# Security Report for Mobile Wallet implemented from NFC Technology for Mobile Payment

Abhishek Soni* and Dr. Vikas Kulshreshtha**
*Assistant Professor, Department of Information Technology, Government Engineering College Jhalawar
Abhishek11_soni@yahoo.co.in
**Assistant Professor, Department of Information Technology, Government Engineering College Jhalawar
vikas.kulshreshtha@gmail.com

**Abstract:** The trend of using non-cash transaction in Ecommerce is very common and widely used in this era. But customer needs confidence in security of the services for adoption of mobile banking and payments. Now a days Mobile wallet is used broadly for cashless payment. So in this paper we introduce the mobile wallet and its security and as well as NFC (Near Field Communication) Techniques used in Mobile wallet for payment or transferring money with in nearly 4 cm Distance. We also shows security mechanism used in Near Field Communication techniques for ensuring secure data transfer between two NFC devices.

**Keywords**: Mobile Wallet, NFC(Near Field Communication), RFID(Radio frequency identification), NFC tags, proximity card, electromagnetic induction, transponder, Miller coding , Manchester coding, Service Access Point (SAP) , Service Data Unit (SDU) , Protocol Data Unit(PDU).

## Introduction

Today all digital data is transferred between devices, between devices and servers and sensors to devices in the open environment. Most of the data contains personal and financial or business related information which should have restricted access or should be confidential and unmodified during transfer. Instead of wired Ethernet, mobile devices use wireless networks for transferring these data, which requires additional security mechanisms. If cellular devices or mobile phones is used to conduct financial transaction like online banking and payment for shopping then it refers to Mobile Banking. So throw mobile, an user can perform various activities like transfer funds between accounts, pays bills, view account statement/balance/mini statement etc which needs some security mechanism so that the user can confidently use Mobile Banking.

### Mobile Wallet

A mobile wallet is a way to carry cash in digital format through which a user can link his credit card or debit card information in mobile device. A user can also transfer money online to mobile wallet. It is not necessary that a user have to use physical plastic card to make purchases, but also he can pay with his smart phone, tablet, or smart watch. For loading money in digital wallet, individual's account is required to be linked to the digital wallet. For transmitting data in device based mobile wallets between mobile payment device and merchant Point of Sale(POS), various types of communication technologies is used . Some techniques for mobile device to merchant Point of Sale communication includes Magnetic Secure Transmission[1] (MST), Near Field Communication[2] (NFC), Security of Mobile Payments and Digital Wallets, Quick Recognition (QR) Code[3] , Bluetooth[4] , Bluetooth Low Energy[5] (BLE), and Short Message Service[6] (SMS), as well as the Internet. Working of Mobile Wallet include by run an application (app) on mobile, validate by PIN, password or fingerprint and then access the information which they want to need. Near-Field Communications (NFC) Technology is used by the Mobile Wallet application to interact with mobile wallet ready payment terminals. The mobile wallet keeps various security features to ensure that such sensitive information remains secure.

### Near Field Communication (NFC)

Near Field Communication(NFC) is a techniques in which two devices placed within a few centimeters and it allows to exchange information to each other. Each device must have NFC Chip for communication. The concept of Near-Field Communication is grows from radio frequency identification (RFID) technique which contains a set of communication protocols to establish communication in which an NFC chip operates as one part of a wireless link and once it's activated by another chip, few amounts of information can be transferred between the two devices in the distance of few centimeters i.e within 4 cm (1.6 in) from each other[7]. Each NFC device can work in three modes:

(1) NFC card emulation - enables NFC devices such as smart phones to work like smart cards, allowing users to perform financial transactions such as payment.
(2) NFC reader/writer - enables NFC devices to read information which is stored on inexpensive NFC tags embedded in labels or smart posters.
(3) NFC peer-to-peer - enables two NFC devices to communicate with each other for exchanging information in an adhoc fashion.

NFC tags (custom-encoded or sometime industry specification) contains passive data which can be read (read only), and re-writable under some circumstances, by an NFC device. All personal and financial data such as credit card and debit card information, PINs, passwords etc, can be securely stored in these tags. Communication speeds and capabilities depend on configurability, memory, security, data retention and write endurance.

