International Journal of Scientific Research Engineering & Technology (IJSRET)
Volume 1 Issue5 pp 207-211 August 2012 www.ijsret.org ISSN 2278 – 0882

Mobile Payments by short range wireless Connectivity

[1]Rohit, [2]Neeraj Joshi, [3]Navneet Kumar Yadav
[1,2]Department of Computer Science Engineering
[1,2]Meerut International Institute of Technology, Meerut
[1]Rohit.saklan@gmail.com, [2]Njr.scorpian10@gmail.com, [3]Navneetyadav16@gmail.com,

ABSTRACT
For merchants, Point of Sale mobile payments could provide faster throughput at the checkout and the ability to send real time marketing messages to the consumer.
NFC (Near Field Communication) is a short-range wireless connectivity technology which enables the exchange of data between devices over a range of about 10 cm. ISO/IEC 14443 defines specifications for identification cards, contactless integrated circuit cards, and proximity cards, which for the purposes of discussion here we'll call "tags. NFC is an evolution of the original specifications used to create RFID tags and contactless payment systems. Mobile Devices equipped with NFC enable applications like chip payments, ticket services, access control and loyalty programs, in such cases the mobile is operated in card emulation mode. RFID technology is employed in the MIFARE-based cards that are widely used for transit systems and secure building access, biometric passports, and contactless payment systems like pay Wave and MasterCard's, Pay Pass. NFC alone does not ensure secure communications in transaction of mobile payments.

Key words: *NFC, RFID, Contactless*

I. INTRODUCTION
NFC (Near Field Communication is a short-range wireless connectivity technology which enables the exchange of data between devices over a range of about 10 cm. The technology is a simple extension of the ISO 14443 contactless card standard, RFID that combines the interface of an ISO 7816 smart card and an RFID reader into a single device. NFC (Near Field Communication) is a passive RF technology usually based on ISO/IEC 18092, different from classic passive RFID by virtue of NFC's ability to act as both a tag and reader. Talk of NFC integration into cellular phones has become a consistent topic of technology journalism in recent years, and has approached a point where main stream cell phone adoption seems inevitable [1].

I.

NFC forum defines three communication modes

- Peer-to-Peer mode is defined for device to device link-level communication. Note that this mode is not supported by the Contactless Communication API.
- Read/Write mode allows applications for the transmission of NFC Forum-defined messages. Note that this mode is not secure. This mode is supported the Contactless Communication API.
- NFC Card Emulation mode allows the NFC-handset behave as a standard Smartcard. This mode is secure. This mode is supported by the Contactless Communication API.

NFC Terminology

- NDEF - NFC Data Exchange Format - standard exchange formats for URI, Smart Posters, other
- RTD - Record Type Definition - An NFC-specific record type and type name which may be carried in an NDEF record
- NDEF message - Basic message construct defined by this specification. An NDEF message contains one or more NDEF records
- NDEF record - Contains a payload described by a type, a length, and an optional identifier.
- NDEF payload - The application data carried within an NDEF record.[2]

Payment

A payment can be handled in the same manner as for ticketing. There are both online and offline systems. In an online system the serial number stored in the chip is linked to a database containing the value or the credit limit of the user. In an offline system the chip is pre-filled and the remaining value is stored in the memory of the chip. The chip memory may contain a smart card emulator and smart card applications to enable easy upgrades of older systems. The greatest consumer benefit would be if the chip was integrated into, e.g., a

mobile phone rather than a credit card, and the POS is linked to a debit system. Upon a transaction larger than a preset threshold, the user would be asked to agree or enter a personal identification number (PIN) or password via the user interface of the mobile phone. Thus large transactions are secure while small transactions are kept swift and simple. With a well implemented and marketed standard this could be the new means for both small and large payments.

