EUROSMART

The Voice of the Smart Security Industry

Position Paper

NFC Trends

October 2009

Disclaimer

Eurosmart has taken reasonable measures to ensure the quality of the information contained in this document. However, Eurosmart will not assume any legal liability or responsibility for the accuracy, reliability or completeness of any information contained herein or for any consequences of any use.

INDEX

1. Introduction on NFC trends

What defines NFC?

Near Field Communication (NFC) is **a contactless technology framework enabling** proximity transactions between a consumer device and a reader. The main consumer benefit is the convenient “tap and go” gesture meaning that one only has to wave one’s card, phone or any other NFC-compliant device over the reader to perform the transaction. NFC is a short-range high frequency wireless communication technology which enables the exchange of data between devices in the range of up to 10 centimetres distance. The technology is an extension of the ISO/IEC 14443 proximity-card standard (aka contactless). The NFC technology is compliant with the current and future transportation and payment contactless ISO/IEC 14443 infrastructures as well as with other contactless applications such as loyalty, ID, access control, etc.

NFC incorporates a variety of standards including ISO/IEC 14443 Type A, Type B and Type C and ISO 18092.

ISO/IEC 14443 operates in the 13.56MHz RF band, half duplex, data exchange rates 106, 212, 424 and up to 848 Kbit/s with typical operating distance of up to 10cm (4 inches).

The core NFC specification is developed and maintained by the NFC Forum (www.nfc-forum.org), a standard organization created in 2004 for the purpose of leveraging the success story of mobile contactless services in both Korea and Japan.

Rationale of NFC vs. other Wireless Connectivity Technologies
Although NFC has a limited bandwidth (up to 848 Kbit/s), it brings attractive convenience and ease of use (unambiguous short range and single shot transaction) to most major connectivity technologies that have adopted it to simplify and secure devices pairing. This feature, called Out Of the Band (OOB) pairing, has been defined in the following standards:
- Bluetooth 2.1,
- Wi-Fi Protected set up (WPS),
- UWB protected set up.

Those specifications are also complemented by the NFC Forum Handover specification.

In comparison with Bluetooth, NFC is compatible with existing, widely deployed, contactless applications and infrastructures. It can also work when the host device is not powered by a battery (e.g. on a phone that may be turned off, a contactless smart credit card, a smart poster, etc.).

Target Use Cases
As defined by the NFC Forum, the core NFC use cases are:

- Connection of Electronic devices for Data Transfer – Peer to Peer (PC to Mobile, Mobile to Headset, MP3 Player to Music Station, others). This mode allows the connection of two devices that will communicate and exchange information (e.g., business cards, multimedia files, etc).

- Access to Digital Content on the move – Reader/Writer (read information from Smart Posters, tags). In this mode the NFC device activates a passive contactless tag and reads out the stored information and takes action accordingly.

- Card Emulation Mode - Mobile Payment and Ticketing based on Smart Card Security. The NFC device behaves like a contactless payment card or ticket.

Applications

NFC has the potential to make the old idea of mobile wallet a reality, combining different personal services in the mobile phone, such as payment and loyalty cards, tickets, business cards, etc. Leveraging the 3 basic use cases and the promise of the mobile wallet, the most targeted NFC applications are currently:

- Mobile ticketing in public transport — an extension of the existing contactless infrastructure.
- Mobile payment — the device acts as a debit/ credit payment card.
- Smart poster — the mobile phone is used to read RFID tags on billboards in order to get info on the move.
- Connectivity pairing — The process of activating Bluetooth on both sides, searching, waiting, pairing and authorization will be replaced by a simple "touch" of the mobile phones.
- Electronic ticketing — airline tickets, concert/event tickets, and others
- Loyalty and couponing
- Access control and electronic keys — car keys, house/office keys, hotel room keys, etc.
- Identity documents

Applications architecture

Based on the early implementation phase of the NFC technology, several Secure Element architectures are available to address the special needs of customers and markets in terms of secure storage of both applications and credentials. All the solutions require the NFC controller to communicate with secure devices. The difference in the solutions can be seen in the host of the secure application:

- Secure Element on UICC (SIM): Smart Card device that hosts the secure application (Banking, Transportation, others) in addition to the standard functionalities of the SIM Card. The UICC SE has been standardised by ETSI and supports the Single Wire Protocol (SWP) to communicate with the NFC controller.

- Embedded Hardware Secure Element: Hardware tamper-resistant component based on Smart Card technology that is soldered in the Mobile Phone. Several field trials have been done based on this solution, which has a maturity level comparable to the UICC.

- SD Card Secure Element: Hardware tamper-resistant component based on Smart Card technology that can be removed from the Mobile Phone based on standard form factors (e.g. microSD™). Solutions with very complex integration level (i.e., SE and antenna in the SD Card) are available that only use the Mobile Phones as User Interface Device. Other solutions merge completely with the NFC environment of the Mobile Phone.

- Secure Element features integrated in the Mobile Device Baseband Processor: Implementation of a secure memory area in the Baseband Processor. The secure memory is

totally separated by firewall from the other parts of the Baseband Processor to be tamper-resistant. Right now this is a more long-term solution, as the security level does not yet match mainstream SEs.

