A CLOUD BASED FRAMEWORK FOR HCE ENABLED NFC SERVICES

[1]BUSRA OZDENIZCI, [2]VEDAT COSKUN, [3]SEVINC GULSECEN, [4]KEREM OK

[1,2,4]NFCLab Istanbul, ISIK University
[3]Informatics Department, Istanbul University
E-mail: busra.ozdenizci@isikun.edu.tr

Abstract- Near Field Communication (NFC) gained further appreciation with the recent advances in Internet of Things, Ubiquitous Computing, and Cloud Computing. The deficiencies of existing Secure Element (SE) alternatives for NFC services bring new Secure Element opportunities over time. Cloud based SE concept emerged especially after the introduction of Host Card Emulation (HCE) technology with Android 4.4 (KitKat) OS by Google. HCE provides new functionality for card emulation operating mode of NFC and introduces new methods for storing, accessing, and managing private data on the Cloud instead of on the Smartphones. The aim of this study is to provide a complete Cloud based framework for enabling NFC services those benefits from HCE technology. The proposed framework is described through involving actors, roles and responsibilities, and also through system components which are system registration, system management and system usage. The secure interaction between actors and the communication model of system registration and system usage components are presented as well.

Index Terms- Cloud, Framework, Host Card Emulation, Near Field Communication, Secure Element

I. INTRODUCTION

Near Field Communication (NFC) as a new promising short-range wireless communication technology is a significant contributor of several technologies such as Internet of Things (IoT), Ubiquitous Computing (Ubicomp), and Cloud Computing [1].
NFC is compatible with the existing infrastructure of RFID (Radio Frequency Identification) technology and contactless ISO/IEC 14443 contactless smart cards which occurs between two NFC compatible devices within few centimeters with 13.56 MHz operating frequency [2].

The appeal of NFC technology comes from its ease of use for triggering the functionality and seamlessly enabling a secure communication in the meanwhile. In order to engage in an NFC communication, the user needs to touch her NFC Smartphone to either an NFC tag, another NFC Smartphone, or an NFC reader.

When NFC Smartphone is touched to an NFC tag, Smartphone reads/writes data from/to an NFC tag; when touched to another NFC Smartphone, they exchange data; and when touched to an NFC reader, the reader reads the valuable and private data stored on Smartphone. An operating mode name is given to each interaction: reader/writer mode to the tag interaction, peer-to-peer mode to the Smartphone interaction, and card emulation mode to the reader interaction [1].

The most promising and exciting NFC operating mode is card emulation, which enables an NFC Smartphone to behave as a contactless smart card. Card emulation mode enables realization of diverse applications such as mobile payment, ticketing, coupon, loyalty, access control, identification and so on.

In this mode, SE is the most important part of NFC Smartphones for securing the private data and mobile application executable code. Up to now, several hardware based SEs including Universal Integrated Circuit Cards (UICC), embedded SEs, and SD based SEs are emerged for enabling –secure– card emulation services. However, several technical and business limitations have already been observed; and therefore offering further efficient SE alternatives for storing private data have become an important issue nowadays [1].
Cloud based SE concept emerged after the introduction of HCE (Host Card Emulation) technology in Android 4.4 (KitKat) OS by Google, which separates the card emulation functionality from the SE [3]. HCE technology enables storing, accessing and managing private data on the Cloud instead of on the Smartphones. The Smartphone still performs card emulation functions but the private data is stored, secured, and accessed on the Cloud.

This paper aims to present a novel Cloud based framework for enabling NFC services those benefits from HCE technology. The proposed Cloud based framework can be used for several NFC services such as access control, security, identification, and loyalty. The framework has mainly three components; system registration, system management and system usage. The security and communication issues of system registration and system management components are also described depending on Tokenization standards and specifications.

II. HOST CARD EMULATION

HCE can be referred as Software based SE, in which data is stored and managed on the Cloud; whereas

HCE functionality is located in libraries and APIs of mobile OS (Operating System), and these libraries and APIs are used by the application running on the host CPU [4]. So, the mentioned application becomes able to exchange APDU commands with an NFC reader. HCE support is currently available on the Android OS (Android KitKat 4.4 and higher) and the BlackBerry OS.

The motivation behind HCE technology is its isolated status from hardware based SE alternatives. In case of hardware based SEs, the APDU commands coming from the NFC reader are passed to the application on SE of NFC Smartphone with the help of NFC controller, so that SE handles the APDU commands in order to emulate a contactless card securely [3].
HCE technology eliminates the need for a hardware based SE; and the private data is stored on a remote server as the Cloud. There exist two methods for performing HCE services: Full Cloud based HCE solution and Tokenization based HCE solution [5].

In case of Full Cloud based HCE solution; card emulation is performed completely on the Cloud. The mobile application on NFC Smartphone authenticates the user and enables the secure connection to the remote server. NFC Smartphone aiming to obtain the credentials on the Cloud needs to connect to the remote server repeatedly for each distinct transaction. As a matter of fact, this solution requires rather fast 4G or even 5G networks, which creates a network bandwidth and security limitations [5].

