15

Services, Use Cases and Future Challenges for Near Field Communication: the StoLPaN Project

Carlo Maria Medaglia[1], Alice Moroni[1], Valentina Volpi[1],
Ugo Biader Ceipidor[1], András Vilmos[2] and Balázs Benyó[3]
[1]CATTID- "Sapienza" University of Rome,
[2]SafePay
[3]Budapest University of Technology and Economics
Italy

1. Introduction

Over the last couple of decades, the mobile phones have become more and more integrated in everyday people's lives. According to the International Telecommunication Union (ITU), at the end of 2009 the penetration of mobile phones in the developed economies was 97% (ITU, 2009 as cited in European Payments Council [EPC], 2010). Not only the penetration has grown, but also functions and services accessible from mobile phones have improved, thanks to the growing availability of communication technologies and to the miniaturization of electronic components inside consumer's devices.

As an example, thanks to location technologies such as GPS, the mobile phone can nowadays be used to locate a person's position and, thanks to wireless communication technologies, such as Wi-Fi, GPRS and UMTS, personalized content can be delivered on the person's device. Automatic identification technologies such as RFID are not excluded from this process of integration and convergence of communication interfaces in the worldwide most popular electronic device. In fact, one of the latest short-range auto-ID technologies, named Near Field Communication (NFC), can be described as the integration of an RFID HF reader into a mobile phone, moreover allowing the device to act as a contactless smart card. NFC originates from RFID technology, but differently from the latter it supports bidirectional communication, making possible to overcome the distinction among tag and reader device. From the technical point of view, NFC operates within the unlicensed Radio Frequency band of 13,56 MHz and it is used to provide easy short-range connectivity to different electronic devices. As described in the standards (ISO/IEC 18092, ECMA-340 and ETSI 102.190), the communication distance is up to 20 cm but the real operating distance is strictly related to the antenna dimension and design: if integrated in a mobile phone, the antenna has to be very small and so the communication distance is typically 2-4 cm. The standard for contactless smart cards (ISO/IEC 14443) is also related to NFC operational mode: data stored on the NFC secure chip can be read in the same way proximity cards OF proximity cards.

As mobile phones are the most popular personal devices worldwide, extending them with an RFID reader and a "card emulation mode" makes it possible to create a wide set of applications and services, from mobile payments and ticketing, to mobile social networking and pervasive advertising services. The main goal of companies and merchants is to give people services they really need, moreover improving their experience as consumers or users.

2. NFC services and use-cases

As it enables several ways of use, NFC is a really adaptable technology. It can operate in three communication modes, based on three different types of interaction between the mobile phone and other NFC-enabled devices (Figure 1).