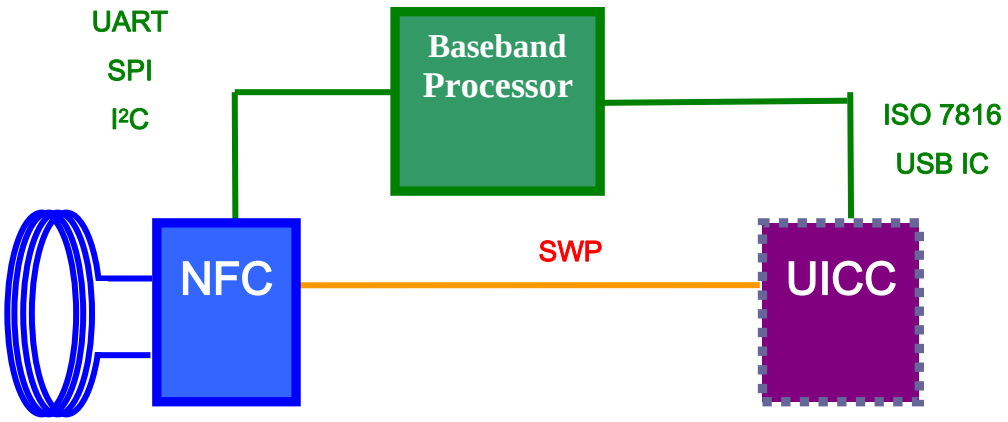
All these architectures are relying on the same standards for application development, OTA provisioning, remote personalization and life cycle management. As a consequence, the NFC applications will share the same development environments, architectures … whatever the Secure Elements, thus ensuring a maximum re-use and interoperability of service providers' investments.

The most common execution environments for NFC applications are:

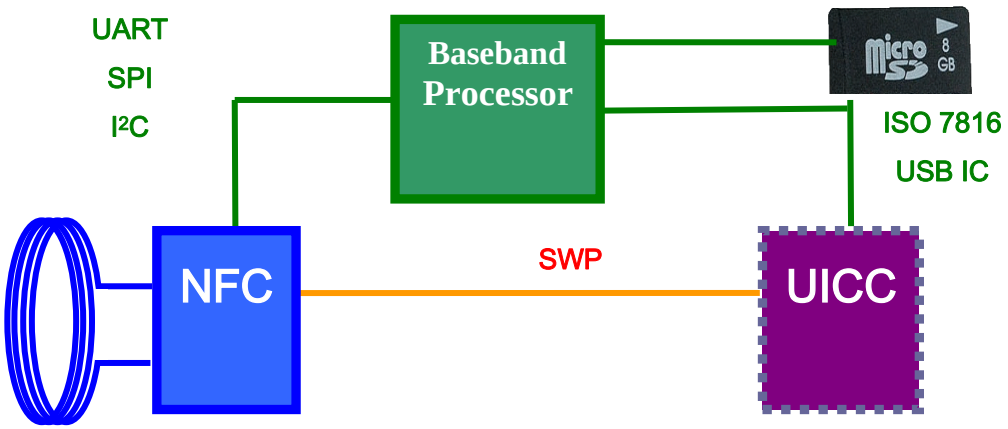
- Java Card™ and Global Platform in the SE: Java Card™ is the main execution environment for secured applications in the SE and could rely on SIM Toolkit or the Smart Card Web Server for implementing a man machine interface. Global Platform will be used as the main life cycle management standard whatever the SE.

- Java for Mobile in the handset: the man machine interface of the NFC applications is likely to use Java for Mobile in most phones (except Smart Phones) with its NFC related API: JSR257 for NFC services and JSR177 for exchanges with the SE. The rise of smartphones will see the emergence of similar API in OS like Android, RIM, iPhone, Symbian, LIMO, Windows Mobile, etc…

NFC with Secure Element on UICC (Universal Integrated Circuit Card) or SIM Card
The NFC chip communicates with the UICC via the Single Wire Protocol (SWP) which has been an ETSI standard since 2008. The UICC will host the applications in a trusted environment. These applications can be enabled by the NFC chip. Since the UICC will also operate as standard SIM card in the Mobile Phone, services like over the air (OTA) updates (provisioning, personalization, life cycle management) can be performed. This offers the possibility to install additional applications (payment, ticketing, access, loyalty…) on the UICC and to increase the services of NFC products in the field. A pre- and post installation of applications and user information is possible.

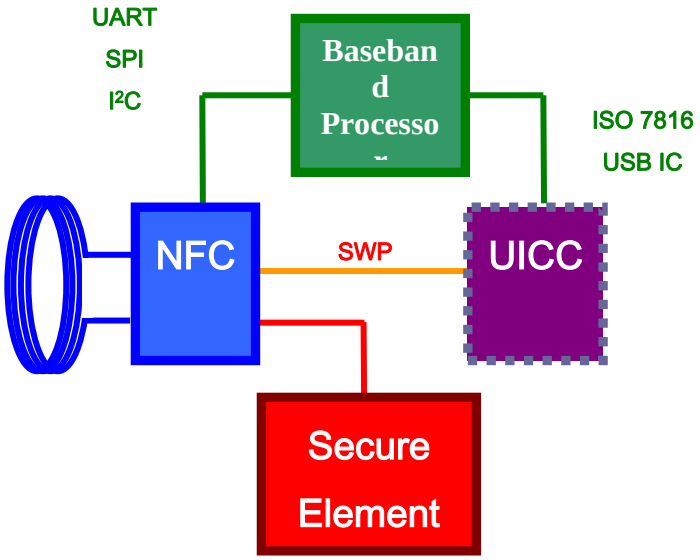


NFC chip communication with microSD™ Card



This NFC approach combines in the form factor microSD™ cards a Smart Card Security Chip and optional external Flash Memory. This form factor is known by many handheld electronic devices such as digital cameras, mobile phones, car radios, computers, MP3 players and many others. The smart card chip of the microSD™ and UICC have the same security level. The microSD™ will host the applications in a secure environment that can be enabled by the NFC chip. Both security chips microSD™ card and the UICC act as independent secure elements with different interfaces to the NFC device. Target applications are payment, ticketing, access, and others. Since the OTA update of the microSD™ card will be possible a pre- and post installation of applications could be supported.

