Cloud-based NFC Mobile Payments

Pardis Pourghomi, Gheorghita Ghinea
School of Information Systems,
Computing and Mathematics
Brunel University
Uxbridge, UK

Abstract

Near Field Communication (NFC) is a short-range radio communication technology that enables the contactless method of data transmission for mobile phones, tablets, PDAs, laptops, PCs, etc. One of the main features of NFC technology is that it provides contactless payments. People can use their NFC enabled digital devices to pay for products and services. They are also able to use NFC applications such as loyalty and ticketing apps. Secure and cost beneficial implementation as well as adoption of NFC technology has caused a delay regarding its popularity and usability amongst people. NFC payment is mostly on trial in different countries to examine the consequences of the collaboration between involved parties and also to investigate if people accept this new method of payment. Managing different NFC applications which contains sensitive information as well as not having complete set of standards to finalize the relationships between ecosystem stakeholders has created some issues that address the ownership, card personalization, manageability and flexibility of the NFC ecosystem. In this paper, we discuss different Secure Element (SE) architectures and argue that using the Cloud technology in mobile payments will resolve some of the current issues in NFC payments.

1. Introduction

Two inductively coupled devices that are operating at 13.56 MHz can establish a communication channel based on transmission protocol and Radio Frequency (RF) interface with NFCIP1 (near field communication and transmission protocol) also stated as NFC/ISO 18092. With this technology active devices such as mobile phones and PDAs can act as a passive token or a reader which enables these active devices to access the Radio Frequency Identification (RFID) application and establish a short range peer to peer communication method [1].

As involved stake holders in NFC technology such as financial institutions and Mobile Network Operators (MNOs) were interested in placing payment and ticketing applications on NFC phones, these two applications became the key drivers for the creation of this technology. Also, the result of a research which was conducted by Visa International indicated that 89 percent of people, who tried NFC transactions, prefer phone-based transactions rather than alternative payment methods [1].

2. NFC enabled mobile handset

Although NFC payments are proven to be secure but as this technology is new to consumers, its safety and security countermeasures should be clearly described in order to educate people to improve user awareness regarding privacy issues in NFC payment systems. Some people might think what happens if they lose their phone when several methods are in place to protect user credentials. For instance, if a consumer loses his NFC phone, there is a way to block transactions from a specific PAN (Primary Account Number) by remotely disabling the information on the mobile phone. Also, consumers can protect their phone by setting up a PIN number in order to prevent unwanted users to access their phones.

In terms of usability, it is more likely that people carry their phones rather than their credit cards or their wallet with them at all times. In other words, credit cards are not as ubiquitous as mobile phones. From the variation point of view, loyalty programs and other value-added applications are supported in mobile wallet interface. NFC technology can improve card-based contactless payments infrastructure as well as current payment networks. Different applications can be integrated with main payment functionalities as NFC enabled handsets provide solid processing power that supports robust interface. An integrated SE is responsible for storing payment credentials which can be accessed through a protected application. Having said the advantages of NFC contactless payments, there are some challenges which have delayed the adaption of such technology. From the handset architecture point of view, there are several available architectures which have been designed and manufactured by different companies. However, having different architectures does not prevent the operation of NFC contactless payment but it has brought some issues in terms of

flexibility, manageability, personalization and ownership of service components. Business partnerships are yet to be improved which will probably be more complex and may cause client inconvenience. Upgrades are required for the physical Point-of-Sale (POS) terminals as most of the merchants do not accept NFC contactless payments. Thus, software upgrades might be required for the installed physical contactless POS terminals in order to accept NFC transactions.

NFC enabled devices can be used as electronic wallet; that means, with the use of payment, ticketing and other applications we can use our mobile phone to pay for day to day requirements. Eventually, this can replace debit, credit, loyalty and other countless cards that people carry every day. Primarily, NFC-enabled devices are being used in small payment circumstances, like parking meters and vending machines [2]. For example, people can check how much credit is left on their multi-use smart ticket without having to check the ticket machine every time. Thus when all NFC infrastructure and secure transaction handling are in place, NFC enabled devices can be used as a proper credit card with unlimited payment limit.

