ISSN:2321-1156
International Journal of Innovative Research in Technology & Science (IJIRTS)

MOBILE DEVICES USING NFC IN PAYMENT APPLICATIONS

A.Allyson1, V.Jothi Lakshmi2, A.Packialatha3

Abstract

Now-a-days people do not face complications and problems of establishing a network of connections between devices and each other, leading to Near Field Communication (NFC). This can also be termed as "Tap 'n Go" because it conveys the clear picture of how it is used in different technologies. In the past few years there have been numerous successful NFC operational trials conducted on many applications globally. In this paper, we propose a method of short range radio communication which enables users to exchange data between devices and how it is effectively used in payment applications using mobile phones only using NFC.

Keyword: Near Field Communication; Security; Mobile transaction; GSM authentication

.

Introduction

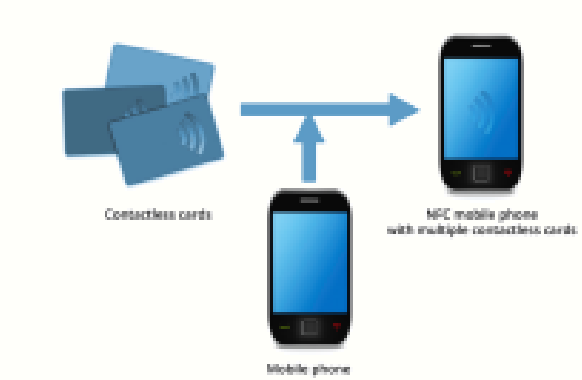
Near Field Communication (NFC) standards were first developed by the NFC forum, which was founded by a consortium of Nokia, Sony and Philips in the year 2004. It is a wireless communication standard using radio frequency waves. The devices use the 13.56MHz frequency which enables short-range data transfer and communication. NFC transfers data at speeds ranging from 106 Kbit/s to 424 Kbit/s, depending upon the protocol used. The devices should be in close proximity to one another to enable communication. The range may vary depending upon the device form, casing and the antennae size, but it is less than 10cm (usually less than 4cm). The link is established in a very short period of time, ranging from 100-150 milliseconds. With NFC technology, mobile phones can have additional functionality to act as a contactless card to be used as an easy method of payment. Successful development of NFC technology has recently started in some countries where companies offer several services based on the contactless card technology and mobile phones. We also aim to accelerate the development of NFC mobile payment services by describing the NFC ecosystem in order to raise the attention of business players in terms of the new potential models that can be implemented in order to achieve a cost beneficial and less complex ecosystem framework. We used the existing security features of GSM network to achieve authentication, data integrity and data confidentiality.

2. Survey

Pourghomi has proposed a model referred as "NFC Cloud Wallet" which deals with a complete transaction mechanism based on NFC and GSM networks [1].

Although this technology is increasingly becoming mainstream, it still has issues that need to be addressed [2]. These issues are mainly security concerns with Secure Element (SE) personalization, management, ownership and architecture that can be exploitable by attackers to delay the adaption of NFC within societies.

This newly developed intelligent device is proposed as an all-in-one personal device that can be personalized and used



in a highly interactive environment [3].

The above figure demonstrates the concept of the NFC mobile phone which is made by the combination of mobile phone and contactless IC card [4].

Universal Integrated Circuit Card is (UICC) is one of the most reliable components to act as a SE in NFC architecture [5]. It is removable, provides the same security as a smartcard, can run multiple applications issued by multiple providers, it is compliant with all smart card standards and it supports GSM and UMTS network.

According to GSMA guidelines, UICC is the most appropriate NFC Secure Element in mobile phones [3]. NFC mobile services are important emerging area for NFC technology with great potential for growth. The NFC forum analyses how to expand the excisting contactless card ecosystem to enable NFC mobile services, identifies new functionalities [4].

Issues related to the level of security that should be provided by NFC handset to store personal data and application in safe place have then arisen.Indeed, multiple secure element alternatives depending on the position of secure element in the handset can be considered and NFC stakeholders encounters difficulties to define which of them should be favored[5].

