Trusted Integration of Cloud-based NFC Transaction Players

Pardis Pourghomi
School of Information System, Computing and Mathematics
Brunel University
London, UK
pardis.pourghomi@brunel.ac.uk

Muhammad Qasim Saeed
Information Security Group (ISG)
Royal Holloway University of London
Egham, UK
muhammad.saeed.2010@live.rhul.ac.uk

Gheorghita Ghinea
School of Information System, Computing and Mathematics
Brunel University
London, UK
george.ghinea@brunel.ac.uk

***Abstract*— Near Field Communication (NFC) is a short range wireless technology that provides contactless transmission of data between devices. With an NFC enabled device, users can exchange information from one device to another, make payments and use their NFC enabled device as their identity. As the main payment ecosystem players such as service providers and secure element issuers have crucial roles in a multi-application mobile environment similar to NFC, managing such an environment has become very challenging. One of the technologies that can be used to ensure secure NFC transaction is cloud computing which offers wide range of advantages compare to the use of a Secure Element (SE) as a single entity in an NFC enabled phone. This approach provides a comprehensive leadership of the cloud provider towards managing and controlling customer's information where it allows the SE which is stored within an NFC phone to deal with authentication mechanisms rather than storing and managing sensitive transaction information. This paper discusses the NFC cloud Wallet model which has been proposed by us previously [1] and introduces a different insight that defines a new integrated framework based on a trusted relationship between the vendor and the Mobile Network Operator (MNO). We then carry out an analysis of such a relationship to investigate different possibilities that arise from this approach.**

Keywords- Near Field Communication; Security; Mobile transaction; GSM authentication.

I. INTRODUCTION

A Secure Element (SE) as a single entity that acts as a controlling party is unable to carry out remote operations within the NFC ecosystem. In other words, current card issuance models cannot support dynamic post issuance personalization process [2]. The remote operations include installation and loading of new applications in an external party, creation of security domains for an external party, activation and personalization of the applications that are loaded on the SE for an external party [3]; And this is because service providers:

- Can only decide whether to use their applications or not and also have no control over the SE
- Cannot control other applications that are stored on the same SE
- May not have the permission to contact the SE or have the opportunity to get to know their customer personally

At present, many restrictions and unknown constraints have created problems for the operations of Service Providers (SPs) and Secure Element Issuers (SEIs) in the mobile NFC world. Those restrictions have presented a new approach for business cooperation in which collaboration is essential between unknown parties, and none of the parties are able to influence the service environment substantially. Therefore, a technical solution and a clear framework are required in order to define constant procedures for ecosystem players. These constant procedures improve the interaction of business partners while it makes the negotiation and description of each interaction unnecessary. It also provides easy management and deployment of applications for unknown business partners. The Near Field Communication (NFC) ecosystem will not succeed without having such an approach which results in unacceptable business framework that does not provide satisfactory services for clients. Technical standards and fundamental interoperability at the basics are essential to be achieved for industries working with NFC technology in order to establish a positive cooperation in the service environment.

Interoperability is also missing in the complex application level of the service environment which has resulted in the slow adoption of NFC technology within societies. Current service applications do not provide a unique solution for the ecosystem therefore the service environment does not meet the right conditions [3]. The current situation is that, many independent business players are making decisions based on their own benefits which may not be acceptable by other business players.

A. Our Contribution

Our goal is to provide a concept for an NFC ecosystem that is technically feasible, is accepted by all involved parties and thus provides a business case for each player in the ecosystem. The purpose of this paper is to introduce a new cloud-based NFC framework that is an extension to our previously proposed NFC cloud wallet model (section IV) [1]. We then describe the transaction process which is based on the trusted relationship between the vendor and the Mobile Network Operator (MNO) and discuss a new scenario which can improve the trust in the mobile payment ecosystem. Furthermore, a general analysis of the scenario is carried out to investigate the potential limitations of this approach.

The rest of this paper is structured as follows. Section II gives a comprehensive overview of the SE lifecycle within NFC ecosystem. Section III discusses the role of cloud in NFC transactions and determines the benefits of cloud-based NFC transaction approach. Section IV evaluates the previously proposed NFC cloud wallet model. Section V proposes a new approach to NFC cloud wallet model based on the trusted relationship between vendor and MNO. Section VI describes several scenarios based on our assumptions in order to analyse the new approach. The security analysis is then carried out to investigate the possibilities of weaknesses within our approach. Finally, Section VII presents the conclusion.