NFC [8] [9] operates at 13.56 MHz on ISO/IEC 18000-3 air interface. A transfer bit rate range is between 106 kbits/s and 424 kbits/s. NFC always has an initiator and a target; the initiator actively generates an RF field and that RF field can power a passive target. When advance research happen in proximity card technology, NFC uses electromagnetic induction between two loop antennas located within each other's near field, effectively forming an air-core transformer. It operates within the globally available and unlicensed radio frequency ISM band of 13.56 MHz[10]. In passive communication mode, the initiator device provides a carrier field and the target device answers by modulating the existing field and the target device may draw its operating power from the initiator-provided electromagnetic field, which makes the target device a transponder. In Active communication mode, initiator and target device both communicate by alternately generating their own fields but a device deactivates its RF field while it is waiting for data and also both devices typically have power supplies. NFC use Miller coding with 100% modulation if an active device data transfers rate is 106 kbit/s, otherwise it use Manchester coding with a modulation ratio of 10%. All NFC devices are full-duplex.

## Security in Mobile Wallet

The major issue and their solution for securing mobile wallets are[11]-

**User Authentication**

It requires the user to authenticate to the device in order to perform a payment in the case of stolen device. Solution includes fingerprint identification sensor (the TouchID) or a PIN number, password, or pattern to authenticate a transaction.

**Device Authentication**

It requires that the transaction is coming from an authorized device or not. A unique identifier and a cryptogram is used to authorize the transaction which ensure that even if the token is stolen, it can't be used from another device because the token must come from the device to which it was registered. Unique Identifier may be periodically changed from servers.

**Data Protection**

Data protection can be done through the following techniques :-

Tokenization technique in which instead of using real PAN and card verification(CVV), a token is created when the user enroll his card, that is stored on the device and used during payment operations . This design decision minimizes the exposure of real confidential data and allows the user to quickly block a card if the device has been stolen, having the card working. This approach also limits attacks from untrusted merchants, who never have visibility of the real PAN or CVV.

Leveraging the Secure Element techniques in which a Secure Element (SE) present in devices using a highly secure chip that is tamper proof i.e if it detect any attempts at reading its contents, it automatically zeros memory ensuring that no keys can be extracted.

Debit card or Credit Card data is sent from the payment network or card issuer encrypted using payment applets that reside in the secure element. Sometimes the card sensitive data stores on databases hosted in a secure cloud environment.

Installation of rootkits/malware are a significant threat vector and can also be leveraged to directly monitor and hijack / manipulate API calls as they are being marshaled to/from the mobile payment API endpoint and hence manipulate variables in transit e.g., payment amounts.

Mobile Operating System Access Permissions A mobile OS may give access to certain resources with the permission of the user. Even if, a given application might not be malicious, holding certain permissions might potentially give access to sensitive data or be used by another application to elevate access.

## Security in NFC

Since the range of Near Field Communication is limited to a few centimeters, but there must be need some cryptographic protocols to guarantee secure communications or establish secure channel between NFC devices[12][13]. Because the antennas can picked RF signal for the wireless data transfer and the distance from which an attacker is able to eavesdrop the RF signal depends on multiple parameters, but is typically less than 10 meters[14]. Also the NFC occurs in the open air, data can be nabbed by anyone easily who tries to intercept. For securing the NFC NFC-SEC[15] is used which is illustrated in Figure 1 uses the OSI reference model specified in ISO/IEC 7498-1[15].

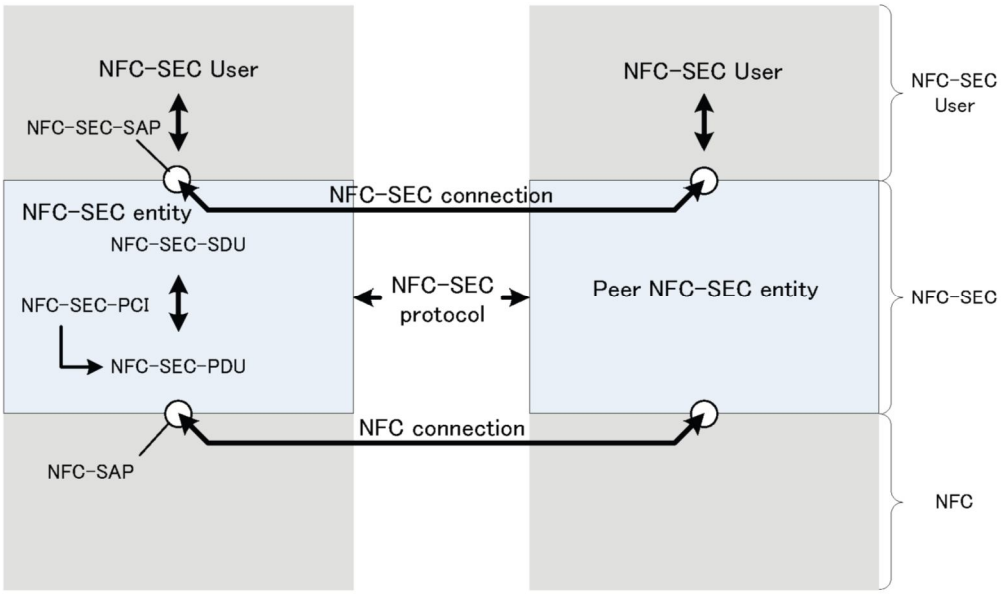


Figure 1 — NFC-SEC architecture[15]