On the other side, as a second option Tokenization method comes, which opens up the possibility of enabling secure and efficient offline transactions. Tokenization replaces the actual data exchange by a token, which is a disguised representation of the original value [5, 6].

For each transaction, the mobile application on the Smartphone sends token value to NFC reader, and Service Provider of the NFC reader sends token to Token Service Provider (TSP) for getting the actual credential; after which the Service Provider may authorize the transaction. The card emulation is performed by the mobile application on NFC Smartphone; there is no need for the NFC Smartphone to access to the Cloud; transactions are completely based on tokens in this solution, providing more secure communication. Threats via brute force attack to the Tokens can be prevented by several methods such as limiting the number of transactions or limiting the validity time.

Several standardization bodies have efforts to develop standards and specifications for Tokenization; ASC X9 (Accredited Standards Committee X9), PCI DSS (PaymentCard Industry Data Security Standard), Visa, and EMVCo(EuroPay, MasterCard, Visa) and so on.

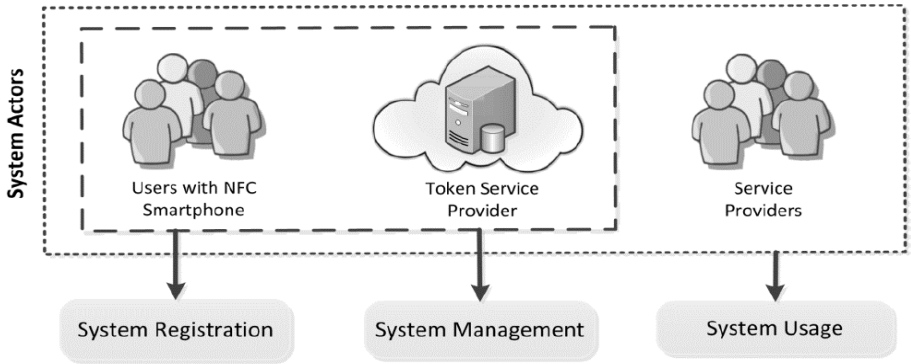

Fig.1. System Actors And Components

III. CLOUD BASED FRAMEWORK FOR NFC SERVICES

Depending on existing specifications, a promising Cloud based framework for NFC services using HCE is presented. The proposed framework enables secure NFC service on the Cloud by promoting HCE technology. Valuable data of the NFC Smartphone users are securely stored on a remote server of trusted party called Token Service Provider (TSP).

The ecosystem of proposed framework includes three major actors: NFC Smartphone users who need to own HCE enabled Smartphones; Service Provider that supplies HCE enabled NFC service(s); TSP that provides token generation, secure data service, and token mapping processes.

As the NFC Smartphone stores some data on the server of the TSP, the corresponding token is replied by the TSP which is then stored on the NFC Smartphone. For each NFC transaction, Service Provider requests authorization from TSP for the token value received from NFC Smartphone. TSP performs token mapping (i.e., de-tokenization) process, and then sends an authorization response including the original data to Service Provider in case of affirmative evaluation result.
The proposed system is examined in three components as illustrated in Fig. 1; system registration, system

management and system usage. The participating and involving actors of each component and their roles and responsibilities differentiate. System registration and system management components realize between users with NFC Smartphone and TSP; on the other hand, the system usage as primary component of the system realizes among all actors. This approach helps us to understand framework with a holistic perspective in terms of security and communication issues.

A. System Registration

System registration process is illustrated in Fig. 2 which occurs between NFC Smartphone user and TSP. The registration process is described step by step hereunder:

Step (1): First, user downloads the TSP's mobile application on her NFC Smartphone.

Step (2): User opens the mobile application and enters her personal information including name, surname, ID, birth date and phone number details.

Step (3): The mobile application on user's Smartphone creates a token value (userToken) by using a random number generation algorithm at the same time.

Step (4): The mobile application first sends only user's phone number information to TSP for verification of the user.

Step (5): TSP sends an OTP (One Time Password) to the user.

Step (6): User enters the password; and the mobile application sends user's all personal information, userToken and password to TSP.

Step (7): TSP checks and validates the phone number of user and password.

Step (8): TSP saves all user details and userToken data to its own database server; completes registration of the user.

Step (9): Finally, TSP sends an approval / verification message to user.

B. System Management

Registered users can perform rich, diverse use cases by their mobile application on their NFC Smartphones. With the proposed framework, users can store valuable data for several applications (i.e., access control and security, loyalty and couponing applications) on the remote server of TSP, as well as users can manage, control and display their valuable data on theCloud.

In terms of access control and security applications; users can display their identity information and their company details, arrange meetings in their companies; also check their past and upcoming meetings in their companies with their mobile application. In terms of loyalty and couponing applications, users can display their membership status details, check campaign details and loyalty points.

C. System Usage

The core component of this framework is system usage which focuses on the utilization of the system. The proposed framework uses two phased Tokenization for providing secure communication among all actors. For providing user identity management, NFC Smartphone stores a token value as user Token that refers to the user's identity data (i.e., ID, first name, last name, etc.). Also in our centralized system, each Service Provider may have one or more HCE enabled NFC services. Thus enabling identity management of each Service Provider's application is also important issue in our system. To distinguish and identify applications of all Service Providers in this centralized model, a token value for each application as app Token is used.