NFC communication with Embedded Hardware Secure Element

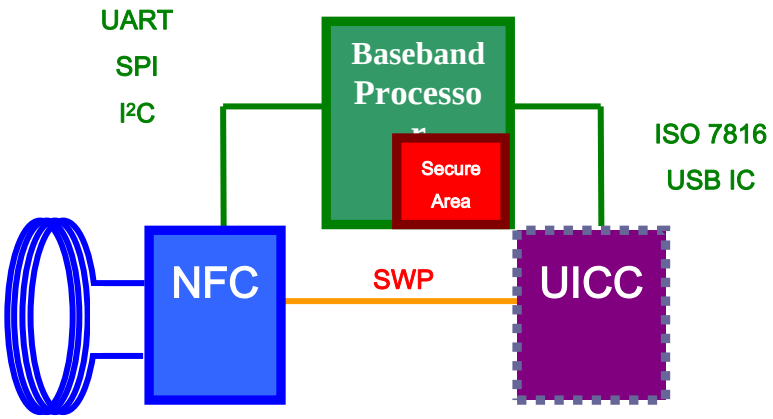


As in the previous solutions, the Embedded Secure Element (eSE) is based on the smart card technology. In this case the eSE is embedded in an electronic packaging and is

hardwired to the mobile phone (and thus not removable). This is the main difference with the UICC and microSD™ cards solutions. The eSE has the same security level as the other solutions and works independently from other secure elements in the mobile phone environment. The NFC controller can enable the secure applications stored on the eSE. Target applications are payment, ticketing, access, and others. In future the eSE could additionally also host the MTM (mobile trusted module) functionality helping to secure the mobile phone.

Each of the target applications could be installed based on the users request during the life cycle of the mobile phone.

NFC Communication with Secure Element features embedded in Mobile Device Baseband Processor



This approach will not require an additional device for the storage of the secure application (e.g. microSD™ cards or Embedded Secure Element or the UICC). The host of the secure application will be the baseband processor of the mobile phone itself using portions of secure memory and processing.

The current Secure Baseband Processors (SBP, based on such technologies as ARM's Trust Zone) could functionally be used as a secure element. But secure baseband solutions have not yet been subject to security certification nor regulatory approval in payment contexts and do not reach a comparable security level as a dedicated security controller. The NFC controller can enable the secure applications stored in the SBP. Target applications are payment, ticketing, access, and others.

The SBP could be addressed OTA for installation, personalization and updates of the secure applications.

2. Technological Status

A rich standards ecosystem has quickly flourished around the NFC promise. The highest impact industry bodies have been the NFC Forum, ETSI and the GSM Association. Other ones have also been instrumental in defining key brick or additional services around NFC like Global Platform, Wi-Fi Alliance and the Bluetooth SIG.

GSM Association
This leading association of Mobile Network Operators has published from January 2007 to November 2008 a set of four position papers, requirements documents and technical guidelines defining a functional architecture with the SIM Card as the main Secure Element.
The GSMA has notably been the first to draft the TSM (Trusted Service Manager) functional role as the cornerstone of the NFC architecture.
The latest GSM Association requirement document, published in November 2008 and aiming at handset vendors, is setting the pace for most of the NFC handsets to be released in 2009.

NFC Forum
The NFC Forum was created in 2005 with the aim of defining a global standard to replicate the mobile contactless success stories in Japan and Korea. The Forum has defined three main use cases for NFC:
- The Reader/Writer mode, which is supported by four defined type tags and their data format (NDEF and RTDs),
- Peer to peer (implemented by the LLCP specification) ,
- Card emulation.

The NFC Forum has published the following specifications:

- **NFC Data Exchange Format (NDEF) Technical Specification**: Specifies a common data format for NFC Forum-compliant devices and NFC Forum-compliant tags.

- **NFC Forum Tag Type Technical Specifications**: The NFC Forum has mandated four tag types to be operable with NFC devices. This is the backbone of interoperability between different NFC tag providers and NFC device manufacturers to ensure a consistent user experience. The operation specifications for the NFC Forum Type 1/2/3/4 Tags provide the technical information needed to implement the reader/writer and associated control functionality of the NFC device to interact with the tags. Type 1/2/3/4 Tags are all based on existing contactless products and are commercially available.

- **Record Type Definition Technical Specifications**: Technical specifications for Record Type Definitions (RTDs) and four specific RTDs: TEXT, URI, Smart Poster, and Generic Control.

- **NFC Forum Connection Handover Technical Specification**: Defines the structure and sequence of interactions that enable two NFC-enabled devices to establish a connection using other wireless communication technologies. Connection Handover combines the simple, one-touch set-up of NFC with high-speed communication technologies, such as Wi-Fi or Bluetooth.

The following candidate specifications have been published for comments:

- **Digital Protocol Candidate Technical Specification**: This specification addresses the digital protocol for NFC-enabled device communication, providing an implementation

specification on top of the ISO/IEC 18092 and ISO/IEC 14443 standards. It harmonizes the integrated technologies, specifies implementation options and limits the interpretation of the standards.