As an independent and non-profit organization which is concerned with smart card development and management, GlobalPlatform introduces a new way of managing the security of each application within the SIM. They have defined a way which guarantees the security and isolation of each application. For instance, a bank can control/be in charge of its application while the transport operator controls its own mobile ticketing application. Consequently, the MNO will have the full control of its mobile service subscription. GlobalPlatform also defines a new model that can be used to add and remove applications in the SIM at any time.

The SIM is divided into different domains and each Service Provider (SP) has been given a security domain. Each SP has full control of its own domain and no other SP can access other domains. This security model is necessary for division of responsibilities, roles and accesses especially in NFC ecosystem which contains multiple SPs. Fig.1 illustrates the GlobalPlatform SIM architecture [3].

Figure 1. Global platform SIM architecture

In this paper we consider different positions of a secure element within NFC architecture and compare them in accordance to certain criteria. We then describe the role of Cloud in NFC ecosystem as well as explaining the ways in which it can increase the manageability of NFC applications that are followed by proposing our model which focuses on the ease of managing the whole NFC ecosystem.

2. Secure Element (SE)

Secure element is a secure tamper resistant microprocessor that provides secure authentication for NFC transactions as well as secure memory for the storage of payment applications (MasterCard, Visa, etc.). SEs are also capable of supporting secure identification, payment and ticketing, and building access. The security of NFC is supposed to be provided by a component called security controller that is in the form of a SE. the SE is an attack resistant microcontroller [1] more or less like a chip that can be found in a smart card. SE provides storage within the mobile phone and it contains hardware, software, protocols and interfaces [4] [1]. SE provides a secure area for the protection of the payment assets (e.g. keys, payment application code, and payment data) and the execution of other applications [5]. In addition, SE can be used to store other applications which require security mechanisms and it can also be involved in authentication processes. To be able to handle all these, the installed operating system has to have the capability of personalizing and managing multiple applications that are provided by multiple SPs preferably Over-The-Air (OTA) [6]. However, the ownership and control of SE within NFC ecosystem may result in a commercial and strategic advantage but some solutions are already in place and researchers are developing new models to overcome this problem. We have also proposed our model in this paper.

2.1 Baseband processor

One of the most important components in a mobile phone is baseband processor that manages application operation and handles cell phone connectivity. The secure memory of baseband processor can host the SE. Also, the user does not need to insert an external memory card into his phone to use security services of SE. The major drawback of using baseband processor is when the phone gets lost. In this case, the SE must be changed as it might be used in another handset. Proprietary protocol is the underlying protocol layer between the baseband processor and the NFC controller that is not standardized yet [6].

2.2 Embedded hardware

The embedded hardware should be stored in the handset during the manufacturing stage. The SE is like a smart card inside the handset and cannot be removed. The security level of the SE is as high as the security level provided by the smartcard [7]. Personalization of SE must take place after the handset is delivered to the customer because the customer should imply the design of a new personalization process which increases the price of the handset. As the SE cannot be used in another handset, every time the user changes his handset, the embedded SE should be replaced and personalized in the new phone. The communication between the NFC controller and the embedded hardware is based on proprietary protocols and is not standardized yet. For this reason, the compliance of SE with all smart card standards (i.e. EMV, Java, etc.) does not solve the embedded SE's usability in other phones issue. Fig 2 shows the division of SE architectures based on their removability.

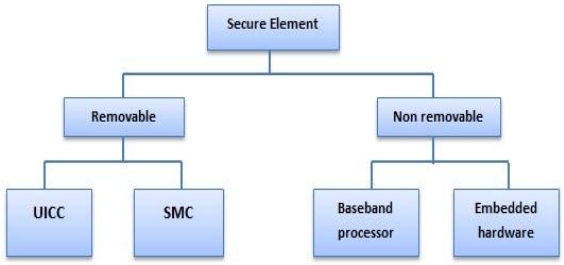

Figure 2. SE alternatives

2.3 Secure Memory Card (SMC)

A removable SMC is combination of memory (e.g. MMC, SD), smart card and smartcard controller that provides the same high level of security as a smart card. SMC is compliant will the main smartcard standards, environment and interfaces (e.g. EMV, Global Platform, ISOc 7816, Javacard, etc.) [4]. It does not have to be reissued when the user buys a new handset and it also has a large capacity memory which can host large number of applications. Although the communication between SMC and NFC controller is not standardized yet, but SMC can be inserted to any NFC enabled devices.