3. Proposed model

Compared to traditional payment solutions, NFC payment primarily leads to faster and easier payment at the Point of Sale (POS), e.g. at the supermarket checkout or at a ticket vending machine. At present, a customer conventionally pays either by cash or with a debit card. In the first case when paying cash, the user is required to always carry cash money with him. Then, at the POS the proper amount of invoiced money as well as the change need to be counted and scrabbled together. This leads to a cumbersome and time-consuming procedure.

Once an adequate payment terminal is available, paying with a usual debit card is certainly more efficient, but there is still an expenditure of time. The appropriate card needs to be picked out of the wallet, it needs to be inserted into the terminal with considering the correct orientation and the right PIN needs to be entered. With NFC payment a single movement of the hand is sufficient. By just waving the NFC-capable phone over the reader device, the payment is enforced. Entering a PIN however might still be necessary and advisable for security reasons.

Moreover, the NFC phone can not only replace the debit card itself, but also store personalized discount coupons and bonus cards. This additionally contributes to making a traditional wallet becoming redundant. Also, a simple person-to-person money transfer is imaginable by simply holding two phones closely together and by using the discussed NFC peer-to-peer operating mode. On the user side, the biggest barrier however for using such contactless ways of payment probably remains the psychological concern of feeling insecure when transferring sensitive data invisibly over the air without physical contact. Anyway, most of the major banks and related stakeholders have been working on trial applications and efficient architectures for NFC based mobile payment solutions. Some of the proposed models are below:

3.1 Google wallet

A first meaningful and promising concept available for the public has been developed by Google, called Google Wallet [6]–[8]. It was officially presented for the first time in May 2011 and launched in September 2011. Google Wallet is primarily built upon an application for Google's own operating system Android and is available at the Android market free of charge. Currently however, only a single NFC phone is supported, that is Google's Nexus S 4G smartphone. Also, the number of supported credit cards and the number of available payment locations is still limited at present.

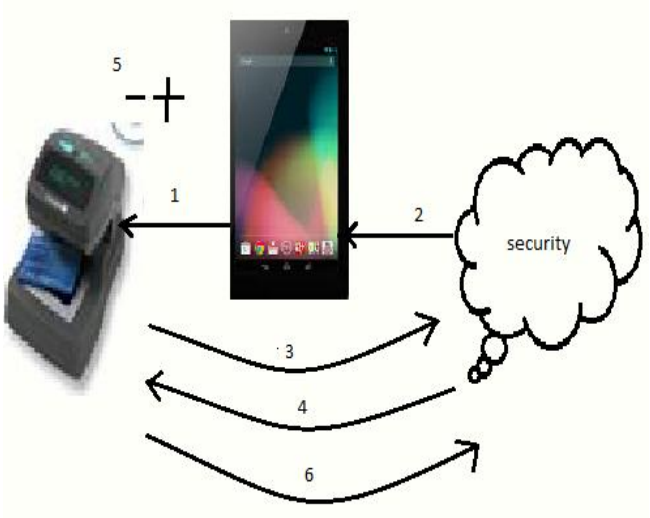
3.2 SIMpass technology

A different approach for mobile payment is conducted by a technique called SIMpass, developed and distributed by Watch data System Ltd. This solution however is currently only available and adapted for the Chinese market.

3.3 NFC Cloud Wallet Model

This model brought the idea of using cloud computing in order to manage the NFC payment applications which resulted in flexible and secure management, personalization and ownership of the applications [1]. This architecture provides easy management of multiple users and delivers personalized contents to each user. It supports intelligent profiling functions by managing customized information relevant to each user in certain environments which updates the service offers and user profiles dynamically. Depending on the MNO network's reception, deployment of this service takes around one minute and deployments can be scaled to any number of users.