- **NFC Logical Link Control Protocol (LLCP) Candidate Technical Specification**: The specification defines an OSI layer-2 protocol to support peer-to-peer communication between two NFC-enabled devices.

ETSI

ETSI, the reference standard body for mobile telephony, has been active in defining the SIM Card as the standard Secure Element. Since 2006, ETSI has defined the Single Wire Protocol (SWP) interface between the UICC and the NFC chip (aka CLF) and the Host Controller Interface (HCI) to act as a router protocol between the SEs, the mobile handset and the NFC chip.

Both protocols have been through first integrations and field tests under the umbrella of the GSMA and lead MNOs in the past 3 years (the first SWP + HCI handsets were released in Q1 ’06 and more than 15 handsets have been released so far). SWP and HCI are now in a reasonable stage of maturity, still undergoing minor revisions, and have been implemented by the major SIM Card and NFC chips vendors.

Global Platform

This standard body is defining the reference protocol for secure application provisioning, remote personalization and life cycle management. The GP protocol is to be integrated in the Secure Element, whatever the format (UICC, embedded SE or SE in SD Card).

Bluetooth SIG

In July 2007, the Bluetooth standardization body adopted NFC as a simplified pairing protocol (aka OOB Pairing or Out Of the Band Pairing) in the Bluetooth 2.1 release. A pre-version has already been implemented by device vendors like Nokia and Parrot (loudspeakers and picture displays).
A usual Bluetooth pairing process requires up to 12 key strokes to be completed, while NFC-enabled pairing greatly simplifies the process, requiring only one key stroke (Yes/No selection).
This specification has been complemented by the NFC Forum Connection Handover Technical Specifications.

Wi-Fi Alliance

The Wi-Fi promotion body has adopted NFC in January 2007 as one of the lead pairing mechanisms in its WPS (Wi-Fi Protected Set-up) requirements. NFC WPS is aiming at simplifying the pairing and security management of Wi-Fi networks. This specification has been complemented by the NFC Forum Connection Handover Technical Specifications.

Certification Processes

The NFC Forum is setting up a compliance program to be ready to certify NFC devices from the second half of 2010. This program will integrate the following NFC Forum specification set:

- Reader mode with all the 4 types of NFC Forum tags and data format (RTD, NDEF),
- Peer to peer (LLCP),
- Analogue, Digital and Activity (e.g., Protocol Switch, etc…) specifications.

Before the readiness of the compliance program, the NFC Forum is organizing timely Plug Fests with NFC vendors.

Major applications based on card emulation will require going through a specific certification program for both the handset and the SIM (if the UICC is used as the SE), this applies for Payment and Transport applications while other ones will depend on the application vendor or service provider certification policy. Those certification processes will enforce the interoperability of the SEs + Devices couples with the installed base of the application's readers.

Both Visa and MasterCard propose certification programs for mobile devices embedding payment application. Those programs target the usual Application, Analogue and Digital parts. Payment certification, or part of it, is likely to merge in the EMVco association on the medium term.
The situation is not as clear for transport applications as each transport authority has its own certification process. It is likely that each NFC device will have to undergo those processes.

The SE, should it be the UICC, an embedded SE or a SD-based SE, will be submitted to usual security certifications for its embedded applications (e.g., Cast for MasterCard, Visa Risk for Visa, etc).

For the Secure Element, both ETSI and Global Platform propose a declarative certification process using test suites and tests tools to be published.

Device availability
In the past 4 years, the target segment for NFC has been mobile phones further to the success stories of mobile contactless integration developed in Japan with Docomo and Korea with SKT and KTF. However, NFC's potential has harnessed the creativity of consumer electronics, laptops and numerous other device vendors.

Mobile Phones
The first "proto-NFC" mobile phone was the 5141 engineered by Nokia and unveiled at the GSM World Congress in February 2005. Since then, most of the mobile phone vendors, and among them the Top 5 owning nearly 80% of the market, but also numerous Tier 2 (like Sagem) and Tier 3 (in Taiwan and China like BenQ, ZTE, Huawei and the like), have prototyped NFC phones in both GSM and CDMA standards.

The road to maturity has been quite long as both the standards and the use cases were a moving target until end 2008. But also the complexity of integrating NFC had to be learned the hard way through a long and painful experience curve. The lack of clear Telco and Service Providers requirements have also been a major factor in delaying NFC adoption.

Most of the leading handset manufacturers have now acquired the *NFC Touch* through 2 or 3 prototype phones that have fuelled the more than 100 NFC trials around the world.

Commercial handsets from the Top 5 vendors are now forecast for the end of 2009 to support commercial launches in 2010.

Laptops & PCs
As often in the PC market, Innovation is entering through the laptop or accessories segments.
The leading use case to integrate NFC in the PC world is to offer a reader for leading contactless applications (like on-line payment access or transport ticketing) or a new interface for access control, relieving the integration of contact Smart Card readers.

A few laptops, like the Vaio from Sony, and a couple of accessories like desktop keyboards are now offering an NFC interface.

Consumer Electronics
There have been quite a number of prototypes and demonstrations of NFC enabled TVs (including CE giants like Sony and Philips) with use cases around DRM management, payment of VOD, etc.

