NFC Technology for Contactless Payment Echosystems

EL Hillali Wadii
ENSEM, B.P 8118, Oasis,
Casablanca, Morocco

Jaouad Boutahar
EHTP, B.P 8108, Oasis,
Casablanca, Morocco

Souhail EL Ghazi
EHTP, B.P 8108, Oasis,
Casablanca, Morocco

***Abstract*—Since the earliest ages, the human being has not ceased to develop its system of exchange of goods. The first system introduced is barter, it has evolved over time into currency by taking various forms (shells, teeth, feathers, etc.). The evolution of micro-electronics has favoured the appearance of a new form of payment that is the credit card. Currently it is the most used means of payment throughout the world. Today financial institutions want to replace the credit card by mobile phone for the implementation of contactless payment systems via NFC. This mode of operation is called Host Card Emulation or HCE. We will present in this article the basic element at the heart of this technology, which is the Secure Element. We will present the different forms that this element can take and possible cases of use of this technology for the establishment of an ecosystem of payment by mobile or purchase tickets transport.**

***Keywords*—NFC; Secure Element; SIM-Centric; HCE; Tockenisation; MPayment; MTicketing**

I. Introduction

RFID (Radio Frequency Identification) is an automatic identification technology that first appeared during the Second World War, to identify friendly or enemy aircraft in airspace. Until then, the use of this technology remained restricted to military use and control of access to sensitive sites, for example nuclear zones [1].

The advances of this technology have continued through the years, giving rise to the passive tag "Smart Tags" which are smart chips comprising a programmable chip enabling once powered by an electromagnetic field by a responder transmitter by an identification code via Its antenna, this unique identifier allows the remote identification of objects or persons.

Today, RFID technology is widely used in most industrial sectors (aeronautics, automotive, logistics, transportation, health, etc.). Faced with the imposition of this technology, the ISO (International Standard Organisation) has in turn contributed greatly to the establishment of technical and application standards enabling a high degree of interoperability or even interchangeability.

NFC (Near Field Communications) technology is a technology derived from RFID technology that was jointly developed by Philips and Sony in 2002, it is a Semi-Duplex communication protocol. This communication protocol provides two-way communication, but in one direction at a time (not simultaneously). Generally, once a party begins receiving a signal, it must wait until the transmitter stops transmitting before responding [10]. This technology allows easy and secure communication between two compatible devices, enabling the exchange of data of the most advanced formats (business cards, telephone contacts, bank data, etc.) within a few centimetres (10cm in maximum) with a frequency Operating costs of 13.56 MHz.

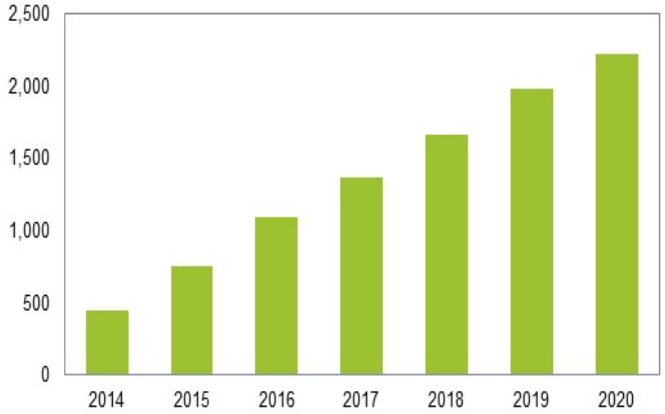

Fig. 1. World shipments of NFC-enabled Cellular Handsets (in Millions of Handsets Shipped) *(Source:* IHS inc. June 2015*)*

Mobile payment is the driving force behind NFC technology over the past seven years, it is widely used in contactless mobile payment, VISA estimates that mobile payment via NFC will replace the bank card in the coming years, Most manufacturers of smartphones have equipped their devices with this technology, according to a latest study conducted by IHS Technology, shipments of NFC chips are expected to increase to 756 million by 2015, against 444 million by 2014, today NFC technology has arrived at A very mature level, but the next five years will prove more fruitful with 2.2 billion deliveries of NFC handsets by 2020 (Figure 1) [2]

II. Radio Frequency Identification

In principle, an RFID application integrates a reader which has an antenna and a demodulator for translating an analogue information to a digital data by radio link, the reader first transmits a signal to one or more radio tags located in its read field, and waits for a feedback signal to be received. A dialogue is then established according to the predefined communication protocol to exchange the data. These are then relayed to a computer for processing.