MasterCard introduced its contactless payment solution Pay Pass in 2002. It is based on the ISO 14443 standard and enables quick and easy payments by tapping the credit card on the POS terminal reader. The standard ISO ID-1 credit card format is the most common size used, but smaller tags or key fobs and watches are available. The card is limited to 106 kbps, but the terminals may optionally also support 212 kbps and 424 kbps. The terminals are programmed to allow only one card in the field. This restriction ensures that the right person and card is charged with the purchase. The communication is encrypted using standard PKI (Public Key Infrastructure) technology. The limit for unsigned transactions varies by merchant category, but is generally below USD 25. The customer can also retain possession of the card during the transaction, which makes it feel safer. The Pay Pass implementation of RFID was put through a large-scale field test in Orlando, Florida, in 2003. More than 16,000 cardholders and over 60 retailers participated in this trial. MasterCard in cooperation with Nokia has also tested the Pay Pass technology incorporated into the Nokia 3220 mobile phone in Dallas, Texas. Further trials have been made in cooperation with Motorola. In January 2006, 7 million Pay Pass cards had been issued and 30,000 merchant locations accepted Pay Pass payments. [3]

II. MOBILE PAYMENTS IN GLOBALIZATION

The attraction of mobile payments is unquestionable. For Mobile Network Operators, mobile payments are an attractive proposition for achieving a return on the investments made in infrastructure over the last two decades through both extra payment related revenues and the associated increase in air time and data use. For merchants, Point of Sale mobile payments could provide faster throughput at the checkout and the ability to send real time marketing messages to the consumer. However, faster throughput could also be achieved through contactless cards and it is yet unclear whether consumers would actually want or appreciate real time marketing messages from the merchant on their phone. Remote mobile payments provide another channel for merchants and as such are an attractive proposition if the use of the channel can gain wide scale adoption at lower costs than existing channels. From the perspective of the end consumer, the mobile phone has achieved 'permanent share of pocket', i.e. next to the wallet and keys it is the object that is most likely to be constantly with the consumer. Furthermore, consumers are increasingly more comfortable with the mobile phone fulfilling more than one function, with mobile.

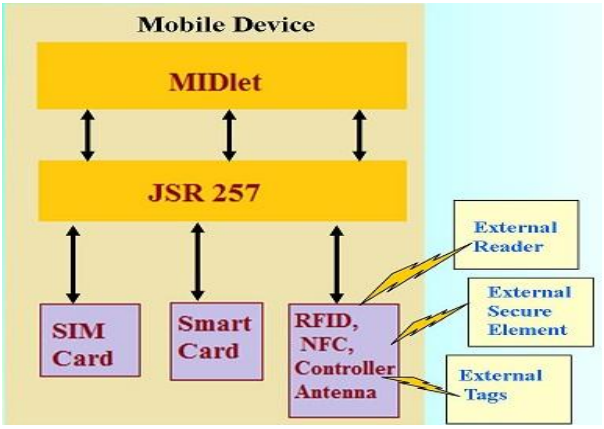

Figure 1: Structure of NFC builds Mobile

Success of Mobile Payments in market- Case Study

Mobile payment involves tension between a merchant-consumer desire to minimize risk and costs and maximize usability. Analysis of several contexts through this realization shows that Purchase of non physical goods (e.g. ring tone, parking, etc) would benefit from payment solutions that link directly to existing financial instruments such as current accounts and cards and allow for the use of these instruments without registration. NFC solutions should prepare for a long and hard battle to break into the Point of Sale market because of the attraction of existing solutions such as debit and credit cards. The current focus of these solutions is the promotion of their usability features (e.g. contactless, interactive communication on mobile device, etc). The key deterrent from consumer and merchant sides will be their high costs. While providers may gain temporary success with early adopters or niche industries they must

focus on bringing down costs to establish any reasonable market share Public transport is likely to provide the highest volume potential for mobile payments. However it is not clear what advantages mobile payments bring in this context over contactless payments. Remote Point of Sale, e.g. vending machine has obvious benefits from mobile payments if costs of these solutions can be kept low. Most service providers are aware of the behavioral barriers of new products such as economic switching costs (e.g. activation fees, learning costs, obsolescence fees, etc) but what service providers often don't take into account are the psychological barriers associated with behavioral change. These psychological barriers include the overvaluation of current methods of payment and loss aversion where people are more upset at losing a benefit than they are delighted at gaining a similar benefit. These barriers imply that one of the keys to successful adoption of a new innovation is the degree of change demanded from the receiver of the innovation. The smaller the consumer's change in behavior needs to be, the greater the chances of success are. [5]