II. II. SECURE ELEMENT (SE)

Security of NFC technology is provided by a component called security controller. This component is in the form of an SE which is a tamper-resistant secure memory location, for example a smart card. SE acts as a platform within a mobile device or a cloud environment which specify a multi-application architecture and it consists of hardware, software, protocols and interfaces [4][5]. Regardless of SE's location (either in a mobile device or a cloud environment), in the context of NFC transactions, it provides protection storage for transaction assets such as keys, transaction application code and transaction data. According to [6], Universal Integrated Circuit Card (UICC) is the most flexible and reliable components to act as an SE within the NFC architecture. UICC is capable of running multiple applications which can be issued by multiple application issuers while it provides the same security as a smartcard. Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS) networks are supported by UICC and it is compliant with all smartcard standards. The rest of this section describes the lifecycle of an SE which stands as a single and secure entity for storing client's credentials as well as dealing with authentication mechanisms with the vendor's Point-Of-Sale (POS) terminal. More specifically, details of SE management are described in [6]. In section III of this paper, we discuss the ways in which cloud computing changes the use of SE in NFC transactions by using the UICC as an authentication component. In this case, the cloud provides the main SE (virtual SE) which stores the client's confidential transaction information and mobile phone's SE which is in the form of UICC, is only used for authentication with the vendor's terminal.

A. Lifecycle

The processes for application issuance and the way smartcards used to be managed by service providers are changed since the introduction of SEs. This is because the service providers are not forced to initialize and personalize smartcards before issuing it for NFC handsets. The rest of this section describes the lifecycle of an SE (without the cloud's involvement) within an NFC phone [7].

The **Initialization** of an SE can be completed by different SEIs such as credit card companies, MNO, financial institution or retailers. The SEI can also act as a platform provider. If the SE does not contain any applications when issued; that means there is no platform manager assigned to that SE. A platform manager cannot deal with the SE's applications without having different certifications (i.e. Visa PayWave certification). These certifications are provided by the service provider. In most cases, the assignment of platform managers is dependent on the installation of the first application. Any party that installs the first application on the SE will be assigned as a first platform manager. However, the SE can also be managed by other application issuers. The SE can be issued by pre-installed applications that can be provided by the service provider which means the SE is already under the control of the service provider as its platform manager.

The **Activation** process takes place when the SE is inserted into the phone. The SE then signs in to the NFC controller and NFC controller sends a confirmation message to the platform manager in order to inform the platform manager of the successful insertion of the SE in the phone. The platform manager then sends a confirmation message to the mobile phone in order to activate the SE. The platform manager is the only party that has the authority to hold SE keys for data configuration purposes. NFC controller identifier is also stored in the SE to inform the SE in case if it was inserted into another phone.

During phase 1 of the **Applications Upload** process, the service provider (in this case also the application issuer) contacts the MNO which is the only party responsible for the Mobile Station International ISDN Number (MSISDN). The only way to classify the external party for an Over-The-Air (OTA) transaction with the NFC phone is the MSISDN.

In phase 2, MNO forwards the service provider's request to the platform manager(s) which is in charge of the SE. If there is no SE in the phone, the MNO informs the service provider regarding this issue. In this case, application upload process terminates. But if the platform manager is positive with the request, it will send an offer directly to the service provider to upload its application. In the next phase, service provider selects one platform manager amongst others (if more than one platform manager exist) to load its data to the security domain area which is under the control of the same platform manager. The application data passes through a secure channel to reach the security domain for application personalization. If the handset is logged in to the network, the service provider has no problems in terms of alteration and deletion of data stored in the security domain. Having security domains ensures the privacy of each security domain in a way that different service providers will only have access to their own area within a specific security domain.

The **Deactivation** procedures are also managed by the platform manager where it can deactivate the SE (OTA in the case of theft or loss). If SE is installed in a new device, then the activation process should be renewed and the platform manager is the only party that should confirm the activation process to enable the SE to be used for contactless transactions.

The above description is dependent on the multi-host interface implementation that is not standardized yet. Accordingly, a control instance is required in order to control the SEs within the handset. Currently, there is only one control instance for the whole phone and not individual control instances for individual SEs. The control instance is responsible for establishing a direct communication between the NFC controller and the Subscriber Identity Module (SIM) through the Single Wire Protocol (SWP) [8]. It also deals with the communication between the NFC phone and the MNO and routes the communication. While an SE only act as a tamper-resistant data container, this communication channel is required to establish data channels and also to send short messages.