Fig. 2. Example of RFID tag

In addition to contactless data transfer, communication via the antenna also allows wireless transfers between the reader and the label, unlike the bar code. The RFID tags are in the form of self-adhesive labels (Figure 2) which can be glued or incorporated into products or in the form of microscopic capsules (Figure 3) that can be implanted in living organisms (animals, human body) .

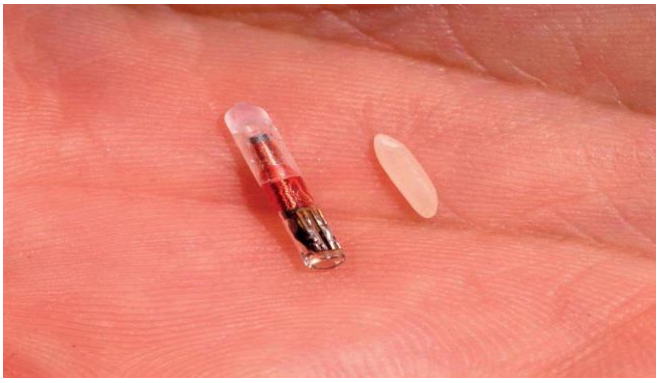

Fig. 3. Example of an RFID capsule

A. Type of RFID tags

There are three types of RFID tags: active, semi-passive and passive:

1) Passive Tags: Most RFID tags operate passively (without internal energy, battery or DC), unlike active tags, they do not have an internal battery because they take their energy from RFID readers. The RFID reader sends electromagnetic waves to the antenna of the tag, which will react (wake up) and return a signal to the reader using the energy of these waves. They are therefore the most economical and commonly used RFID tags in supply chain applications.

2) Active Tags: They use their own energies to emit their waves, using an internal battery and can thus have a very long reading distance (Figure 4), they are more expensive than passive tags and are therefore generally used to trace valuable items.

Fig. 4. Example of active tags used for payment on highway

3) The Semi-Passive Tags: These are intermediate tags between active tags and passive tags. They typically use a battery as an energy source (such as active tags), but can also transmit data using the energy generated by RFID reader waves (such as passive tags).

B. Categories of rfid tags

For each type of RFID tag, there are several categories of RFID tags, including:

1) "READING ONLY" LABELS: They are labels with an identification number engraved by the manufacturer, which can be read without being modified.

2) "READING ONCE, MULTIPLE READING" LABELS: They are labels allowing the registration of the unique identification number when the label is first used. Then, it is only possible to read this information.

3) "READ / WRITE" LABELS: They are labeling integrating pages of memory, in addition to the unique code, they allow the writing and modification of the new associated data.

The memory of a radiofrequency tag generally comprises a ROM (Read Only Memory), a Random Access Memory (RAM) and a non-volatile programmable memory for storing the data.

The ROM contains the security data as well as the operating system (OS) instructions for the basic functions such as response time, data flow control, energy. RAM is used for temporary storage of data during interrogation and response processes.

C. Frequency of rfid tags:

Once energised, the RFID chip begins transmitting a radio signal via its antenna in a radius ranging from a few centimetres to a few meters, depending on the power of the system, and especially according to the frequency used:

- LF : 125 kHz - 134,2 kHz : Low frequencies, or a reading distance of a few centimetres.

- **HF: 13, 56 MHz:** High frequencies, i.e. a reading distance ranging from 50 to 80 centimetres.

- **UHF: 860 MHz - 960 MHz:** Ultra-high frequencies, i.e. a reading distance of one to several meters.

Thus, and according to these frequencies, there are three types of operation of the RFID technology, each of which is used in a specific field:

- When it is a short distance of less than 5 cm, this is called the **NFC (Near Field Communication)**, Example (Access control, contactless payment).
- When the average distance is between 1 and 9 meters, it is the **RFID** range, Example (Transport Logistics).
- When the range is several hundred meters, then the **UHF** range, Example (Location).