A major use case in the CE domain is the easy pairing of either Bluetooth devices or Wi-Fi networks (using the Wi-Fi protected set-up from the Wi-Fi Alliance) to support the growth of the connected home paradigm (home media servers, multimedia set top boxes and DSL boxes, etc…).

Other Devices
USB keys or dongles have started the integration of NFC some two years ago, the leading use case being to offer a low cost NFC reader for PCs with different purposes serving contactless applications like strong authentication for on-line banking or purchase of transport tickets over the Internet. Vendors like Neowave in France or SCM in Austria have been pioneering this segment.

More innovative devices, like the TazCard from TazTag which is a standalone multi-application wallet with a touch-screen interface presented at the latest CES show, are about to be released and already raising significant interest from large industry players.

Bridge Products
There is a palpable *NFC frustration* in the mobile ecosystem that is pushing some players to think out of the box and innovate with new NFC-enabled concepts. So called "*bridge products*" (i.e. *bridging* current phones with future NFC phones) could be segmented in two categories:

- Passive accessories: those are mainly "stickers" performing only card emulation (emulation of a contactless card) and derived from the smart card form factor. Those stickers are mostly targeting mobile handsets with applications such as contactless payment, loyalty or identity.

The sticker is independent from the phone and does not offer the interactivity and Man Machine Interface of a fully fledged NFC solution. Those stickers could be sourced from a growing number of vendors, mostly smart card players or actors of the electronic packaging segment.

The Micro SD Card format is another form of accessory raising interest from the ecosystem. Although limited to card emulation, like the sticker, it is however connected to the handset execution environment, offering a richer interactivity and user experience.

- Active accessories: more sophisticated appliances performing both card emulation and reader mode. This solution requires a connection to the mobile phone which could be made either using Bluetooth or via a physical port like USB.

Those appliances have two purposes:

1) Kick start the NFC usage by incorporating basic NFC features (e.g., tag emulation only) to support a limited use case or service (e.g., payment or transport only or vertical niche applications).

2) Decouple the NFC feature from the handset in order to push services or business models independently from the Mobile Operators.

3. Uses Cases driving NFC

1. Introduction

The Near Field Communication technology initially emerged in the mobile phone segment to offer convenient end user services based on contactless applications such as contactless payment or contactless ticketing. A simple 'Touch and Go' was enough to make a transaction.

Now, other applications and market segments have adopted the NFC technology, thus increasing the demands of services. NFC operating modes such as Tag or Card Emulation, Reader and Peer-to-Peer increase the use of this technology in new market segments, contactless devices and applications.

2. Use cases in mobile phone

The mobile phone world is the first segment to adopt NFC technology by promoting **contactless payment** and **contactless ticketing** and using the existing infrastructures in the field.
Other applications have now appeared. The most common one is **Bluetooth Pairing** which can set up Bluetooth communication extremely fast through a simple reading of the Bluetooth identifier stored as NFC tag information.
The typical Bluetooth accessories addressed with this use case are mainly the headset, camera and also consumer devices such as printer, photo-frame or camera.

The **Smartposter** application is also one of the driver applications for NFC. This use case describes the capability to read any information stored in NFC Tags on a poster or in a NFC device. For example, reading a URL in a poster can launch the Internet connection and provide access to internet services such as tourism information, shopping, reservations (flight & train schedule, hotel vacancies, emergency numbers, etc…) expanding the user's experience. If the NFC Tag offers a larger memory (typically 1kByte and more), complete services (as opposed to only links to services) can be read, such as gift vouchers, promotion tokens, access rights for events, product information, thumb nail pictures, ring tones, longer text and even small applets. A key advantage is that this can be done even if the NFC phone does not have network connection, e.g. in subways or buildings, and also no airtime charges would apply for the user.

Considering that a mobile phone is an everyday tool that everyone keeps in his pocket, it seems really useful and easy to replace our traditional **physical Access Card** or **Cafeteria Card** with an application located in an NFC mobile phone running in card emulation operating mode for any company having an installed contactless infrastructure.

In addition, today the mobile phone is used as an electronic agenda and can store personal information such as a business card. The **fast exchange of this kind of information** between two NFC devices is now a driver of NFC applications using the Peer-to-Peer operating mode.

In reality, any proximity or vicinity contactless application able to be integrated in a mobile phone and driven by the operating modes such as Tag / Card Emulation, Reader or Peer to Peer could drive a new NFC use case.

3. Other electronic devices

If the mobile phone segment remains the first one which has started using the NFC technology, other electronic devices are starting to integrate this technology. The objectives are the same as for the mobile phone market, giving the end user and the device providers more flexibility, convenience and user-friendly applications.

One of the most important and interesting segments emerging today is the PC computer market and mainly the laptops due to the large number of devices used in the field and the really large number of accessories available. In this domain, the **IT security access** and **Corporate ID application** are the main drivers as well as all the applications able to simplify connections to peripherals such as PC screens, keyboards or mice. **WIFI setup simplification** is also a key element of the NFC technology adoption.

The second segment in the full NFC development phase is the contactless reader market which increases reader capabilities in terms of RF communication in PC-Link readers as well as Point-of-Sale or Handheld readers.

As usual, the main driver applications remain the **contactless payment**, **the control access** and the **IT corporate right access**.

To enlarge the deployment and use of NFC technology, some system integrators are starting to offer new form-factors such as a USB-NFC dongle which can drive a reader application when the dongle is connected to a PC (**IT right access**, or **data download** and **data update**) and card emulation applications when the dongle is used in standalone mode (ticketing, payment or loyalty).