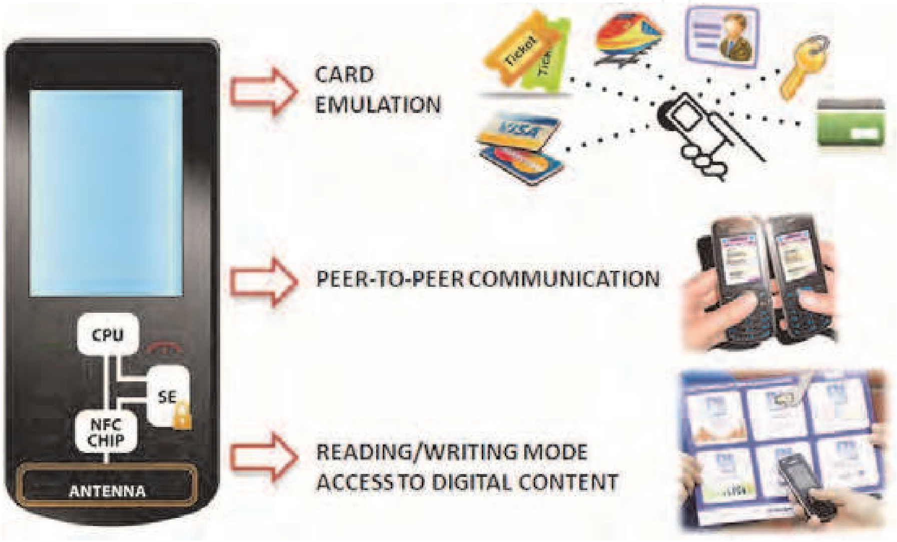


Fig. 1. NFC communication modes

The first one is the above mentioned “card emulation mode”, that is compatible with existing contactless infrastructure (based on ISO/IEC 14443 standard). In a card emulation mode scenario, the mobile phone communicates the sensitive information stored inside an internal secure, tamper-resistant chip (Secure Element - SE) linked to the NFC module by moving itself close to a reader, for example a validation machine on a bus or a POS terminal in a shop, etc. In this way the mobile device acts as an authentication token for enabling services that require high level of security, such as mobile payment, mobile ticketing, mobile identity, access control and so on. Compared to a traditional card support normally used for enabling the above mentioned services, the mobile device offers additional capabilities, first of all a display and a keyboard, as well as the possibility to connect to the Internet by a mobile network, via GPRS/UMTS or via Wi-Fi.

The second type of interaction is peer-to-peer communication between two NFC-enabled devices (for example two NFC mobile phones, or an NFC phone and a printer, or a camera). As they touch together, they can exchange data and information such as the business card or the identification key necessary to quickly initiate a configuration (e.g. pairing) with Bluetooth or Wi-Fi connections.

The third and last type is the read/write mode that enables the mobile phone to initiate a service by reading the information stored in a RFID tag, maybe added to a smart poster situated in a strategic place, for example the bus stop, the shopping centre or the pub. The information stored in the tag consists of a few kilobyte: it can be a URL address, a phone number or a short text message. When the mobile phone touches the tag and reads the data inside, the related application on the device can connect the mobile browser to a web page that can also be a social network profile.

The interoperability and the easy integration with different wireless and wired technologies favor the use of NFC in a multi-application scenario. Moreover, if used within a smart poster or combined on a kiosk or a totem, NFC can be a very useful technology to clear the information overload giving the right information in the right place at the right moment.

Over the last half-decade, several pilots involving services based on NFC technology have been conducted all over the world. One of the first pilot was hosted in Caen, France, in 2005: it enabled two-hundred mobile phone users to interact with NFC smart posters, as well as with car parking machines and ticket terminals. Once the NFC was tested from a technical point of view, the consumers acceptance was checked and the results have showed that end users like the quickness and convenience of NFC technology (Kannainen, 2009).

Currently, the most tested services are those involving NFC in card emulation mode, such as proximity payments and ticketing. They usually follow a client-side payment and validation model based on offline micro-payment transactions using the existing contactless infrastructure.

3. The role of the StoLPaN consortium in the development of NFC technology

3.1 Research challenges and objectives

Although NFC is one of the most promising technology in the near future, one of the main problems in creating an NFC mass market is the lack of application level standardization and interoperability: while the low-level standardization process has been already completed by standardization bodies such as ISO/IEC, ETSI and also by NFC Forum, as detailed in the following paragraph, there are still significant differences between NFC implementations (devices, operating systems, etc.) that have to be considered.

The StoLPaN (Store Logistics and Payment with NFC) consortium, which includes companies and research centers all over Europe, has worked on overcoming standardization and interoperability issues, mainly dealing with application level standardization, creating in this way a transparent technical environment for the Service Providers and a homogeneous user experience for the customers.

The two major research challenges the consortium faced during a three-year project (2006-2009) co-funded by the European Commission within the 6th Framework Programme were related to the multi-application operation in the mobile handset and the elaboration of a smart retail procedure and payment process based on auto-ID technologies such as RFID and NFC. The whole project aimed to reach a consistent user experience contributing to the industry progress.

The StoLPaN Project was based on three main research questions:

- What is the technical environment that can ensure the integration of NFC based services and applications provided by different Service Providers into a single device, irrespective of its features and operating system?
- How can a smart retail scenario including payment process be implemented making use of auto-ID technologies such as RFID and NFC?
- What business model can support a mass adoption of NFC based services?

Besides investigating the research challenges and related questions, the following objectives were part of the defined goals of the StoLPaN project:

- To elaborate transparent logistical and technical processes that can be relied on in the various business interactions that provides a tool for dynamically managing individual service portfolios even with international scope.
- To develop a handset-independent JME-based mobile host application in order to provide seamlessly multiple services.
- To demonstrate the effectiveness of the proposed proof-of-concept solution in a smart retail environment.