2.4 Universal Integrated Circuit Card (UICC)

Universal Integrated Circuit Card is (UICC) is one of the most reliable components to act as a SE in NFC architecture. 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. As UICC supports GSM, UMTS networks, it has the capability to run GSM, UMTS applications as well as other non-telecom applications such as ticketing, payment, loyalty, etc. [8]. UICC was originally made for mobile networks but since the standardization of Single Wire Protocol (SWP) was introduced by European Telecommunications Standard Institute (ETSI), the use of UICC as a SE is on track. The SWP defines the physical and data link layer between the frontend that is embedded into NFC controller and the UICC. After short period of time, ETSI introduced a new interface to complete its first standard. Host Controller Interface (HCI) is the software layer which runs a layer above the SWP. The main role of HCI is to create gates, pipes and register as well as defining commands to allow the communication of the frontend and the UICC. Table I demonstrates the evaluation of SE alternatives.

Table 1. SE alternatives evaluation

Criteria / SE Alternatives	Security	Reusability	Standardization	Total
Baseband processor	+	-	-	-
Embedded hardware	++	-	+	++
SMC	+	++	+	++++
UICC	++	+	++	+++++

2.5 Data stored in SE

This approach is a basic configuration for the operation of mobile wallet system which has been introduced few years ago. In this configuration the payment credentials are stored in SE that is installed within the NFC handset. A radio frequency antenna and an NFC chip are also installed in the handset. The payment details are securely transmitted from the NFC phone to the POS device when the user scans the NFC enabled device on the reader. In this case, the card present transaction occurs as the phone acts like a credit card. The best example for this approach can be the initial lunch of Google Wallet in 2011 where the mobile handset was dependent on the NFC and SE chips. The owner of the handset or the MNO which supports the handset is often the main driver of this configuration.

There are some positive and negative issues regarding the mobile wallet system that uses the NFC and SE chips in the handset. For example, in terms of continuity, the current payment schemes as well as existing card provisioning and security models are replicated with this approach. Because of the presence of SE, security of this solution is one of the most reliable options in the mobile wallet system.

Having multiple mobile wallet SPs are supported in this type of configuration which makes it extensible. From the stability, usability and security perspective, this solution is sufficiently proven as Google Wallet has been successfully living in the market for the past two to three years. From an ease of use point of view, an NFC handset only needs to be waved in front of the reader in order to operate. There is no need for the handset to be lined up with a reader. It is also very simple. Clients do not need to learn anything extra as all they have to do is tap and pay, just like the way a credit card payment works.

There are also some negative issues with this approach. One of the main drawbacks is the need for equipping mobile phones with the NFC and SE chip. Consequently, merchants have to install POS terminals in order to support NFC phones. Another issue is that clients might get disappointment because of not having the mobile wallet service in a particular handset as the particular MNO may not support the service of the mobile wallet provider. In terms of flexibility, only one party controls the SE which can create problems in the case of network congestion or any other technical problem within the ecosystem [9].

3. The role of cloud in NFC mobile payments

Having several parties involved in the NFC ecosystem with the lack of standards to define their roles and accesses to NFC components and applications, companies are more looking into use the Cloud environment as a single entity to make the things easier. Cloud-based payment solution can help the adaption of NFC as it only requires downloadable applications for both retailers and customers. However, it might bring more openness towards the security of customer's credentials (e.g. bank account details) but it terms of flexibility and manageability, it makes the whole process much clearer and easier to handle.

Cloud computing introduces a new method of storing payment credentials which improves the manageability of the NFC ecosystem. Rather than having all the sensitive information in NFC handset, Cloud can store this information and transmit when required. When a client scans his NFC phone on merchants POS terminal, encrypted payment credentials are taken out from a virtual SE that is stored in the Cloud and transfer to the SE that is stored in the NFC handset. The purpose of having a SE in NFC handset is to provide temporary storage in order to store authentication assets. Once payment credentials reached the NFC phone, they are again pulled out to get transmitted to the merchant's terminal in order to perform the transaction. In this scenario, the communication between merchant's terminal and NFC phone is established through an NFC link. The Cloud solution enables the client to manage transaction data by using a Cloud-based payment application that is subscribed by both client and merchant. The payment application is accessible via a mobile phone using either email or a mobile browser and the transaction report can be in the form of SMS, email or just a sound. Examples of this approach include PayPal and PayCloud Mobile Wallet [10] [11]. Although in this approach, most of the concentration has been towards vendor gift cards however, Cloud-based approach is also feasible in open payment systems.