In addition, the capability to **connect and/or initiate a service** by using NFC technology also gives system integrators the opportunity to offer many different kinds of module devices for a large variety of markets. We also notice that the portable music devices, gaming, TV or also automotive markets can be interested by the NFC technology where the Bluetooth or WIFI pairing may be a key factor of the improvement of use.

As an example of the automotive demand, the **pre-configuration or personalization of the automotive accessories and parameters** through an NFC mobile phone provides a highly practical use case for end users.

NFC applications are expanding and depend now only on the capability of the manufacturers to integrate contactless technology in their devices.

4. Impact on the value chain

As NFC is bringing new actors (e.g., TSMs) and multi-application into the ecosystem, the value chain is becoming more and more complex and this has led to the slow development of the market up to now. Nevertheless, this brings new services, and new business opportunities based on the combination of multiple market segments.
The first and most active domain can be identified as mobile phones today. It will expand existing smartcards or tickets usage to mobile payment or mobile ticketing applications. On top of this new use cases or business models from reader/writer or NFC peer to peer perspective will be deployed in mobile phone.

The figure below depicts the Mobile handset ecosystem and the NFC value chain.

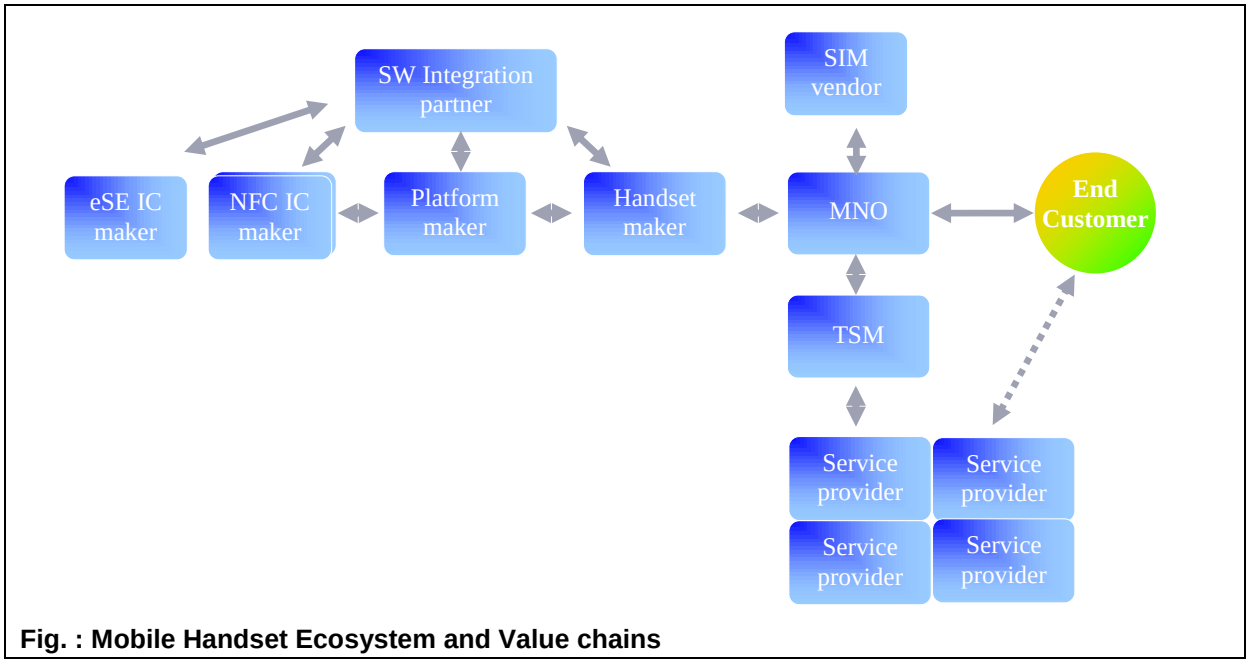


Fig. : Mobile Handset Ecosystem and Value chains

The PC market is starting is to benefit from some traction due to a significant move from contact readers to contactless technology.