3.2 Overview of the NFC standardization process

In July 2006, when the StoLPaN Project started, the NFC low-level standards already completed were the Near Field Communication Interface and Protocol-1 (NFCIP-1), about "modulation schemes, codings, transfer speeds, and frame format of the RF interface, as well as initialization schemes and conditions required for data collision control during initialization" [ISO/IEC 18092 (ECMA-340), 2004] and the Near Field Communication Interface and Protocol-2 (NFCIP-2), about "the mechanism to detect and select one communication mode" between Card Emulation, Peer-to-Peer and Reader/Writer modes [ISO/IEC 21481 (ECMA-352)].

The ECMA International started to work on Near Field Communication standard in 2002. An apposite Task Group was charged to define signal interfaces and protocols. In December 2002 Near Field Communication Internet Protocol-1 (NFCIP-1) was adopted as Standard ECMA-340, which came to a second edition on December 2004. ISO/IEC adopted the NFCIP-1 as a standard in December 2003.

On the other side, the first, historical edition of ECMA-352 that specifies the mechanism to select one communication mode between Card Emulation, Peer-to-Peer and Reader/Writer modes was published in December 2003 and approved as an ISO/IEC standard (ISO/IEC 21481) in 2005. ECMA published the second edition of the ECMA-352 (Near Field Communication Interface and Protocol-2) standard on June 2010.

Also the European Telecommunications Standards Institute (ETSI) is involved in the standardization of NFC technology. More in detail, the ETSI's Smart Card Platform group (ETSI/SCP), which deals with the SIM card specifications, has worked on specifying the interface between the SIM card (but in this context it is better to refer to the UICC – Universal Integrated Circuit Card, which is the physical support on which the logical module known as Subscriber Identity Module, or SIM, is present) acting as a Secure Element and the NFC chipset stored in the phone (ETSI TS 102 622, ETSI TS 102 613). The first standard adopted by ETSI SCP, approved in 2007, was related to the physical connection between the UICC and the NFC chip: as there was only one free contact in the UICC, the connection with the NFC chipset was required to use one single wire and, due to this reason, was named "Single Wire Protocol" (SWP). In 2008 ETSI also approved a protocol standard that specifies how chips embedded in NFC mobile phones communicate between each other. This standard is called "Host Controller Interface" (HCI).

Nevertheless, the interoperability remains a crucial issue in the NFC ecosystem. Some of the most used contactless technology compatible with NFC, like MIFARE system developed by NXP or FeliCa by Sony, are currently proprietary standards, and use their own security solutions. Anyway, since Nokia, NXP and Sony were the first to developed the NFC lower layer communication, when the open standard NFCIP was developed, the backward compatibility with the proprietary solutions was assured (Mayes & Markantonakis, 2008).

Although the physical layer of the NFC technology could refer to well-known established international standards available to enhance interoperability, the application standardization scenario was more uncertain. A number of researchers and associations has worked on defining a standard in implementing NFC applications and services. The NFC Forum, a non-profit industry association that promotes the use of NFC short-range wireless interaction in consumer electronics, mobile devices and PCs (NFC Forum, http://www.nfc-forum.org/home/) has defined a common format for message encapsulation, called NFC Data Exchange Format (NDEF), for exchanging data between an NFC Forum Device and another NFC Forum Device or an NFC Forum Tag (NFC Forum, 2006). In 2007 the GSM Association (GSMA), a global trade association representing more than 700 mobile network operators across 218 countries of the world launched two initiatives for the development of NFC applications into a common ecosystem: the Mobile NFC initiative, supported by nineteen MNOs, which have worked together to develop a common vision on Mobile NFC services, promoting the development of a stable and efficient ecosystem and preventing market fragmentation (GSMA, 2007a, 2007c) and the Pay-Buy-Mobile project, supported by thirty-four of the world's largest MNOs (GSMA, 2007b), focused on contactless and mobile payment scenario, trying to standardize the operational approach with NFC technology.

Another relevant initiative for promoting the development of mobile payments based on contactless and NFC technology in Europe was conducted by the AEPM (Association Européenne Payez Mobile), an association established in October 2008 in France. The AEPM has published a set of specifications that define a common approach for enabling mobile contactless proximity payments. The technical solution proposed by both the GSMA and the AEPM is based on the UICC as the Secure Element for a mobile payment transaction.

The Mobey Forum (Mobey Forum, 2010) and the Global Platform (Global Platform, 2006) have respectively published guidelines and technical documentation focused on possible alternatives and multi-application architecture for the Secure Element.