The idea of this approach is that every time the customer makes a purchase the payment application which contains the customer's credentials is downloaded into the mobile device (SE) from the cloud and, after the transaction, it is deleted from the device and the cloud will update itself to keep a correct record of customer's account balance. Figure 2 illustrates the steps that should be undertaken to complete the transaction process [1].



The execution of the model is described in what follows:

1) Customer waves the NFC enabled phone on the POS terminal to make the payment

2) The payment application is downloaded into customer's mobile phone SE.

3) The reader communicates with the cloud provider to check whether the customer has enough credit or not.

4) Cloud provider transfers the required information to the reader.

5) Based on the information which was transferred to the reader, the reader either authorizes the transaction or rejects customer's request.

6) Reader communicates with the cloud to update customer's balance - if customer's request was authorized, the amount of purchase will be withdrawn from his account otherwise customer's account will remain with the same balance.

4. GSM Authentication

When a mobile device signs into a network, the Mobile Network Operator (MNO) first authenticates the device (specifically the SIM). The authentication stage verifies the identity and validity of the SIM and ensures that the subscriber has authorized access to the network. The Authentication Centre (AuC) of the MNO is responsible for authenticating each SIM that attempts to connect to the GSM core network through Mobile Switching Centre (MSC).

5. Implementation of NFC Cloud Wallet Model

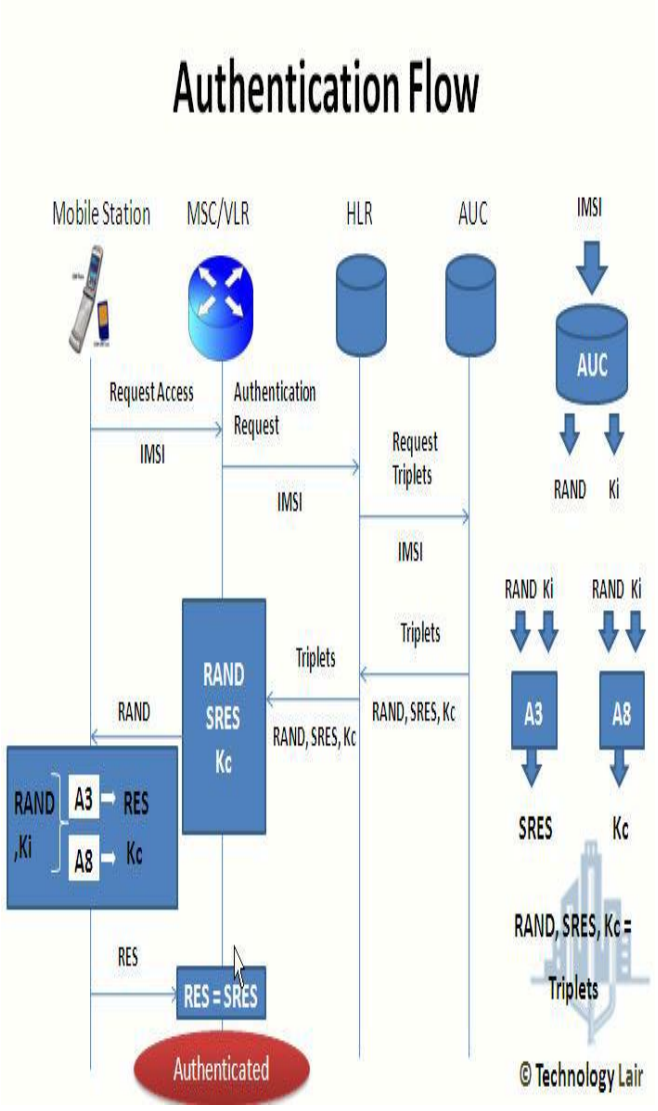
This model is based on cloud architecture where the cloud is being managed by the MNO. The cloud and the banking sector are the subsystems of MNO, in addition to the existing subsystems of an MNO. The main assumption is that the communication is secure between various subsystems of the MNO. The shop POS terminal, registered with one or more MNO, shares an MNO specific secret key with the corresponding MNO. This key is issued once a shop is registered with the MNO. The bank detail of the shopkeeper is also registered with the MNO for monetary transactions. The communication between the shop POS terminal and the mobile device is wireless using NFC technology. The mobile device has a valid SIM. The existing feature of GSM network for mutual authentication. A recent study by reference [9] proposed a mechanism for GSM authentication in NFC environment.