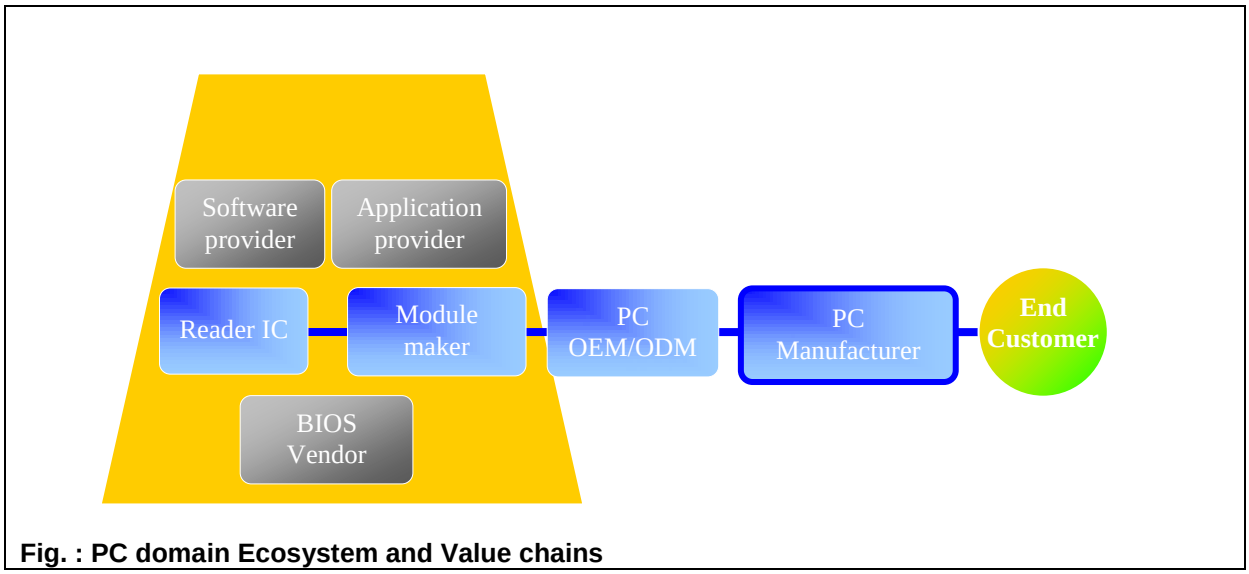


Fig. : PC domain Ecosystem and Value chains

4. Works in Progress

For many years now NFC has been seen as one of the most promising technologies in the telecom world. Mobile Operators, and also banks, transport operators and all kind of Service Providers from all over the world have expressed their deep interest for the new services that will be provided to mobile phone users. It explains why NFC is probably one of the technologies for which the most pilots or trials have been made (more than 100 worldwide in the past 5 years). Nevertheless, we can notice today that outside Japan and Korea, few commercial services have been launched so far. Consequently, we could suppose that obstacles or missing links of a technical and business nature are still slowing mass commercial roll out of NFC services.

1.1. The technical vision

From a technical perspective, one can only observe that a huge amount of work has been done, both in standardization committees and in products development. Nevertheless, some obstacles seem to still remain. This chapter aims to highlight the points that could still be considered as obstacles for NFC mass roll outs.

a) Standards

Since the first NFC proofs of concept, standardization committees have been very active in creating a frame allowing the development of NFC products. Today, the main technical bricks are standardized and available to support mass roll out. However, standardization is still ongoing in Global Platform and ETSI to allow MNOs and Service Providers to have the highest flexibility and convenience level. The finalization of last NFC related standards is expected for end 2009, as well as Global Platform amendment C.

b) Required adaptations for legacy infrastructures

In order to meet the full NFC promise, it is crucial for NFC devices to be compatible with the existing contactless infrastructures (i.e. public transportation, payment, etc).

This raises challenges. First, with contactless, one contactless card was generally hosting one contactless application. This results in a great heterogeneity of technology, which NFC actors have to bypass in order to provide end-users with a seamless view of the contactless world that surrounds them. Secondly, contactless applications were not designed to be used in an NFC environment. In particular, means have to be found to allow contactless applications to be used with a user interface and to be accessible via Over-The-Air mechanisms.

Major payment and transport schemes have undergone the process of learning how to address those issues in the past few years and we are now seeing viable and mature specification sets adapted to NFC.

c) Certification

As NFC is going to allow the use of sensitive applications, especially banking applications, the industry is preparing the mobile equipment to be compliant with adapted NFC certification schemes. Secure Elements, for example, should have a similar certification process as in the current contactless banking market. Discussions between MNOs and banks have revealed that the existing banking certification schemes should be adapted for NFC, mainly because

of the multiple applications the NFC Secure Element will host. In order to reach this objective, a new working group has been created in Global Platform: The requirements for an NFC certification scheme should be available from mid 2010.

d) Interoperability

This is the last important technological challenge for the NFC industry. MNOs and Service Providers should be guaranteed the highest level of flexibility. Therefore, they can expect that any phone will work with any SE and that any SE is able to host any kind of NFC applications and support interactions with any kind of Trusted Service Manager. Thus, the industry should be able to ensure an end-to-end interoperability. In addition to implementing the same NFC standards, the industry will have to offer a complete validation scheme so that the technical elements necessary to run NFC services will be completely transparent for Service Providers and MNOs.

1.2. Business vision

So far, MNOs, banks and transport operators used to have separate markets. Now with NFC, all those actors will target the same NFC end users. Therefore, business agreements have to be found between them in order build a new NFC market.

a) Ecosystem creation

From the ecosystem creation perspective, France is certainly a leading market for NFC. In this country, NFC organizations have existed for more than two years to define a global frame for NFC business. For example, in AEPM (Association Européenne Payez Mobile), MNOs and banks have defined together the services they want to offer to customers and the roles and responsibilities of each actor. Ulysse and Ergosum are similar organizations that did the same respectively for transport and retail. This has definitely created a solid ground to develop a profitable NFC market. At the same time, it shows how important those cross-market projects are.
This 'geo-market' consortium approaches are being adopted all over Europe with major initiatives in Turkey and Norway and the more global Pay Buy Mobile program from GSM Association, embedding 52 mobile operators on a worldwide basis.

b) Business models

Ongoing business discussions are being conducted bilaterally between service providers and MNOs on two major modes:

- Memory rental: The service operator (e.g. a bank) will pay a monthly fee to the MNO (in case of UICC) in order to rent some space in the NFC secure element (e.g. the UICC) to install and personalize the trusted application in a secure domain to enable the given proximity service (e.g. payment applet…)

- On use: The more the end user will use the NFC secure element to travel, pay… the more money the MNO will get. In fact, the service operators will share a small percentage of his revenue with the MNO

The March 2009 announcement by Orange and Barclaycard to launch NFC services in 2010 reveals that such agreements are on-going and likely to flourish in the course of 2010.