Let's concentrate on usage of the system which is illustrated in Fig. 3 as well:

Step (1): NFC Smartphone user first touches an NFC reader of Service Provider (e.g., an access or security point, loyalty POS terminal and so on). NFC reader requests identity of the user; after which userToken value on the NFC Smartphone is sent to NFC reader.

Step (2): NFC reader passes the userToken value to its backend system.

Step (3): Service Provider concatenates the corresponding application's appToken value with the userToken value coming from NFC reader, and then performs authorization request from TSP.

Step (4): TSP performs token mapping process of userToken and appToken values and obtains the private data of the user from the data server.

Step (5): TSP sends an authorization response together with the secured data to Service Provider.

Step (6): Provider transfers the authorization response to its NFC reader.

Step (7): NFC reader sends a verification and authorization message to the NFC Smartphone of user.

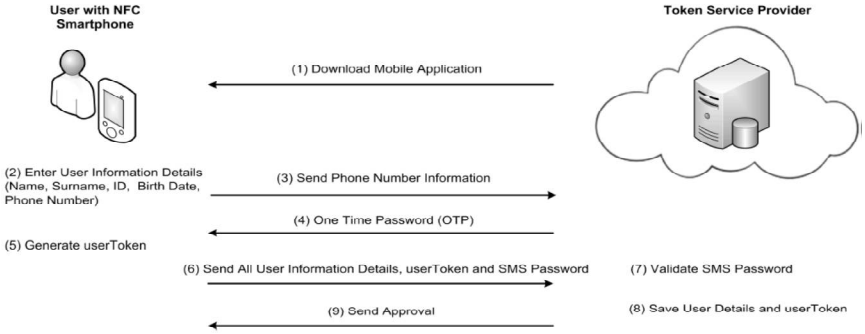

Fig.2. System Registration Communication Model

CONCLUSION

Cloud based SE for NFC services is a popular concept nowadays with the introduction of HCE technology. In this paper a novel Cloud based framework for HCE enabled NFC services is presented. This framework enables easy user registration, secure data management and data service on the Cloud for promoting HCE based NFC services; and benefits from two phased Tokenization model for providing secure communication among all system actors (i.e., user with NFC Smartphone, TSP and Service Providers). Tokenization as an important security method has important contributions for promoting HCE enabled NFC applications; loyalty and couponing, access control, identification, and security applications.

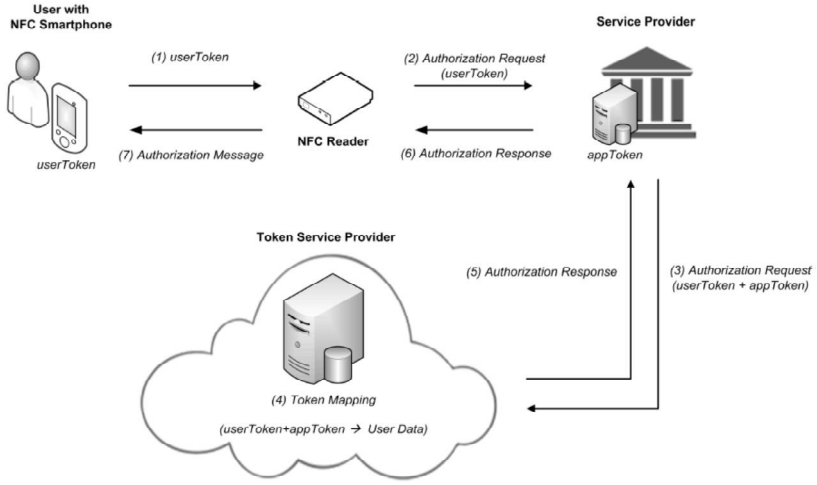

Fig.3. System Usage Communication Model

REFERENCES

[1] V. Coskun, B. Ozdenizci and K. Ok. The Survey on Near Field Communication, Sensors, 15, 2015, 13348-13405.

[2] V. Coskun, K. Ok, and B. Ozdenizci. Near Field Communication (NFC): From Theory to Practice, 1st ed.; 2012, John Wiley and Sons: London, UK.

[3] Smart Card Alliance Mobile and NFC Council, 2014. Host Card Emulation (HCE) 101, White Paper. Available Online: http://www.smartcardalliance.org/wp-content/uploads/HCE_Webinar_FINAL_061815.pdf.

[4] M. Alattar, and M. Achemlal, Host-based Card Emulation: Development, Security and Ecosystem Impact Analysis, Proceedings of the IEEE International Conference on High Performance Computing and Communications, August 20-22, 2014, Paris.

[5] Mobey Forum, 2014. The Host Card Emulation in Payments: Options for Financial Institutions, White Paper. Available Online: http://www.mobeyforum.org/whitepaper/the-host-card-emulation-in-payments-options-for-financial-institutions/.

[6] PCI DSS, 2011. Tokenization Guidelines Version 2.0. Available Online:https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf.

★★★