III. CLOUD-BASED NFC SOLUTION

Although using SE as a main secure component in an NFC mobile phone was a good start for the development of this technology, however once it got to the real stage of its global implementation, the ecosystem players faced many problems. We believe that bringing the cloud infrastructure into the NFC business will help to overcome many of the current problems. A cloud-based approach [9][10] offers several advantages over the use of an SE as a single secure component in terms of storing and managing sensitive data for an NFC transaction. However, according to the speed of the present generation mobile data services [11][12], it seems an NFC cloud-based approach needs another two to three years to become commercially feasible.

The NFC cloud-based approach introduces a new method of storing, managing and accessing sensitive transaction data by storing data in the cloud (virtual SE) rather than the mobile phone. When a transaction is carried out, the required data is pulled out from a remote virtual SE which is stored within the cloud environment and pushed into the mobile phone's SE in an encrypted format. The mobile phone's SE provides temporary storage and authentication assets for the transaction to take place. After reaching the SE in an NFC phone, data are again pulled out from the handset and reach vendor's terminal. In general, the communication between the cloud provider and the vendor terminal is established through the NFC phone. Fig. 1 illustrates the overview of this approach [13]. In the rest of this section we describe number of fundamental advantages that this approach provides over the existing solutions:

The storage capacity of the SE should be large enough to store user applications with unknown sizes. As the user may wish to add more applications to his NFC phone, this issue brings a limitation for existing solution because each SE supports certain storage capacity [14]. The other issue with the SE is that companies have to meet the requirements of organisations such as Europay, MasterCard and Visa (EMV) [15] to provide high level security in order to store cards data.

This approach makes the SE expensive for the companies, while the cloud-based approach reduces this cost. In the NFC cloud-based approach, the phone's SE can only be responsible for user/device authentication and not for storing data. This solution increases the cost efficiency compare to the current costs that SE makes for a company. Also, the NFC controller chips will be smaller and cheaper since they would not have to support all functionalities. Furthermore, the concept of the phone's SE can be completely avoided by replacing it with the concept of a trusted zone that can be created within the processor of a mobile phone.

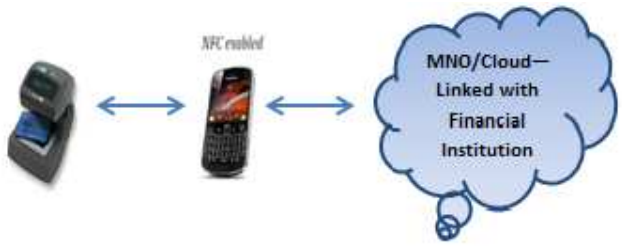

Figure 1. The vendor and the MNO communicate through the NFC Phone

The NFC cloud-based approach also makes the business simpler for companies for the integration of SE card provisioning. It would be much easier for businesses to implement NFC services without having to perform card provisioning for every single SE. An NFC phone user will be able to access unlimited number of applications as they are stored within a cloud secure server and not in the phone's SE. In terms of flexibility, all users would be able to access all their applications from their devices (e.g. phones, tablets or laptops) since the applications are stored in a cloud environment. Moreover, fraud detection would be instant as the system fully runs in an online mode.

Since all the information is stored in a cloud (virtual SE), there is no need for mobile wallet. Therefore, in order to change their mobile wallet information, users can easily use the virtual SE to access the information they require online via a web browser. This approach also improves SP services as they are no longer required to develop different applications for different types of mobile phones. This approach reduces the risk of third parties getting unauthorised access while the phone is being shipped to a new user or for repairing purposes. This is because there is no SE with stored user confidential information in the NFC phone as this information is stored in a cloud environment and not in the handset itself. The cloud-based transaction method provides the card present payment, since the phone's SE deals with the authentication between the handset and the vendor's terminal. This solution enables the NFC phone to be linked to multiple virtual SEs (stored in the cloud) that allows any user to access its own SE in order to modify the information (e.g. to add/delete applications). The acceptance of the NFC cloud-based transaction method is dependent on having the ability to implement strong authentication mechanisms as well as conducting transactions quickly enough in order to increase the performance. The processing times are far quicker in this approach because the virtual SE is stored in a cloud where there is more computing power available in contrast with phone's SE. However, more time is required for data request to reach the cloud server and return back to the vendor terminal. Thus, the lack of connectivity can impede the use of the system.