The proposed protocol executes in three different phases: Authentication, Keys generation and Transaction. The protocol initiates when the customer places his cell phone for the payment after agreeing to the total price displayed on the shop POS terminal. The details of these phases are described in what follows:

Phase 1: Authentication

As soon as the user places his mobile device, NFC link between the mobile device and the shop POS terminal is established. The shop POS terminal sends an ID Request message to the mobile device. The mobile device sends TMSI, LAI as its ID. The shop POS terminal sends TMSI, LAI, and Shop ID to respective MNO for customer authentication and shop identification.

In case of wrong TMSI declined message will be sent.MNO generates authentication triplets(R,S,Kc) and send to POS terminal then to mobile device through POS.SIM generates Rs and concatenates with R ,then encrypts with Kc and send it to MNO via POS.



MNO checks the validity of SIM. It decrypts Ekc(R||Rs) using Kc.MNO compares R with R in response. If both are

same transaction will be authenticated otherwise STOP message will be sent.

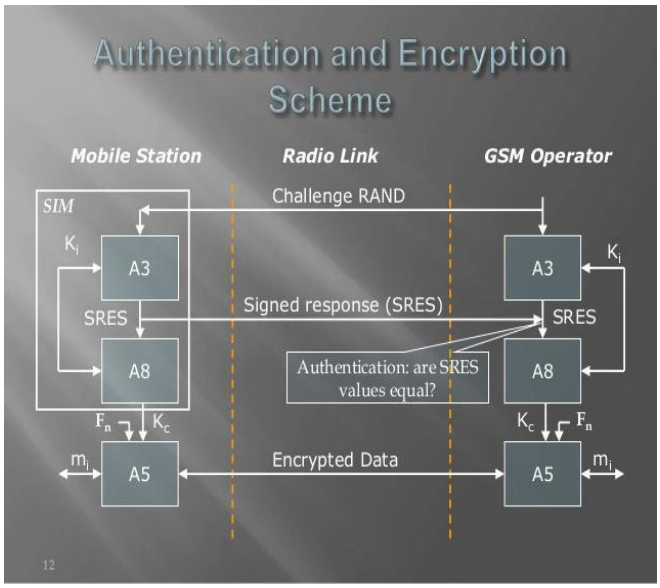
Phase 2: Key Generation and PIN Verification

Shared key is a shared secret between the MNO and the shop POS terminal. Kc is the shared secret between the MNO and the customer's mobile device. There is no shared secret between the POS terminal and the mobile device till this stage.

Using One-Way Hash function MNO and Mobile device generates KC1 from KC.It is encrypted with Kp and send to shop POS terminal. Mobile device compute Kc2 as it already has Kc1. Kc2 is the encryption key between MNO, shop POS, and customer's mobile device. Shop POS encrypts the Total Price and Receipt Number using Kc2 and sends it to Mobile device.

User's Mobile device decrypts the details and displays it to the User. If User agree with that he will type the PIN.PIN is another layer of security.PIN is stored in a secured location SIM.SIM compares both the PINS typed by User and the Shop Keeper .If both are same transaction will be authenticated. Otherwise Protocol will be stopped.

Phase 3: Transaction



The customer's cell phone generates two messages, PI and TRM, such that;

PI= Receipt No, Total Price, Time Stamp (TSU) TRM=PI, Rs, Transaction Counter By this way transaction happens in a secured manner. TSU gives the exact date and of Transaction. Tc is incremented for every transaction to prevent the replay attack.POS decrypts PI only with Kc2 to check its correctness.