III. NEAR FIELD COMMUNICATIONS

NFC near-field communication is a short-range wireless communication technology that allows information exchange between devices up to a distance of about 10 cm (Figure 5). This technology is an extension of the ISO / IEC 14443 standardising proximity cards using radio-identification (RFID) [11], which combine the interface of a smart card and a reader within a single device.

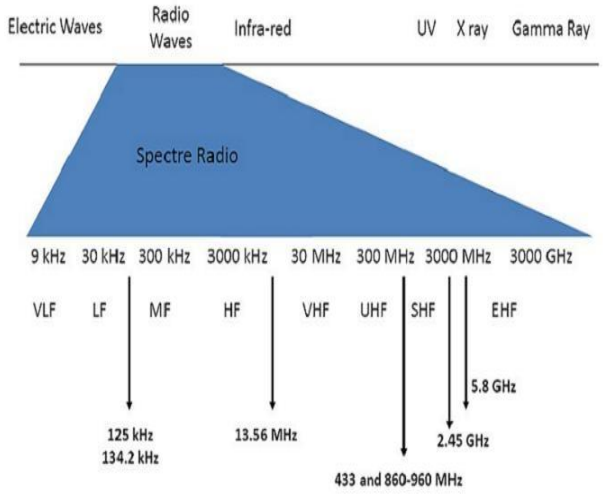

Fig. 5. Frequency band of different wireless technologies

The need for NFC technology has evolved considerably in recent years, given the number of applications that support it. This technology has established itself especially after its integration in smartphones, and it is implemented in several areas also mainly:

- Contactless payment from a mobile phone or credit card,
- Access control (company badges, car keys, ticketing, transport cards ...)
- Couponing (coupons or loyalty cards ...).

A. Near field communication on mobile

NFC on mobile is the most used and most supported technology in contactless payment at point of sale. It allows consumers to use their smartphones for contactless payment services, ticketing, or as an access badge or ID. It also allows a phone to behave like a real reading module of contactless card writing. The mobile phone operates in three modes thanks to the NFC chip:

- Card Emulation Mode.
- Read / Write tags Mode (MIFARE ...).
- Peer to peer mode (initiator & target).

1) Card Emulation Mode: Also called passive mode, or the mobile terminal behaves like a contactless smart card. The uses are multiple: payment, ticketing, couponing, access control ... (Figure 6).

Fig. 6. Using card emulation mode

The technological element that is at the heart of the card emulation mode is the Secure Element. It hosts and governs the various NFC applications of the user and can operate around four main models:

- A so-called "Device-centric" architecture in which the "Secure Element" is a constituent and inseparable component of the mobile phone.
- A so-called "SIM-centric" architecture in which the SIM card hosts the "Secure Element";
- A "Host Card Emulation" architecture where the "Secure Element" is hosted in the cloud.
- An architecture known as "SD-Centric" where the "Secure Element" is housed in an SD card.

a) Device-Centric Mode: Also called eSE or Embedded Secure Element, this is a secure zone in the smartphone that manufacturers are beginning to integrate into their new devices (Figure 7). The architectures of this component differ from one manufacturer to another and do not cease to evolve, but they all guarantee a secure access via a monitor of access control independent of the OS of the smartphone, has secret data (Identifier, Fingerprint, ...) and only to applications or authorised persons.

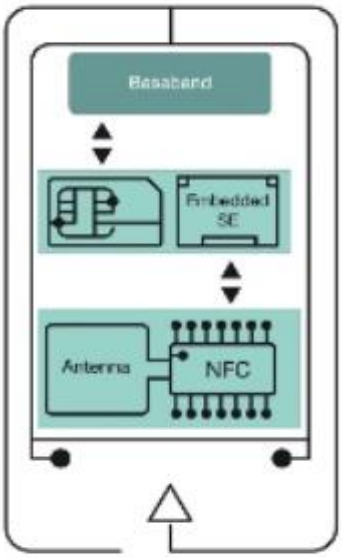

Fig. 7. Embedded Secure Element

b) SIM-Centric Mode: The SIM card has been a security feature of choice for Mobile Network Operators (MNOs) for many years, the information stored in the SIM card is used to authenticate and identify the user on the mobile network, in others Terms, the SIM card is a secure passport allow users to access mobile networks.