Focusing on the evolution of the market scenario during the years covered by the StoLPaN project, the first commercial NFC-enabled mobile phone was launched on the market by Nokia (Nokia 6212, which supports UMTS connectivity) in 2008. One year earlier, in 2007, Nokia launched the Nokia 6131 NFC, a fully integrated NFC mobile phone with GPRS connectivity, which was still a prototype. Even Motorola, Samsung, LG and Sagem, other stakeholders of the sector, developed their own NFC prototype models. At that time there was still uncertainty about the Secure Element's position. Nokia first built it into the handset (embedded Secure Element). Now, encouraged by GSMA, it seems that most of the handset manufacturers accepted to put the SE on UICC. The NFC ecosystem moves all around this issue and the related business and operating models driven forward from competing forces (manufacturers, MNO's, banks, etc.).

4. How the StoLPaN consortium contributed to the industry progress

Under the scenario described above, the StoLPaN consortium contributed to the ecosystem and industry progress by working on the management and distribution of services in a dynamic and open scenario, presenting a proposal for the post-issuance procedures for multi-application SEs (StoLPaN consortium, 2008a). Moreover, the consortium has detailed the technical environment necessary for the dynamic management of NFC services, building a proof-of-concept prototype of the NFC wallet application (StoLPaN consortium, 2008b) and demonstrated the effectiveness and efficiency of the solution in a smart retail environment (StoLPaN consortium, 2009a).

In the following sections, we will give an overview on the main findings of the StoLPaN project in reference to the three abovementioned issues.

4.1 Dynamic application management on SEs

The StoLPaN consortium identified the post issuance and application management as the key issues to be faced to offer users a variety of NFC applications on the same device and building so a real ecosystem. In the current section we are describing the technical model for the dynamic card content management of Secure Elements placed in a mobile handset.

The StoLPaN model provides a solution for dynamic application management that can be uniformly used in local, as well as in global operations, both between parties with consolidated contractual relationship, but also between ad hoc business partners.

One of the main challenges of the new mobile NFC service environment is that the present card issuance models are not designed to support the dynamic post issuance personalization process because the Service Providers:

- have absolutely no control over the cards – we also refer to them as Secure Elements (SEs) in the following – on which their application should be stored, except making a decision of using them or not;
- have no control over the other applications stored in the same Secure Element;
- may not know personally their clients, and may not have the chance for a physical contact with either the Secure Element Issuer or with the user.

The existing technical diversity calls for early standardization of the post issuance and personalization process, otherwise local island solutions will prevail and the technology will not be capable of adequately serving several hundred million users and thousands of Service Providers expected when the NFC services will reach critical mass.

The new logistical and technical model that ensures the necessary openness and interoperability fulfils the following criteria:

- open relationship between the Service Providers, the Secure Element issuers and the Users;
- technical transparency for the Service Providers;
- service homogeneity for the user.

It is possible to establish one single logistical process for loading, personalization and life cycle management of applications that is technologically agnostic and supports all types Secure Elements, even multiple ones, in the communication devices. In this environment the user can freely decide which Service Providers and what services to use, and can even enjoy the services of multiple Service Providers. The result is free access to the customer base of the multiple SE issuers, and improved economics of developing NFC services.

4.1.1 Issues to consider

The first issue that has to be taken into account for providing dynamic card content management of Secure Elements is related to the complexity of the mobile NFC value ecosystem. In fact, main characteristics of the service environment are as follows:

- There are potentially many Service Providers who would place their applications on the Secure Element in the mobile handsets and there are potentially multiple Secure Element issuers in any countries.
- The Secure Element is an external condition for all the Service Providers, without any possibility of influencing its technical parameters, with only a “take it or leave it” choice.

- Users are mobile and may wish to use NFC services even if they are abroad. They may also wish to dynamically change the service portfolio they use even after the issuance of the Secure Element, adding services here and there and deleting others when they are not needed any more.
- A number of Service Providers are global and prefer to have uniform solutions for the applications deployment and operation, irrespective of the specific market where the application is delivered.
- Even if the various NFC applications have their own specifics and requirements, they need to share the same Secure Element and must coexist side-by-side, and eventually interoperate.