Development of this approach can be easy for vendors as they might not need to install new POS terminals. Thus, this approach gives the opportunity to vendors in order to better differentiate and customize applications. Another advantage that this solution offers to vendors is that, in the case of operating a different payment type, the solution might be lower cost for the vendor. Also, clients are already familiar with this type of payment methods (i.e. PayPal).

As Cloud-based NFC payments might be treated as card-not-present in some cases, it is more likely that the transaction fees will be higher than the normal card payments. Furthermore, in order to execute a transaction, a connection is required to the Cloud. Executing a transaction may not be possible if this connectivity is somehow interrupted. Also, some security issues may arise from using email and SMS that can be the sign of a transaction notification. As the current payment infrastructure is not leveraged, there might be a possibility that a vendor should install a non-standard application in order to process a payment. Replacement of current POS terminals with the NFC terminals may be required as the POS have to be capable of communicating with an NFC enabled phone. The transaction execution performance depends on the network connection speed, data capacity and the way that wallet's data are accessed. And last but not least, both client and vendor have to sign up with the Cloud service provider to use its services.

3.1 Data stored in cloud

There are two main components in an NFC enabled handset: SE and NFC controller. As mentioned in section 2 of this paper, SE is responsible for providing secure storage for sensitive data while NFC controller enables short-range data transmission. Although number of NFC handsets are increasing in the market, NFC payments are not widely adopted yet. The main reason for this is the existing issues with managing and controlling

different accesses to SE. At present, operation of NFC payments requires the participation of both card issuers and SE owners that should be established through a defined relationship. In the concept of Cloud-based NFC payments, the ecosystem architecture is designed in a different way where the main SE is stored in the Cloud (virtual SE) and NFC controller stays in the handset in order to provide a limited and temporary space for authentication assets to deal with the authentication process between the NFC phone and the POS terminal. This approach is beneficial in terms of controlling the SE (card issuer access the SE easily). In this case, client credentials are stored in the virtual SE rather than being stored locally in the NFC handset. When a client scans his NFC phone on the POS reader to make a payment, transaction credentials are transmitted from the virtual SE to the NFC handset and from there to POS terminal. NFC controller is responsible for handling the authentication between NFC phone and POS. The newer version of Google Wallet which was launched in August 2012 [12] is based on this approach, however, this approach is not implemented widely yet. Google has provided a central Cloud environment where clients' payment credentials are kept. Thus, clients are able to link different credit cards with their mobile wallet service. For example Google Wallet customers can add their Visa, MasterCard, American Express and Discover cards to their Mobile Wallet service. This increases the flexibility compare to previously discussed model where data is stored in the SE that is installed in the NFC handset. Google Wallet solution also defines a proxy card in the handset to enable the transaction at the POS but customer payment credentials are still stored in the virtual SE which is in the Cloud. Storing client credentials in Cloud have some advantages and disadvantages which are discussed below.

From the portability point of view, Wallet service can be available in any device which the user is authenticated to. Also, data transmission method from NFC phone to the POS terminal can be through variety of methods such as a NFC link. Having customer credentials in the Cloud makes it easier for cardholders and financial institutions to get their card into the wallet. As SE does not exist in the phone architecture anymore, there is no third party in control of the SE which improves the security, flexibility and manageability of the service. One of the main challenges of this solution is security of data which has always been the main concern of people and technology providers. In this approach, mobile phone has a key role in data communication as it becomes a conduit for data passing from the Cloud to reach the POS. Not having proper security design on the phone may result in data leakage. On the other hand, an internet connection (WiFi or 3G/4G) is required in order to deliver data from the Cloud to the phone to be used at the POS. Connection speed has definitely a major impact on the overall service as a slow connectivity or unavailability of internet connection prevents the service operation. Therefore, properly designed solutions must be in place to ensure transaction data are available at the POS. For example, transaction data can be stored on the phone in advance of the payment [13].