The SIM card is comparable to the EMV chip (Europay Mastercard Visa) on bank cards. As a result, financial institutions want to take advantage of the existing telecom infrastructure by offering to safely store credit card information on the SIM card at NFC payment platforms via mobile. In the near future, the memory area of the SIM card will be reserved only for the telecom operator, but it will be shared between several providers wishing to offer mobile payment applications (Transport, Banks, Parking, ...) (Figure 8)

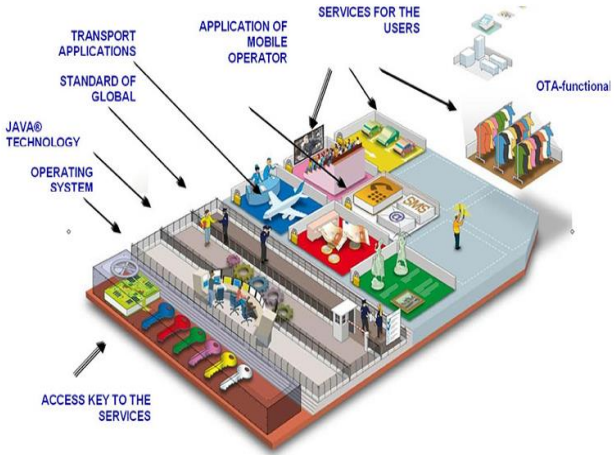

Fig. 8. The use of the SIM card by NFC applications

In this mode of operation, the NFC chip is not on the SIM card, but rather the NFC applications, for example, the application that validates transport tickets. Placing applications on the SIM card ensures high end-user quality of service. If it loses the phone and the SIM card for example, it is possible for the operator to disable the whole remotely, which reduces the risks (Figure 9).

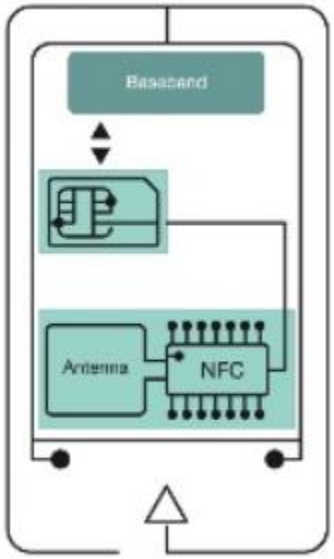

Fig. 9. NFC communication in SIM-Centic Mode

This will clearly give MNOs an important role in the ecosystem, as exclusive owners of the SIM card. The SIM-Centric architecture provides a clear advantage to the MNOs, they have the power to control any information installed on the SIM card, and therefore, financial institutions are obliged to collaborate with them [3].

The contribution of MNOs in the contactless mobile payment ecosystem has spawned new intermediary institutions called **TSM** or **Trusted Service Manager**, an independent entity responsible for the management of an element of Secure Element for mobile payments (Figure 10).

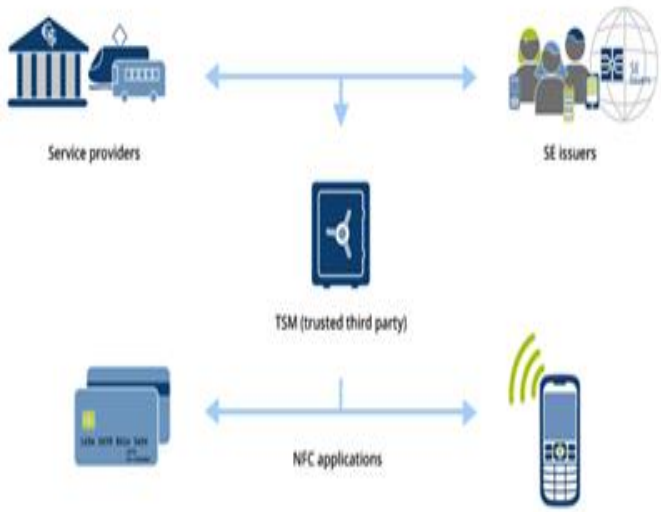

Fig. 10. Trusted Service Manager

The concept of TSM was initially introduced in 2007 by the Global System for Mobile Communications (GSM) to facilitate the adoption of NFC services (Figure 11). GSM is a trade

association representing more than 750 GSM operators in countries and territories around the world. The role of TSM is to provide multi-account services to various NFC mobile devices accessible through a variety of proprietary networks. A key element of the TSM role envisaged by the GSMA is that it is an independent entity serving mobile network operators (MNOs) on the one hand, and financial institutions, potentially banks, Transit cards, authorities, traders ... [4].