After transaction is executed Transaction Information message as: TI=Transaction Serial Number, amount, TSTr. MNO encrypts TI with Kc2 and sends to POS.POS verifies the signature.If it is correct it will send the Shopping Details(SD) and the corresponding digital signature.

6. Advantages

- NFC enables connected consumer applications.
- It makes eTicketing easy.
- It enhances personal mobility.
- It gives you access to your favourite music.
- It connects you to a world of entertainment and information.
- It turns posters into smart posters.

7. Conclusion

Thus NFC demonstrates the another way of payment for all those people who do not have bank accounts. This way of making payments eases the process of purchasing for ordinary people as they only have to top up with their MNO without having to follow allthe banking procedures. This provides a secured and trusted communication to the people. Eventhough this method has some issues, it is a most welcoming technology.

8. Future work

As a part of future work, a proof of concept implementation can be carried out in order to determine the reliability of the proposed protocol in terms of number of factors such as timing issues. This implementation refers to the performance domain of the proposed protocol which can be taken into the account to consider the performance of the protocol rather than its security that is discussed in this paper. The idea of the proposed protocol can also be extended to a multi-party protocol. Furthermore, other possible architectures in this area should be explored and defined in order to finalize the most reliable architecture for cloud-based NFC payment applications.

References

[1]. P. Pourghomi, and G. Ghinea "Managing NFC payments applications through cloud computing," In 7th International Conference for Internet Technology and Secured Transactions (ICITST).IEEE, pp. 772–777, December 2012.

[2]. G. Madlmayr, J. Langer, J. Scharinger, "Managing an NFC ecosystem," In Proceedings of the 7th International Conference on Mobile Business, Washington, DC, USA: IEEE Computer Society, pp. 95–101, 2008.

[3]. P. Pourghomi, and G. Ghinea, "Challenges of managing secure elements within the NFC ecosystem," in 7th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE, pp. 720–725, December 2012.

[4]. NFC Forum" Essentials for successful NFC mobile ecosystems," 2008. www.nfcforum.org/resources/white papers/NFC Forum Mobile NFC Ecosystem White Paper.pdf

[5]. M. Reveilhac and M.Pasquet, "Promising secure element alternatives for NFC technology," In: First International Workshop on Near Field Communication, IEEE, pp. 75 – 80. 2009.

[6]. C. Gaylord, "Google wallet: Shop with a swipe of your phone," september 2011, last visited on January 19th 2012. [Online]Available:http://www.csmonitor .com/Innovation/Tech/2011/0920/Google-Wallet-Shop-with-a-swipe-of-your- phone

[7]. G. P. Ltd, "Google wallet - faq," 2011, last visited on January 19th 2012. [Online].Available:http://www.google.com/wallet/faq.html

[8]. J. Zou, C. Zhang, C. Dong, C. Fan, and Z. Wen, "Mobile payment based on rfid- sim card," in Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on, 29 2010- july 1 2010, pp. 2052 –2054.

[9]. W. Chen, G. Hancke , K. Mayes, Y. Lien, Y, J.H. Chiu, "NFC mobile transactions and authentication based on GSM network" In International Workshop on Near Field Communication, IEEE Computer Society, pp. 83–89. 2010.

Biographies

A. A.ALLYSON is currently doing her Final year B. TECH Information Technology at Jeppiaar Engineering College in Chennai, Tamil Nadu .She has presented a paper based on cloud computing in national level technical symposium and has attended many workshops.
Email - allyson.pushparagam@gmail.com

B. V.JOTHI LAKSHMI is currently doing her Final year B. TECH Information Technology at Jeppiaar Engineering College in Chennai, Tamil Nadu .She has presented a paper based on cloud computing in national level technical symposium and has attended many workshops.
Email - jothilakshmivjl30@gmail.com

C. Mrs.A.PACKIALATHA is working as an Associate Professor in the Department of Information technology at Jeppiaar Engineering College in Chennai, Tamilnadu. Her area of interest is networking technology.
Email - packiafluffy@gmail.com