To summarise, NFC cloud-based solution offers infinite computing services and extensive capabilities in terms of storage, networking of shared devices and computing. The solution provides broad capabilities to enable the use of different platforms bringing the user access into ubiquitous computing. Different virtual and physical needs of clients makes the NFC a flexible technology therefore, the system should have the ability to provide a desired infrastructure in order to make the consumers capable of managing their resources in the best possible way. As mentioned previously, our aim is to discuss the use of NFC in mobile payments therefore we describe the previously proposed NFC cloud wallet in brief to introduce an alternative approach based on this model.

IV. NFC CLOUD WALLET MODEL

This model [1][13][14] introduced the idea of using cloud computing to manage NFC payment applications which result in flexible and secure management, personalization and ownership of the applications. 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 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 that contains customer credentials is downloaded into the phone's SE from the cloud and, after the transaction, it is deleted from the device and the cloud will be updated to keep a correct record of customer account balance. The execution of the model is described as follows:

1) Customer scans the NFC enabled phone on the vendor's 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
4) Cloud provider transfers the required information to the reader
5) Based on the information that 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 balance if customer request was authorized, the amount of purchase will be withdrawn from his account otherwise customer account remains with the same balance

Fig. 2 illustrates the steps that should be undertaken to complete the transaction process. As an addition to this model, we suggest: when NFC enabled phone sends a request to its cloud provider to get permission to make a payment (step 1), cloud provider sends an Short Message Service (SMS) requesting a Personal Identification Number (PIN) number to identify the user of the phone. This is how cloud provider ensures the legitimacy of the phone user. For the purpose of verification, the customer sends PIN back to the cloud provider as an SMS.

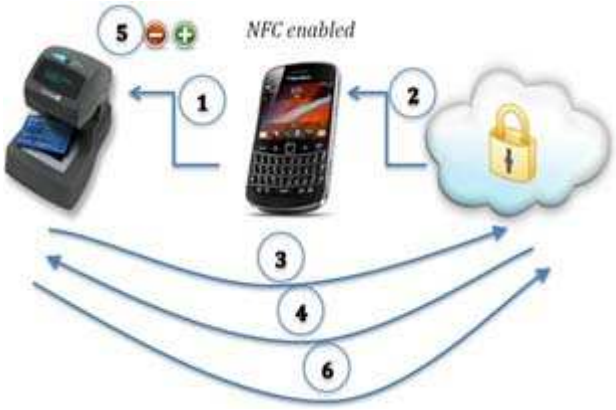

Figure 2. NFC Cloud Wallet

V. PROPOSED MODEL

We propose an extension to previously proposed NFC Cloud Wallet model. Since there are multiple options applicable to this model, we designed our model based on the following assumptions:

- The virtual SE is part of the cloud which is managed by the MNO
- The phone's SE is only used for authentication purposes. SIM as SE is the best approach in this scenario (i.e. UICC)
- The MNO manages the SE/SIM
- Banks, etc. have connections with MNO
- *The vendor trusts the MNO*

The virtual SE securely stores personal data such as debit and credit card information, user identification number, loyalty program data, payment applications, PINs and networking contacts, among other information. However, the phone's SE consists of authentication data such as keys, certificates, protocols and cryptographic mechanisms. As explained in section II, SE is in the form of UICC in our model (SE part of the SIM) therefore, the SIM only deals with the authentication of handset to MNO and handset to vendor terminal. Rather than that, the main transaction data are stored in the SE within the cloud environment. During the whole process, MNO manages the cloud environment and it is the only party that has full access and permission to manage confidential data which are stored in the cloud. As MNO is the owner of the cloud, it fully manages the SIM in terms of monitoring the GSM network and controlling cloud's data. The key assumption of this framework which makes the whole process logical in terms of its protocol design is the trusted relationship between the vendor and MNO. The analysis of this assumption is described in section VI. Below is the step by step description of the process as illustrated in Fig.3.

1) Customer selects a product. Purchase request sent to the vendor's terminal
2) Vendor's terminal displays the price
3) If Customer agrees with the price, he places his NFC enabled phone on the vending machine
4) NFC link is established between the vendor terminal and the NFC enabled phone
5) The customer requests a message from the MNO to use it in order to prove its legitimacy to the vendor. Customer also informs MNO of the total price.
6) The MNO first authenticates the customer. After a successful authentication, if the MNO agrees with the price, it sends a digitally signed confirmation message to NFC enabled phone (the customer)
7) The mobile device then relays the same message to the vendor terminal
   - Since vendor terminal trusts MNO, it trusts the digitally signed message