NFC-SEC Users invoke and access the NFC-SEC services through NFC-SEC Service Access Points (NFCSEC-SAP). NFC-SEC entities obtain NFC-SEC-SDUs (requests) from NFC-SEC Users and return NFC-SEC-SDUs (confirmations) to them. Two services Secure Channel Service (SCH) and the Shared Secret Service (SSE) are provided to the NFC-SEC User which is describe below. For providing the NFC-SEC services, Peer NFC-SEC entities exchange NFC-SEC-PDUs by conforming to the NFC-SEC protocol over NFC-SEC connections. Peer NFC-SEC entities send and receive NFC-SEC-PDUs through NFC Service Access Points (NFC-SAP). A NFC-SEC-PDU consists of NFC-SEC Protocol Control Information (NFC-SEC-PCI) and a single NFC-SEC-SDU.

Protocol mechanism shall include one or more of the following cryptography standard:

(a)Sequence Integrity

(b)Confidentiality;

(c)Data integrity;

(d)Origin authentication.

The peer NFC-SEC entities shall terminate SSE and SCH using Terminate PDU(TMN).

**Shared Secret Service (SSE)**

A shared secret key between two peer NFC-SEC users are establishes by the Shared Secret Services. Both users will make key agreement and key confirmation mechanisms, according to the NFC-SEC cryptography part that defines the Protocol Identifier

**Secure Channel Service (SCH)**

A secure channel is provided by the Secure Channel Services. SCH establish link key, by key agreement and key confirmation mechanisms, and protect all communication subsequently in either direction across the channel, according to the NFC-SEC cryptography part that defines the Protocol Identifier.

## Conclusion

In the current scenario Contact less payment is the new research field. NFC Technique is used in Mobile wallet for transferring payment but it is necessary to ensure complete protection of data which is transferred between two NFC as well as device authentication and user authentication. Radio frequency identification (RFID) technique is used in Near Field Communication which contains a set of communication protocols to establish communication. For securing the NFC, NFC-SEC technique is used which ensure that it provides confidentiality, authentication and data integrity.

## References

[1] What is MST (Magnetic Secure Transmission)? http://www.samsung.com/us/support/answer/ANS00043865/
[2] Want, Roy. "Near field communication." IEEE Pervasive Computing 3.10 (2011): 4-7.
[3] Walsh, Andrew. "Quick response codes and libraries." Library Hi Tech News 26.5/6 (2009): 7-9.
[4] Haartsen, Jaap C. "The Bluetooth radio system." IEEE personal communications 7.1 (2000): 28-36.
[5] Gomez, Carles, Joaquim Oller, and Josep Paradells. "Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology." Sensors 12.9 (2012): 11734-11753.
[6] Ayabe, Benson S., Sharat Subramaniyam Chander, and Semyon B. Mizikovsky. "Short message service." U.S. Patent No. 6,141,550. 31 Oct. 2000.
[7] Cameron Faulkner. "What is NFC? Everything you need to know".Techradar.com. Retrieved 30 November 2015.
[8] "Home - NFC Forum". NFC Forum. Retrieved 2016-01-01
[9] ”ISO/IEC 18092:2004 Information technology -- Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol (NFCIP-1)". ISO. Retrieved 11 December 2011.
[10] Patauner, C.; Witschnig, H.; Rinner, D.; Maire, A.; Merlin, E.; Leitgeb, E. (24 September 2007). High Speed RFID/NFC at the Frequency of 13.56 MHz(PDF). RFID 2007. Vienna, Austria.
[11] Security of Mobile Payments and Digital Wallets December 2016. www.enisa.europa.eu
[12] *Haselsteiner, Ernst; Breitfuß, Klemens.* "Security in near field communication (NFC)]" *(PDF).*
[13] Gerhard P. Hancke:A practical relay attack on ISO/IEC 14443 proximity cards, February 2005.
[14] Hancke, Gerhard P (July 2008). "Eavesdropping Attacks on High-Frequency RFID Tokens" (PDF). 4th Workshop on RFID Security (RFIDsec'08).
[15] ”ISO/IEC 13157-1:2010, Information technology — Telecommunications and information exchange between systems — NFC Security — Part 1: NFC-SEC NFCIP-1 security services and protocol”ISO. Retrieved 15 November 2014.