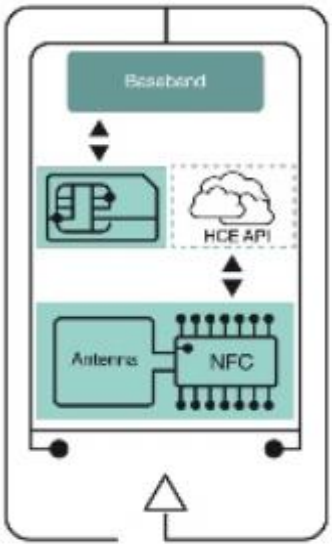

Fig. 11. NFC communication in HCE Mode

c) Host Card Emulation: Contactless mobile payment entitles MNOs and mobile device manufacturers to be major players in this ecosystem as owners of the secure element (SE), as long as the secure information is stored Way in a physical area, access to these locations always passes through these operators. Given that interactions are global, they need to maintain relationships among themselves to ensure the availability of their services via NFC, which makes it very complex to implement, hence the interest in a new architecture called Host Card Emulation or HCE (figure 11), which is a newer architecture introduced in 2013 for storing critical information in a remote location (eg the cloud) [5] [6]. This technology has been adopted by Google on its Android system from the KitKat 4.4 version, to allow the creation of contactless payment applications in a simplified way, without going through the operators and possibly without TSM [7].

d) Tokenisation: Since in HCE mode the secret data is stored in the cloud, recovery and enrolment of this information is still possible, and for security reasons the banks have thought of avoiding the storage of sensitive data in the cloud, but Only a part, is where the idea to set up a system of authentication based on tokens.

Fig. 12. Example of generating a token in a banking transaction

Tokenisation is a process by which the primary account number (PAN) is replaced by a substitution value called "Token" (Figure 12).

De-Tokenisation is the inverse process of changing a Token for its associated PAN value. The security of an individual Token is mainly based on the impossibility of determining the origin of the PAN by knowing only the substitution value [8] [9].

e) SD-Centric Mode: In SD-Centric mode, the Secure Element is included in a specific SD card (Figure 13), usually this card and offered by a service provider to its customers. The use of this mode is too restricted to some industrial applications.

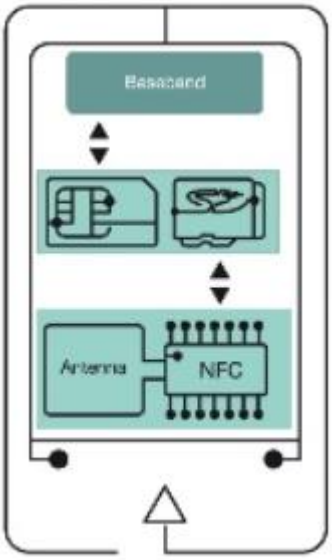

Fig. 13. NFC communication in SD-Centric Mode

2) Read / Write Mode: In this mode, the terminal behaves like a real NFC card reader (Figure 14), Android has set up libraries allowing reading and writing in these different tags.

Fig. 14. Read/Write mode

There are several cases of use of this mode, for example the reading of the information by approaching its mobile in front of electronic labels arranged on the street, on bus stops, monuments, posters... or on packages, Products or on business cards (vCard) ...

3) Peer To Peer Mode (Initiator & Target): This mode allows two mobile devices to exchange information, such as vCards, photos, videos, money, tickets, etc. A device with NFC technology is capable of exchanging information with contactless smart cards, but also with other devices equipped with this technology (Figure 15).