Report Says: In 2002 market experts forecast that by 2006 €55 billion would be processed through mobile payments. However, in 2006 the same sources predicted the market to reach only €10 billion by 2010[c]. In 2009, one source predicted that in 2013 an absurd $800 billion [6] would be transacted by phone while another source predicted a much more conservative $1.5 billion for the United States alone [7].

III. CELLULAR PHONES - NFC APPLICATIONS

Currently existing applications

Only a few NFC compatible cellular phones are released as this report is written. More models are released in Asia compared to Europe and USA. The Nokia 3220 is one NFC enabled model that is available in Europe. It is equipped with an NFC reader/writer capable of reading and writing the Mifare light standard cards. The applications for the Nokia NFC phones marketed on their website are the possibility to read/write web links, phone numbers and SMS to tags which then can be placed where it is most likely to need the information. For example, a tag with the phone number to a towing company can be written and placed on the inside of the car windshield in case the car breaks down. Two NFC phones could also connect to each other, enabling exchange of phone numbers, pictures, or ring tones. [8]

A widely spread vision is to use NFC to connect Bluetooth devices to one another by putting them together and thereby making the indication that they should be connected. NFC handles the transfer of serial numbers and the initialization signaling [9].

Corporate demand:

- Consumer demand for advanced functionality handsets also opened opportunity in the corporate environment for changing the way employee's work and access information.
- Development of enterprise applications for the mobile workforce has increased workplace flexibility for employees and helped corporations become more efficient in their operations and supply-chain.

IV. SECURITY IN MOBILE PAYMENTS

Mobile Devices equipped with NFC enable applications like chip payments, ticket services, access control and loyalty programs, in such cases the mobile is operated in card emulation mode. The card is emulated in a Secure Element. The secure element can be located on a secure smart card like an embedded dedicated component, an SD card and now also a USIM. To give the mobile phone user access to the card functionality, it is required to have a dedicated JAVA application (MIDlet) installed on the mobile device as a GUI. Data under control of the MIDlet is basically insecure, so all sensitive handling of data is performed by Java Card Applets executing in the secure element. An update of a secure data element, such as a balance recharge, the distribution of a ticket or access key can take place over the contactless interface, but with a mobile phone also Over The Air (e.g. GPRS).[10]

Applications may use higher-layer cryptographic protocols (e.g., SSL) to establish a secure channel. Ensuring security for NFC data will require the cooperation of multiple parties: device providers, who will need to safeguard NFC-enabled phones with strong cryptography and authentication protocols customers, who will need to protect their personal devices and data with passwords, keypad locks, and anti-virus software; and application providers and transaction parties, who will need to use anti-virus and other security solutions to prevent spyware and malware from infecting systems. [11]

Function of the Secure Element The secure element (secure memory and execution environment) is a dynamic environment in which application code and application data can be securely stored and administered and in which secure execution of applications occur. The element resides in highly secure crypto chips9 (usually a smart card chip). The element provides delimited memory for each application and functions that encrypt, decrypt, and sign the data packet. The secure element present in mobile devices is Global Platform compliant to provide better interoperability. [12]

The first approach embeds a separate secure element directly in the handset (either mounted on the motherboard directly or connected in some way to the motherboard). A second approach is to embed the secure element into an SD card. A third approach is to embed the secure element in the USIM/SIM card. The industry is still evaluating the pros and cons of including multiple secure elements in a single mobile handset.