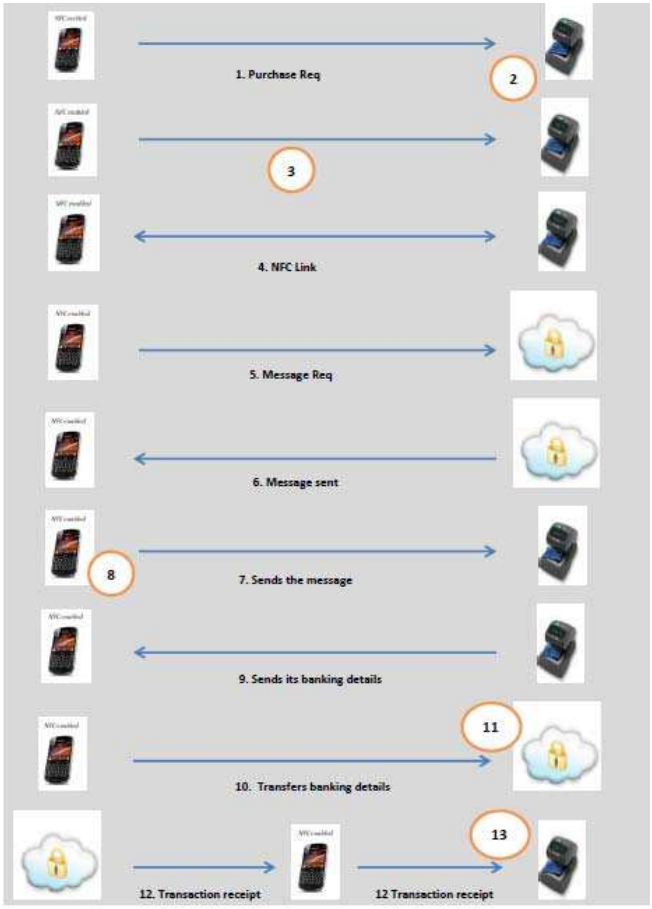

Figure 3. MNO communicates with vendor through NFC phone

8) The NFC enabled phone displays enter PIN to verify its legitimacy and its ownership of the cellphone (additional security mechanism)
9) Vendor terminal sends its banking details in an encrypted form to the NFC enabled phone. This message can be decrypted only by the MNO.
10) NFC enabled phone transfers the same banking details to the MNO
11) The MNO performs the transaction
12) The MNO sends a signed receipt to the vendor terminal through the NFC enabled phone
13) The vendor's terminal verifies the receipt
14) If the verification is successful, the product is delivered and a success message displays on the NFC enabled phone

The trusted relationship between the vendor and MNO establishes when the MNO sends a confirmation message of the vendor through the NFC enabled phone (steps 6and 7). This digitally signed message confirms that the customer has enough credit for the transaction.

VI. ANALYSIS

In this section, we carry out an analysis from security point of view. Since this protocol is used for monitory transactions, it must be as much secure as possible. We sketched multiple scenarios where a buyer or a seller is dishonest and then analysed their success probability.

In the first scenario, we assume that a customer is dishonest and wants to purchase a product without payment. The dishonest customer can only be successful if he can successfully generate a signed receipt in step 12 of the protocol. Since this receipt is signed by the MNO, an illegitimate customer cannot generate a valid receipt. Moreover, the dishonest customer cannot replay the old receipt as the receipt contains time information. Therefore, this scenario is not successful.

In another scenario, we assume that the customer is dishonest and just want to extract the banking details of a vendor. The vendor provides his banking details after it receives a signed confirmation from the MNO. The banking details are encrypted so the customer cannot decrypt and understand this message. This message can be decrypted by the MNO only who needs banking details for the transaction. So a dishonest customer is again unsuccessful.

In the third scenario, the seller is dishonest and plans to extract more than the required amount from a customer. To perform this action, the seller alters the price information at transaction stage. However, the alteration is deducted in the signed receipt provided by the MNO after transaction. This receipt is provided to both, the customer and the seller. The customer detects any alteration in the price by the seller. So this scenario is also not successful.

In the fourth scenario, the seller is dishonest and records all the legitimate messages of a customer. He plans to replay the recorded messages to the MNO to extract money from a customer in his absence. To do this, the dishonest seller impersonates as a customer to MNO. This impersonation is detected by the MNO in the initial steps of the model where the MNO authenticates a customer before proceeding to transaction. This scenario is, again, not successful.