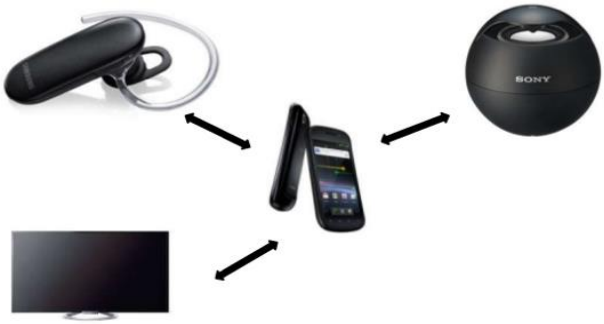

Fig. 15. Peer to peer mode

IV. Discussion

Our research on NFC technology began during the implementation of a mediation system for the payment of mobile services (Invoices, Tickets ...). For solid identification on an application, the Fido standard requires three authentication factors (something you know, something you have, no matter what you are). Thus we have introduced this technology as a means of physical authentication via an NFC card.

The study of NFC technology has shown us that it is possible to evolve our mediation system into a real contactless payment platform thanks to technologies at hand. This kind of platform can be used in several areas such as:

- Contactless Payment
- Purchase tickets.
- Management of loyalty points.
- Management of discount tickets.
- ...

Thus, in this study, we have established a state of the art of the different modes of operation of the NFC and RFID technologies, this allowed us to highlight several important points:

With regard to RFID technology, it is possible to set up an ecosystem for payment of contactless tickets. The deployment of such systems requires the use of electronic cards (Arduino, RaspberryPi, ...) equipped with an RFID reader. The limit is purely due to hardware, as smartphones do not support the RFID frequency band.

NFC technology appears to be more promising in terms of possible use cases. We concluded that it is technically possible to deploy contactless payment applications in the following ways:

Reading mode of writing tags.

Card emulation mode via the cloud.

Card emulation mode via SIM card

The third mode remains the most interesting in terms of portability and security, but since the SIM card always remains a property of the MNO's, and that access is only possible through them, Of the SIM-Centric mode imperatively requires the introduction of MNO's as an actor in the ecosystem.

Following this study, the next step of our work is the implementation of contactless ticket payment platform architecture.

V. Conclusion and Perspectives

Through this paper, we have presented an overall description of the different perspectives for the use of NFC and RFID technologies. In this study, we have concluded that it is possible, thanks to basic technologies, to develop very high value-added services Level, and especially for developing countries or the rate of banking remains low. We used NFC technology, first of all, as a means of physical authentication (something you have) on a mobile payment platform with three authentication factors, after, and thanks to this study we have Found that it is possible to exploit these technologies for the implementation of an architecture for purchasing NFC / RFID tickets by mobile. Prospects for the use of this type of ecosystem are very broad.

References

[1] "The History of RFID Technology", Bob Violino, http://www.rfidjournal.com/articles/view?1338, last visited: 04/09/17

[2] "NFC-enabled Handset Shipments to Reach Three-Quarters of a Billion in 2015", https://technology.ihs.com/533599/nfc-enabled-handset-shipments-to-reach-three-quarters-of-a-billion-in-2015, last visited: 04/09/17

[3] Ondrus, J. (2015, August). Clashing over the NFC Secure Element for Platform Leadership in the Mobile Payment Ecosystem. In Proceedings of the 17th International Conference on Electronic Commerce 2015 (p. 30). ACM.

[4] Cox, C., & Solutions, M. C. (2009). Trusted Service Manager: The key to accelerating mobile commerce. A First Data White Paper, 4-5.

[5] Prakash, N. (2015). Host Card Emulation. International Journal of Scientific and Research Publications.

[6] A. Martin and S. Dubois. HCE, Apple Pay. the shock of simplifying the NFC? Technical report, Galitt - white paper, 2014.

[7] Prakash, N. (2015). Host Card Emulation. International Journal of Scientific and Research Publications.

[8] "PCI DSS Tokenization Guidelines", Scoping SIG, Tokenization Taskforce PCI Security Standards Council, PCI Data Security Standard (PCI DSS),Aug 2011.

[9] "Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization", Smart Card Alliance Payments Council, Oct 2014.

[10] https://en.wikipedia.org/wiki/Duplex_(telecommunications), last visited: 04/09/17

[11] "Understanding the Requirements of ISO/IEC 14443 for Type B Proximity Contactless Identification Cards", Atmel Corporation, Rev. 2056B–RFID–11/05

[12] "Understanding the Requirements of ISO/IEC 14443 for Type B Proximity Contactless Identification Cards", Atmel Corporation, Rev. 2056B–RFID–11/05