3.2 Fujitsu cloud-based data transfer service project

Fujitsu is one of the companies that started the Cloud-based NFC technology by developing a platform that automatically downloads, runs and deletes different applications in a required time and place. Although this platform mainly deals with data transfer and not payment credentials but it can still be used as an initial step towards the development of Cloud-based NFC payment platforms. Demonstration of different scenarios for the above concept is illustrated in figure 3 [14].

Figure 3. Scenarios for information needed at particular times and places

Performance of the systems is based on three steps:

1) The system is combination of Cloud-based communication platform and application runtime environment
2) Application and data transmission is automatically performed from the Cloud
3) Applications are lunched and ran on a device (PC, laptop or smartphone) and are deleted when they are not required anymore

NFC technology enables devices to connect to each other therefore, required data and applications can be transferred from one device to another. For easy observation, applications can be downloaded to a device with any size and they can fit into its screen. An example of this approach is when a user enters a conference room and all the required material for that conference is transferred from the Cloud to his NFC device. All he needs to do is just to scan the NFC enabled device on the reader to receive the required data (i.e. presentation slides, conference information, etc.). An interesting part of the process

is when data is deleted once the conference ends. Also GPS technology is used to find user's location for downloading necessary data from the Cloud. This approach improves the user operational efficiency by reducing the time for setting up apps and transfer data. Fig 4 demonstrates the fit to screen process of the application that is transmitted between devices [14].

Figure 4. Information device connection technology

4. NFC cloud wallet model

There are several scenarios applicable to this approach that needs to be further explored. One scenario is when the financial institution owns a Cloud infrastructure. In this case, payment applications are mainly managed by the financial institution. On the other hand, financial institution may not own a Cloud and have a partnership with a Cloud provider instead (i.e. IBM, Microsoft, etc.). Also, the financial institution can have a partnership with a third party company that both provides Cloud infrastructure as well as dealing with financial side of the service (e.g. PayPal). It is also possible that MNO becomes a Cloud provider and have partnership with the financial institution. Or they all can stand as separate entity in the ecosystem. Generally, the idea of this approach is that when a client scans the NFC phone on vendor's POS terminal, payment credentials downloads from the Cloud's virtual SE to the phone SE (also can be NFC controller or any other form of secure temporary storage) and the phone transfers the application to the POS terminal in order to enable transaction execution. Once the transaction is carried out, the Cloud updates customer balance to keep a correct record of customer's account. Fig 5 illustrates the steps that should be undertaken to complete the transaction process.

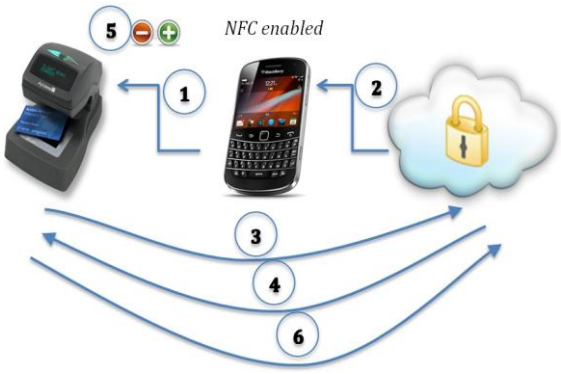

Figure 5. NFC Cloud wallet model

Below is description of the transaction execution process:

1) Customer scans his NFC enabled phone on merchant POS terminal to make a payment
2) The payment application is downloaded from the Cloud into customer's mobile phone secure temporary storage
3) POS terminal communicates with the Cloud provider to check if the customer has enough credit
4) Cloud provider transfers the required information to POS
5) Based on the information which was sent to merchant, POS terminal either authorizes the transaction or rejects customer's request
6) Merchant POS communicates with the Cloud to update customer's account – if customer request is authorized, the amount of purchase is withdrawn from customer's account, otherwise there would be no modification to his account

As an addition to this model, we suggest that when
NFC enabled phone sends a request to its Cloud provider to get permission to make a payment (step 1), Cloud provider send a SMS requesting a PIN number to identify the user of the phone. This is how Cloud provider can ensure user legitimacy. For the purpose of verification, the customer sends the PIN back to Cloud provider as an SMS.