There are many constrains in the mobile NFC world which are unknown for either the Service Providers or the Secure Element issuers in their current operations. This is a new way of doing business, without anyone being able to substantially influence the service environment and with the necessity of cooperating with even unknown partners. There is a need for a transparent logistical model and a technical solution that can ensure uniform procedures for the parties involved, where they do not necessarily have to negotiate and elaborate the details of each and every interaction and where even previously unknown business partners can seamlessly realize the procedures of application deployment and management. Without such an approach, the NFC ecosystem will not prevail, and will not be satisfactory business model and an user friendly, valuable service for the customers.

Another relevant issue is related to the already discussed need of application-level interoperability: the industries working with NFC technology such as ETSI and GSMA are now busy addressing the many different technical issues. However, application interoperability has not been set as a target by any standardization body. Being able to hide handset and NFC platform specifics, so that any application can be loaded on any handset, will allow NFC services to be easily deployed worldwide, addressing millions of consumers. Just this aspect makes a good enough business case for the majority of the Service Providers to launch their services on NFC-enabled devices and will lead to the success of NFC.

The service distribution needs to be defined, too. There is a number of actors involved in the NFC value chain but their roles and form of cooperation is not adequately defined. It means that the distribution of any NFC service application requires special, individual agreements between the partners involved.

The target of the StoLPaN research and development activities is to support the market to develop the application environment to a level where all interoperability issues are solved. We have reviewed the majority, if not all, NFC related standards, use cases and business models. We have then condensed the wide range of requirements into a few preconditions, processes and interfaces and presented our findings in white papers (StoLPaN Consortium, 2008a, 2008b). The research carried out by the StoLPaN consortium led us to conclude that, to support quick proliferation of NFC services, the industry has to achieve a homogeneous, dynamic service environment which would mean that even after the issuance of the cards any services can be loaded onto virtually any Secure Element and managed through the whole life cycle of the application. In the subsequent sections we will introduce a logistical and technical process that provides a solution for these requirements.

4.1.2 Dynamic card content management and roles within the ecosystem

Before describing the logistical process that will contribute to the establishment of a truly global, interoperable NFC service environment based on a standardized dynamic card content management process, we need to clarify what we mean for card content management and to describe the roles necessary to build up the NFC ecosystem.

First of all, let's set what we mean for card content management. In general, there are two types of content management:

- **card content management** which includes the establishment/deletion of the new Security Domain, as well as the application loading and personalization of the smart card application;
- **application content management** which covers the product/portfolio management of the Service Provider.

This section is focusing on card content management, while the complementary application content management process will be discussed in par. 4.2. The solution elaborated below is explained in reference to a Secure Element, which can indifferently be a SIM card, an embedded chip or an SD card as well. The concept discussed in this section also provides the algorithm for a selection process in case of multiple Secure Elements deployed in the same mobile handset. It is the industry's – industries' – task to elaborate such standards in the NFC domain that, if followed, would provide a transparent environment for both the service providers and for the users. Right now, when there are only few commercial handsets on the market, when only trial and pre-commercial NFC services are operating it is the right time to work on these standards without hurting the commercial or financial interest of the parties involved. It would be a great mistake to miss the present opportunity for standardization, for the elaboration of uniform solutions. If not done properly the result will be a more complex and more expensive NFC service environment.

The proposed card content management process is quite complex, but also very flexible with various roles/functions included. We have identified the functions necessary to complete the process, but the actual actors in these roles will always be situation driven.

First of all, we have defined a set of *primary roles*. The complete service scenario cannot be performed without these roles (actors) however one single actor may assume more than one role in the process. The roles (actors) and their relationships are shown in Figure 2.

The primary roles are defined as follows:

- *User*: The User is the person who initiates the request for the post issuance and personalization by selecting the application/service for use.
- *Secure Element Issuer*: The Issuer of the Secure Element is the entity who controls the SE, it has the right to decide over the utilization of the storage capacity of the SE. To exercise these rights the SE Issuer needs to be in possession of the secret key(s) that allow general control over the management of SE. It has the right to define the rules about who, when and under what conditions may utilize storage space on the SE, or may deploy card content onto the SE.
- *Service Provider*: A Service Provider may be anyone wishing to deploy/manage a service application on the Secure Element. There should not be made any distinctions between the Service Providers if they comply with the industry standard security and SE Issuer specific business conditions. Service Providers can be large service operators, like banks, or transport operators for ticketing applications, but they can also be retailers for their loyalty and other programs as well as authorities for various ID cards, etc.