V. SECURITY DOMAINS AND HIERARCHY

The Global Platform specification (Version 2.2) defines multiple security domains that use authorized and delegated management to allow an application to be loaded into the secure element. Any Global Platform-compliant secure element comes with one issuer security domain (ISD) and the option for multiple supplemental security domains (SSDs). As shown in, the SSDs can be TSM security domains or domains belonging to service providers (such as credit card, ticket, prepaid/loyalty card, or transit card issuers). In addition, each secure element can have only one controlling authority security domain (CASD). This security domain architecture enables the service provider and trusted service manager to perform key management and application verification during load and installation processes. [10]

Chip-Level Security

The Smart Card Alliance white paper describes the multi-layer security architecture of a smart card chip. Security features manufactured into the secure microcontrollers used in smart card chips can prevent attackers from accessing sensitive information stored on the card. [13]

The SIMs and USIMs in mobile phones are smart card chips, and have built-in tamper-resistance. Smart Card chips include a variety of hardware and software capabilities that detect and react to tampering attempts and help counter possible attacks. For example, the chips are manufactured with features such as extra metal layers, sensors to detect thermal and UV light attacks, and additional software and hardware circuitry to thwart differential power analysis. With contact and contactless interfaces, increasingly powerful processors, a wide range of memory options, and flexible implementation of both symmetric and asymmetric cryptographic algorithms, smart card technology is a critical component of a secure system design.

Payment Transaction Security

Proximity mobile payments leverage ISO/IEC 14443, the standard that governs communication between a contactless credit or debit payment device and terminal. Payment transactions invoke additional layers of security during transaction processing, regardless of whether the transaction is a magnetic stripe transaction or a contactless or mobile transaction. In the case of a proximity mobile payment transaction, the first layer of security is provided by the secure element itself, which protects the payment application by storing it in restricted access memory. The payment application generates a dynamic cryptogram that is integrated into the transaction messaging/communication process with the terminal. The terminal and the merchant system perform risk management checks; the host system then completes an authorization function, which checks the authorization limit available and card validity, among other things. The security provided by an isolated component in the process does not accurately represent transaction security as a whole. [14]

VI. CONCLUSION

Mobile payment involves Analysis of several contexts through this realization shows that Purchase of non physical goods (e.g. ring tone, parking, etc) would benefit from payment solutions that link directly to existing financial instruments such as current accounts and cards and allow for the use of these instruments without registration. The security provided by an isolated component in the process does not accurately represent transaction security as a whole.

REFERENCES

[1]http://www.nfctimes.com/news/new-apple-nfc patent-casts-iphone-role-device-sharing

[2] http://www.NFC/An Introduction to Near-Field Communication and the Contactless Communication API.htm
[3] MasterCard Worldwide, "MasterCard PayPass",2006-03-27,www.mastercard.com/paypass/
[4] Telecompaper, Bobey Forum – Mobile Payements2011.
[5] www.mobilemonday.net/news/mobile-payment-market-to-reach-eur-55-billion-in-2006
[6] www.marketwire.com/press-release/Xcellink-International-Inc-1031269.html
[7]www.frost.com/prod/servlet/pressrelease.pag?Src=RSS&docid=165875378
[8] Visa International Service Association, "Visa Contactless", 2006-03-27, http://usa.visa.com/personal /cards/contactless/index.html
[9] Proceedings European Wireless 2002, R.Bridgelall "Bluetooth/802.11 Protocol Adaptation for RFID Tags", Symbol Technologies, NY, USA
[10] Hancke, Gerhard P (July 008), "Eavesdropping Attacks on High-Frequency RFID okens" , 4th Workshop on RFID Security (RFIDsec'08), pp. 100–13.
[11] Harley Geiger, NFC Phones Raise Opportunities, Privacy and Security Issues,Center for Democracy and Technology, April 11, 2011.
[12] Gerhard P. Hancke:A practical relay attack on ISO/IEC 14443 proximity cards , February 2005.
[13] http://www.mulliner.org/nfc/ (NFC Security Tools)
[14] A Smart Card Alliance Contactless and Mobile Payments Council White Paper