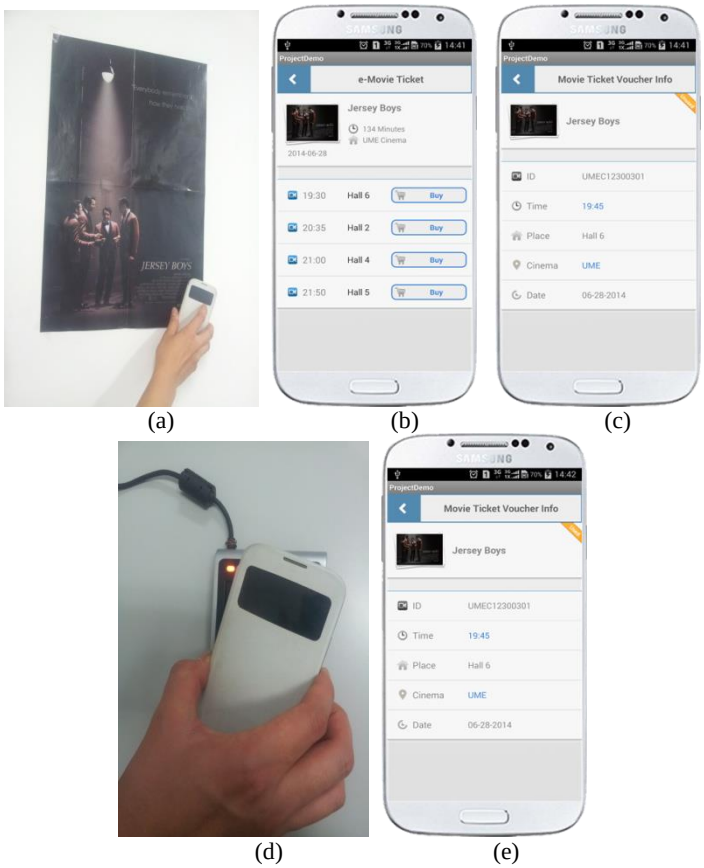


Figure 9. User Interaction in the Mobile eVoucher Application's Service Usage Phase (a) The Consumer Touches the NFC Tag Attached to the Movie Poster (b) The Consumer Views the Movie Times and buys a Movie Ticket Online (c) The Consumer Obtains a Ticket Voucher after Successful Payment (d) The Consumer Touches the NFC Reader for Voucher Redemption (e) The Ticket Voucher's Status is Changed to "Used" after Successfully Redeemed

5. Conclusions

Providing not only online promotional deals and but also offline shopping experience, O2O commerce has proved to be powerful in the local commerce world as it drives offline local sales. The consumer purchases the electronic voucher online and redeems it at the indicated brick-and-mortar store via his/her mobile phone.

Nowadays electronic vouchers are available mainly in the form of text message or QR code. However, these types of vouchers have some big disadvantages. One is the lack of efficiency because it takes much time for consumers to input voucher code manually or get voucher QR code scanned when redeeming vouchers. Another disadvantage is lack of enough secure protection since these vouchers are stored in the mobile phone that lacks secure storage and trusted execution environment.

To resolve the above problems, NFC and SE are adopted in the propose system. NFC is an emerging technology that provides a natural way of interaction between electronic devices. The information can be exchanged quickly just by a simple touch. This characteristic makes it preferable for the electronic voucher system. The

customers are thus enabled to redeem vouchers in a simple and fast manner. Meanwhile, in order to protect the security of vouchers, their sensitive information is stored in the SE as SE is a tamper resistant smart card chip that facilitates secure storage and has independent runtime environment. As the micro SDs are issued and owned by the SPs, we deploy the Mobile eVoucher applet onto the micro SD card's SE.

The proposed system not only enables the consumers to discover, download, manage and redeem NFC-based vouchers easily, but also enables the retailers to distribute electronic vouchers to the consumers' SEs in a simple way.

In addition to provide better user experience than traditional electronic voucher solutions, the proposed solution guarantees the security of management and usage of the vouchers. During the voucher storage process as well as redemption process, the communication entities are mutually authenticated in order to establish a secure communication channel for exchanging voucher information. Moreover, the sensitive information of the voucher is encrypted using the application-specific data encryption key and its integrity is ensured as well by using the specific secure channel MAC key. In this way, the electronic vouchers are distributed, managed and redeemed in a secure manner, which prevents them from being duplicated and illegally redeemed.

We think that the proposed solution can facilitate the large-scale application of NFC-based electronic vouchers. Currently we are working on adding new features like providing voucher template upload functionality and NFC tag writing tool while seeking feedback from the users to fine tune and improve the proposed solution.

Acknowledgements

The work presented in this paper was supported by the Mobile Payment Platform Research project (ID: 2013-265) of Important Science & Technology Projects of Chengdu Science and Technology Bureau.

References

[1] http://techcrunch.com/2010/08/07/why-online2offline-commerce-is-a-trillion-dollar-opportunity/.
[2] http://www.groupon.com/.
[3] ECMA, Near Field Communication White paper. ECMA/TC32-TG19/2005/012, **(2005)**.
[4] http://nfc-forum.org/what-is-nfc/.
[5] http://www.globalplatform.org/mediaguideSE.asp.
[6] http://www.smartcardalliance.org/resources/webinars/Secure_Elements_101_FINAL3_032813.pdf.
[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, pp. 121-126, **(2008)**.
[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] 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.
[10] P. Bihler, P. Imhoff, and A. B. Cremers, "SmartGuide - A smartphone museum guide with ultrasound control", Procedia Computer Science, vol. 5, **(2011)**, pp. 586-592.
[11] Q. Yan, D. Guevarra, and S. Okamoto, "Coupout - A restaurant coupon system for smart phones", In Proceedings of the 21st International Conference on Software Engineering and Data Engineering, **(2012),** pp. 173-178.
[12] M. O. Will, T. Huynh, V. Vogel, and M. Stub, "Word of mouth mobile marketing for real world recommendations", In Proceedings of 2010 14th International Conference on Intelligence in Next Generation Networks, **(2010)**.
[13] http://www.letsbonus.com/.

[14] F. Borrego-Jaraba, P. C. Garrido, G. C. García, I. L. Ruiz, and M. A. Gómez-Nieto, "A ubiquitous NFC solution for the development of tailored marketing strategies based on discount vouchers and loyalty cards", Sensors (Switzerland), vol. 13, **(2013)**, pp. 6334-6354.
[15] S. Dominikus and M. Aigner, "mCoupons: An Application for Near Field Communication (NFC)", In Proceedings of 21st International Conference on Advanced Information Networking and ApplicationsWorkshops/Symposia, **(2007),** pp. 421-428.
[16] http://www.globalplatform.org/.
[17] http://www.globalplatform.org/specificationscard.asp.
[18] 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.