Besides the primary roles described, in order to provide the full functioning, economic and convenient service, the following *support roles* needs to be considered:

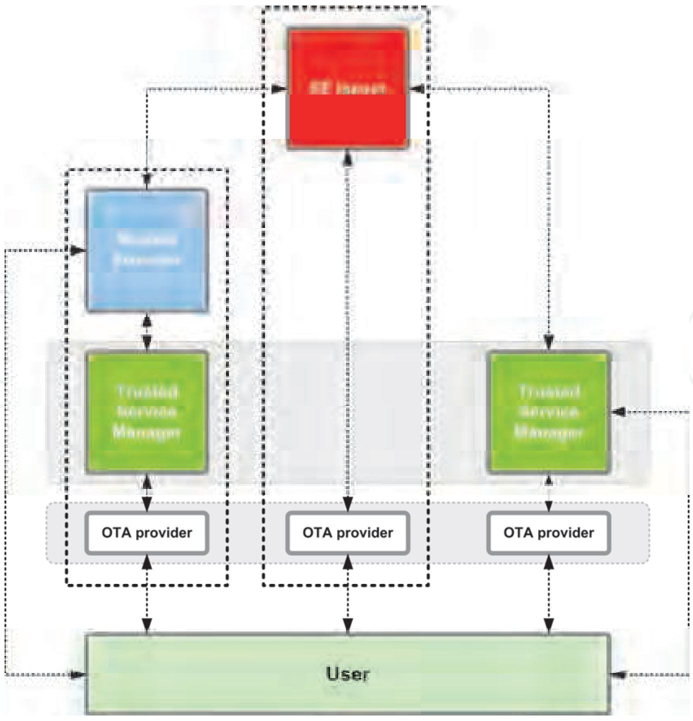


Fig. 2. Roles within the NFC ecosystem

- *OTA Provider*: The Over-The-Air (OTA) Provider is an entity who provides remote access to the Secure Element, enabling the key value added feature of the post issuance and personalization procedure. OTA identifies a service, but at the same time it is also used as a common name for various communication technologies all enabling secure data communication between a Secure Element and a back office architecture. From our perspective, the technical implementations of OTA services are transparent and do not affect the proposed solution.
- *Trusted Service Manager/Trusted 3rd Party (TSM):* As we have already discussed, the NFC technology will be able to support such added value services that are not possible, not even considered in case of the traditional card based contact or contactless (RFID) applications. Service Providers having performed their activities for years may not be able to change the way they act, the functions they provide, but still may want to participate in the new form of service operation or to enhance the services they offer without the need to change existing core processes. The way to solve this conflict is to involve a Trusted Service Manager, who can provide the technology and service support that is necessary for accomplishing these objectives. The Users are also facing a challenge presented by the availability of a large number of applications on a single or in a more complex situation on multiple Secure Elements. The services need to be managed, and to be protected: this is a time consuming and sometimes potentially difficult activity that many Users do not want to bother with. Again, a 3rd party such as the Trusted Service Manager can help the User supporting this activity. The two roles, TSM for the Service Provider and TSM for the User, have different requirements and specifics but they are not exclusive, even the same TSM may act in either position for different parties. It is important to keep in mind that we strictly treat the TSM as a service support function and not as an entity whose tasks would be to solve technical imperfections in the provisioning of the service.

- *Application Issuer*: The application issuer supplies the application that implements and fulfils the business requirements of Service Providers. It is able to guarantee secure interoperability between the card and the card acceptance device. Sometimes the Service Provider itself is the application issuer too.

In reality, there will be many Service Providers offering contactless services and requiring online application management support. There will also be many SE issuers, but most probably a number of other actors too. Some roles will need to be filled, in case of each and every post issuance personalization interaction, for example there is always a User for the service and a Secure Element Issuer providing access to the SE. Although the involvement of the additional actors in the support roles is optional, there is nothing that would prevent the involvement of even multiple actors in one single transaction, all acting in various capacities for either the User, and/or the Service Provider and/or the SE Issuer. While the support functions are required, they do not necessarily need the involvement of additional actors as simple technical infrastructures can perform the OTA and the TSM activities.