NFC Cloud wallet model supports multi-tenant use by managing each user's information in a specific Cloud environment as well as providing simple user profiling which enables easy delivering of personalized data to each user device. Depending on MNO's network reception, service deployment does not take more than one minute for each user and deployments can be scaled to any user. The quality of mobile network certainly has an impact on the performance of the process as poor network quality may cause longer application download time. In the

case of excellent mobile network coverage, the download time/process will be less than when the network coverage is poor.

5. PayBox

A mobile network operator in Austria called A1 has recently developed a NFC mobile payment service that is not based on EMV chip and PIN technology. They named their service PayBox and have recently signed a contract with McDonald's and Merkur supermarket to test development of this service [15]. A1 is a subsidiary of Telekom Austria group which holds the full Austrian banking license. PayBox uses neither Visa PayWave nor MasterCard MasterPass and only allows maximum payment amount of €25 per transaction. Instead, with PayBox, the transaction is processed in a Cloud and rather than having a SE in the handset there is a small NFC sticker installed on the phone to deal with the authentication process. Also, a small PayBox NFC unit is used rather than POS for handling mobile payments. In order to use this service, clients should have a designated account with PayBox to deal with the financial aspects of mobile payment. As a result, every time a client uses the PayBox services, a certain amount of money is deducted from his account. Following steps describe the process of PayBox Cloud-based NFC mobile payments [15]:

1) Client's mobile phone number and account number are joined together in the back office and clients download the payment application to their mobile phones
2) There is no need for other identifying data such as clients bank account details and mobile phone numbers to be downloaded with the application
3) PayBox deducts payments few days later than the actual payment day from the designated bank account
4) The limit of daily purchase is €50 and all the transmitted data is encrypted. So the debit from the bank account can be for multiple transactions
5) Clients receive a confirmation text message for each payment they make and each payment takes half a second to process

6. NFC cloud wallet vs. PayBox

PayBox provides a new NFC unit which does not require chip and pin POS terminal where our approach suggests having a POS terminal that is capable of executing both "chip and pin" as well as NFC transaction readers to improve flexibility for both customers and merchants. With this approach, the transactions are processed in the Cloud-based platform where all the customer credentials are stored.

Depending on contract's type between service providers, customers can have several bank accounts such as MasterCard, Visa, Barclays, etc. to make a purchase where in PayBox, customers should have a bank account only with Paybox to be able to make a payment. With PayBox, customers have a profile in the Cloud containing their user identification number as well as their mobile phone number that are coupled together and also customers are able to download the payment application to their mobile phone which does not contain the mobile phone number as well as the bank account details.

The application only contains customer identity number which is downloaded from the Cloud. After scanning the NFC phone on the POS reader, POS communicates with the Cloud provider to obtain customer's identity number in order to verify customer's details before withdrawing money from customer's account. Another major difference is that PayBox uses a sticker that contains a tag on the mobile phone (like ordinary library books) where our approach focuses on SE, NFC microcontroller or any other form of secure temporary storage that deals with authentication processes only and does not keep sensitive information for a long period of time. Having a SE on a mobile phone is definitely more practical than having a sticker on a mobile phone. Thus, the payment application is deleted from SE after the Cloud is updated. There are also some similarities between both approaches:

- Multiple payments can be deducted from the bank account and few days later and in one stage
- Transmitted data are encrypted
- The required time for transaction process is half a second and a confirmation text message is sent to the client

Table 2 compares both approaches:

TABLE 2. Comparison of two approaches

NFC Cloud Wallet	PayBox
Works with NFC enabled chip and PIN POS	No capability of working with chip and PIN devices
Suggests working with popular financial institutions such as MasterCard and Visa	Transaction processes are directed towards PayBox bank which has less global popularity
Authentication is processed by a secure chip such as NFC microcontroller, etc. in a handset	Contactless sticker is easy to access for malicious purposes
Payment application is deleted from the NFC handset once the Cloud is updated – more secure and saves memory	Payment application lifecycle is not described

7. Conclusion

As the standardization of NFC technology shows, many different parties are involved in such a process. This kind of distributed standardization causes a significant overhead for dividing up tasks and the definition of interfaces. Additionally, the participation of groups with different interests make the process of standardization tough, as it moves back and forward without a common agreement. But on the other hand many different views and opinions are considered during the standardization.