VII. CONCLUSION

In this paper we discussed the NFC cloud wallet model and introduced a different insight which proposed a new integrated framework based on trusted integrations of cloud-based NFC transaction players which are the MNO, the NFC phone user and the vendor. We considered a cloud-based approach for managing sensitive data to ensure the security of NFC transactions over the use of a virtual SE as well as considering the role of mobile phone's SE within the NFC payment architecture. In addition, this paper provides related issues that are essential to investigate other possible ecosystem architectures, players with their roles, different possible access controls and ownership issues in NFC ecosystem. Although this paper suggests a new payment method, but we do not recommend it for large transactions (over £50.00) to avoid security limitations imposed by technology providers. In return, for the convenience, it offers customers in terms of a faster and more streamlined purchasing process. As a part of future research, issues such as the connectivity between the cloud and the NFC phone, the cloud's architecture while operating as a service provider (MNO in our scenario), a framework for application personalization procedures, and the design of security payment protocols can be explored, designed and analysed in order to finalize the most reliable architecture for cloud-based NFC transactions.

REFERENCES

[1] P. Pourghoumi and G. Ghinea, "Managing NFC Payments Applications through Cloud Computing," In 7th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE Press, Dec. 2012, pp. 772–777.

[2] NFC Forum, "Essentials for successful NFC mobile ecosystems," Oct. 2008. [Online]. Available: http://www.nfcforum.org/resources/whitepapers/NFC Forum Mobile NFC Ecosystem White Paper.pdf

[3] K. Curran, A. Millar, and C. M. Garvey, "Near Field Communication," In International Journal of Electrical and

Computer Engineering, vol. 2, Number 3. Institute of Advanced Engineering and Science Press, Apr 2012, pp. 371–382.

[4] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, "On the Security Issues of NFC enabled Mobile Phones," In International Journal of Internet Technology and Secured Transactions (ICITST), IEEE Press, volume 2, Number 3/4, Inderscience Enterprises Ltd, 2010, pp. 336-356.

[5] G. Alpar, L. Batina, and R. Verdult, "Using NFC Phones for Proving Credentials," In Measurement, Modelling, and Evaluation of Computing Systems and Dependability and Fault Tolerance, Springer, 2012, pp. 317-330.

[6] P. Pourghoumi and G. Ghinea, "Challenges of Managing Secure Elements within the NFC Ecosystem," In 7th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE Press, Dec. 2012, pp. 720-725.

[7] G. Madlmayr, J. Langer, and J. Scharinger, "Managing an NFC Ecosystem," In Proceedings of the 7th International Conference on Mobile Business, ser. ICMB '08. Washington, DC, USA: IEEE Press, 2008, pp. 95–101. [Online]. Available: http://dx.doi.org/10.1109/ICMB.2008.30

[8] GSM Association, "Requirements for SWP NFC Handsets V4.0," March 2011. [Online]. Available: http://www.gsma.com/mobilenfc/wp-content/uploads/2012/03/gsmarequirementsforswpnfchandsetsv4.pdf

[9] P. Urien, S. Piramuthu, "Towards a Secure Cloud of Secure Elements Concepts and Experiments with NFC mobiles," In proceedings of International Conference on Collaboration Technologies and Systems, San Diego, USA, 2013, pp. 166-173.

[10] M. Roland, J. Langer, and J. Scharinger, "Applying Relay Attacks to Google Wallet," In proceedings of the 5th International Workshop on Near Field Communication (NFC), Zurich, Switzerland, Feb. 2013.

[11] MasterCard (2013). "MasterPass," [Online] https://masterpass.com/online/Wallet/Help?cid=127568. Accessed 7 April 2013.

[12] Google (2013). "Goole Wallet," [online] http://www.google.co.uk/wallet/faq.html. Accessed 3 April 2013.

[13] P. Pourghomi and G. Ghinea, "Ecosystem Scenarios for Cloud-based NFC Payments," In International ACM Conference on Management of Emergent Digital Ecosystems (MEDES), In ACM Press.

[14] P. Pourghomi, M. Q. Saeed, and G. Ghinea, "A Proposed NFC Payment Application," In International Journal of Advanced Computer Science and Applications (IJACSA), volume 4, Number 8, Sep. 2013, The Science and Information Organization Ltd, pp. 173-181.

[15] J. Pailles, C. Gaber, V. Alimi, and M. Pasquet, "Payment and Privacy: A Key for the Development of NFC Mobile," in Collaborative Technologies and Systems (CTS), International Symposium on, May 2010, pp. 378 –385.