5. NFC Trends

Three scenarios can be foreseen regarding the development of the NFC market, with a focus on Payment and Mass Transit, given the current status of both the ongoing Pilots and the current level of readiness of the technology and standards. Contactless Payment and Mass Transit are essential NFC market drivers: their success is a condition for the entire NFC ecosystem success.

1- Mass Transit Operators are likely to be first to deploy NFC ticketing solutions, leveraging on local agreements (multi-MNOs) to offer a new service, complementary to Contactless Cards and already in use in more than 30 cities above 1 million inhabitants around the world. Technology-wise, NFC solutions are capable of supporting the dominant solutions already in place for Contactless mass Transit (Mifare, Calypso, Felica). This scenario is pretty much only limited by Handsets availability, which should no longer be an issue in the course of 2010, with full speed maturity in 2011.

2- Large Retailers (i.e. major distributors such as Wal-Mart, Carrefour, Metro, etc...) are seeing NFC as an opportunity to accelerate the currently booming trend of disruptive payment services. Retailers are already very active in deploying their own MVNO brands and thus have already mastered the art of managing relationships with MNOs and distributing handsets to consumers. Retailers are ideally positioned to become prime service aggregators (with combined mobile, payment and loyalty services) and NFC payment brings clear value to their customers.

Retailers have a much faster innovation cycle time than traditional Financial Institutions and that scenario is possibly the fastest path to go-to-market for NFC. They also have a global role in both issuing the contactless services and deploying the acceptance infrastructure (contactless POS).

3- Geo-markets consortiums for mobile payment (such as Payez Mobile in France and local initiatives around the Pay Buy Mobile GSMA initiative) are being formed between MNOs and Banks with a key world in mind: INTEROPERABILITY, a condition for success. This scenario is being executed as we speak and is a key element complementing scenarios 1 and 2. As we speak, contactless payment cards are a very strong success worldwide: by the end of 2009, more than 100 million of such cards will have been delivered.

Those 3 scenarios are very closely linked: scenarios 1 and 2 can speed up a process that is currently perceived as slow because Retailers and Mass Transit Operators are crucial to educating consumers about NFC transactions.

NFC needs however to be a win-win-win scheme: the end-user saves times and gains more convenience; the merchants experience a higher average transaction; the Bank captures a portion of the cash payment market, etc...

The best case scenarios see NFC mass deployment as early as 2010 but beyond Payment and Mass Transit, multiple other simple NFC services (smart posters, peer to peer, Bluetooth pairing, etc) who do not require a nationwide secured transaction infrastructure should deploy faster.

6. Eurosmart as an enabler of the NFC ecosystem?

The core function of Smart Secure devices is to manage identities, digital assets and transactions. Key services such as activation and de-activation of services, applications provisioning, and identity life cycle management are going to be crucial enablers of the NFC ecosystem. The benchmarks will always be interoperability, security, convenience and ease-of-use.

Eurosmart members are the experts at not only building Smart Secure Devices, but also at managing devices life cycle from inception (inside personalization centres) to the field with secure over-the-air (OTA) solutions.

Smart Cards and Smart Silicon manufacturers are already key partners of the major NFC actors (Banks, MNOs, Mass Transit Operators, Handset Vendors and Retailers) and are ideally positioned to operate trusted services such as applications provisioning, personalization and life cycle management.

Eurosmart is thus the legitimate representative of the actors who are ready and willing to fuel the NFC ecosystem with key enablers.

Among the key missions of Eurosmart to contribute to the NFC success will be:

- Contribution to EU level coordination (promotion of success stories across Europe) and actions (more EU NFC funded trials)
- Coordinated actions to key vertical standard bodies where Eurosmart members are involved
- NFC market analysis

Is 2010 the NFC year?

The mobile industry is reaching the end of a 5-year cycle dedicated to the creation of the core NFC standards, integration and fine tuning of the technology in mobile devices and trialing of NFC services.

Consumer feed-back has been so far very positive, with acceptance levels above the 85% mark, among the highest in the mobile telephony segment so far.

All the bricks, enablers and know-how are now ready to deliver smart NFC devices and services.

The current next step is the definition and roll out of innovative services from mobile network operators and contactless service providers (e.g., banks, transport operators, etc).

We believe the initiatives to make NFC a success are now in the hands of telecom and contactless service providers with the roll out of consumer-attractive and business-sustainable NFC services.

Eurosmart members are committed to taking a place at the forefront of those initiatives.

What is Eurosmart?

Eurosmart is an international non-profit association located in Brussels and representing the Smart Security Industry for multi-sector applications. Founded in 1995, the association is committed to expanding the world's Smart Secure Devices market, promoting Smart Security standards and continuously improving quality security applications and services.

Eurosmart members are suppliers and manufacturers of smart cards, semiconductors, terminals, equipment and technology for Smart Secure Devices, system integrators, application developers, issuers, associations, laboratories and independent experts. They work into dedicated working groups (communication, marketing, security, electronic identity, new form factors, and prospect emerging markets).

Eurosmart is acknowledged as representing "the Voice of the Smart Security Industry" and is largely involved in political and technical initiatives as well as research and development projects at the European and international levels.

For more information, please visit www.eurosmart.com

Contact:
Eurosmart General Secretariat
Rue du Luxembourg 19-21
B-1000 Brussels
Tel: + 32 2 506 88 38
Fax: + 32 2 506 88 25
eurosmart@eurosmart.com