The present problem during the standardization of NFC payments is that some stakeholders may not disclose their intention in the beginning. Thus a top - down standardization with a holistic overview is not possible. With regard to NFC, the major challenges in standardization are the synchronization with other consortia as well as different views of NFC-Forum members. The standardization of NFC goes hand-in-hand in with the applications and services. Therefore, many different institutions with different core-competences are involved. The major problem is that there is no central institution coordinating the standardization approaches. It may happen that not the best technical solution is chosen, but the one of the player with the most power.

Contactless technology for the Internet of Things requires all parties to agree one common definition and implementation. Having different implementation of one technology blocks interoperability, confuses users and raises the market entry barrier for companies.

8. References

[1] Mayes, K.E. & Markantonakis, K. 2008, Smart cards, tokens, security and applications, Springer-Verlag New York Inc.

[2] Innovation Research and Technology (No Date) "NFC in real world: Turning the NFC promise into profitable, everyday applications" available at: http://innovation-group.com (Access Date: May 27, 2011)

[3] Gemalto (2011) "What is GlobalPlatform?" available at: http://gemalto.com/nfc/global_platform.html (Access Date: May 30, 2011)

[4] B. Choudhary and J. Risikko, Mobile Financial Services Business Ecosystem Scenarios & Consequences, Mobey Forum, c/o Nordea Bank,Satamaradankatu 3 B, 3rd floor, 00020 Nordea, Helsinki/Finland, April 2006.

[5] G. Association, "Mobile nfc technical guidelines," GSM Association, 1st Floor, Mid City Place, 71 High Holborn, London WC1V 6EA, United Kingdom, Tech. Rep., Nov 2007.

[6] Reveilhac, M. & Pasquet, M. 2009, "Promising Secure Element Alternatives for NFC Technology", Near Field Communication, 2009. NFC '09. First International Workshop on, pp. 75.

[7] EMVCo, "Emv mobile contactless payment technical issues and position paper," EMVCo, Tech. Rep., 2007.

[8] J. Guaus, P. K. Liisa Kanniainen, P. Laaksonen, K. Murphy, J. Remes, N. Taylor, and O. Welin, Best Practice for Mobile Financial Services, Mobey Forum.

[9] FirstData (2013) "Perspective: Pros and Cons of NFC Based Wallets with an Onboard Secure Element" available at http://www.firstdata.com/en_us/insights/Perspectives_Pros_Cons_NFC.html (Access Date: February 10, 2013)

[10] WebProNews/Technology (2013) "PayPal Digital Wallet Unveiled At SXSW" available at: http://www.webpronews.com/paypal-digital-wallet-unveiled-at-sxsw-heres-20-minutes-of-demo-2012-03 (Access Date: March 21, 2013)

[11] *Paycloud* (2013) Avaiable at: https://paycloud.com/ (Access Date: March 21, 2013)

[12] NFC World (2012) "Google Wallet 2.0: The easy way to pay with NFC?" available at: http://www.nfcworld.com/2012/08/01/317105/google-wallet-2-0-the-easy-way-to-pay-with-nfc/ (Access Date: August 20, 2012)

[13] FirstData (2013) “Perspective: Pros and Cons of NFC-Based Wallet Storing Credentials in the Cloud” available at: http://www.firstdata.com/en_us/insights/Perspectives-mWallet-in-the-Cloud.html (Access Date: February 10, 2013)

[14] NFC World (2012) “Fujitsu puts NFC into cloud-based data transfer service” av0ailable at: http://www.nfcworld.com/2011/07/22/38759/fujitsu-puts-nfc-into-cloud-based-data-transfer-service/ (Access Date: September 3, 2011)

[15] NFC World (2012a) “McDonald’s to test cloud-based NFC payments in Austria” available at: http://www.nfcworld.com/2012/04/24/315260/mcdonalds-to-test-cloud-based-nfc-payments-in-austria/ (Access Date: April 25, 2012)