4.1.3 The proposed card content management process

While it is not realistic to expect that one concept will satisfy all the service needs, or all the preferences of the Users and Service Providers, most probably there will be several co-existing business models; it is important that all the actors involved can be served andsupported all can be served and supported with the below described technical process, resulting in a uniform service environment.

The process initialization can have different forms, as in the visionary NFC world users can find information about services they like in many ways on multiple channels:

1. The user opens up a newspaper and finds an interactive advertisement promoting a service on which there is an RFID tag. A simple touch of this smart poster hands over all the necessary info to initiate registration and deployment of the service.
2. The user may also browse the Internet with his phone and when he finds something he is interested in, a link helps him in initiating a service relationship.
3. The same service can also be located using a PC. While browsing, the user opens up the advertisement, enters his phone number, which triggers an SMS containing the service specific information.

The ways are endless. However, one important remark is that the originator of these requests is always the User, in a pull-based interaction model. This is important to avoid unsolicited services pushed on the User's mobile phone.

Once received the service request, before the application installation can take place, the Service Provider has to collect information on the targeted device in order to be able to perform the remote card content management procedure. In this phase the proposed service environment needs to be evaluated, the SE Issuer needs to be identified, and the potentially available remote support services need to be defined as well.

More in detail, the information required contains details about the:

1. *NFC device*: The Service Provider and the Secure Element issuer need to identify the end-user device for providing remote management.
2. *Secure Element*: The Service Provider needs information on Secure Element's Card Product Life Cycle (CPLC) to find out the Issuer of the targeted Secure Element and also to evaluate the security environment of the SE itself.
3. *Secure Element Issuer*: The automated contact information of the SE Issuer or a pointer to it are also required.

In the described procedure, it is supposed to store the reference data respectively on the Secure Element (in case of multiple SEs, each SE stores its own specific information) and in the handset's operating system. This information is sent to the Service Provider for evaluation through a message generated by an application on the User's device that is addressed to a specific address of the SP (for example an URL), or to its associated TSM partner, where it can be processed automatically. This relationship is transparent for the users, they do not need to know how the Service Provider delivers the service.

Considering the message received from the User, the Service Provider can decide whether the User's technical environment satisfies its requirements and, in case of multiple SEs, which one it prefers as a storage space/runtime environment for its application on the base of technical, security and financial considerations. The message received may also contain the User's preference in terms of SE selection, which the Service Provider should take into account. Following the evaluation of the technical information, the SP either starts the card content management procedure for the selected SE or informs the User that for some – identified – reasons the NFC service application cannot be loaded onto its mobile handset.

At this point, the Service Provider or its TSM partner can identify the Issuer of the Secure Element selected for use on the basis of the information contained in the service initiating message sent from the User's mobile device. This piece of information is actually the only data element necessary for starting the automated card content management process that is not available at this moment either on the Secure Element or in the mobile phone.

On the base of the information received, the SE Issuer can perform the requested post issuance processes. These processes include the generation of Security Domains (SD), the application loading installation and deletion. The SE Issuer also generates specific keys for the Service Provider to ensure exclusive access to the new SD and to the application. To deliver these tasks to the User, the Issuer may use third party service providers – OTA providers, Certification authorities, TSM – but may also perform these tasks itself using its own in-house infrastructure. Once the requested operations are performed and the required data is loaded onto the card, the Service Provider or its TSM receives from the SE Issuer a confirmation response, together with the specific keys to access the Security Domain.

Alternatively, depending from the SE Issuer policy, the Service Provider may get an exclusive access to its application and assigned Security Domain in order to manage its own application without any interaction of the Card Issuer. This requires special management rights that are described in the Global Platform specifications (Global Platform, 2006).

We are describing a process where, by providing the necessary technical information about the User's environment to the Service Provider, this is enabled to launch an automated process with the designated Card Issuer for the seamless establishment of a new Security Domain and for the loading of a new application.

Figure 3 gives us an overview about the entire card content management process.

Technical cornerstone of the dynamic card content management process is that there is a set of technical parameters and information in possession of the User that could facilitate an automated procedure to establish a new Secure Domain for any selected Service Provider. If the necessary information is provided to the SPs, as well as to the Issuer of the SE, they will be able to manage between themselves a seamless deployment process.

According to our proposal, the SE shall contain a reference (for example an URL) to the current Issuer of the specific Secure Element. This could be a pointer to a database which maintains the list of SE Issuers or even a direct access information to the Issuer itself.

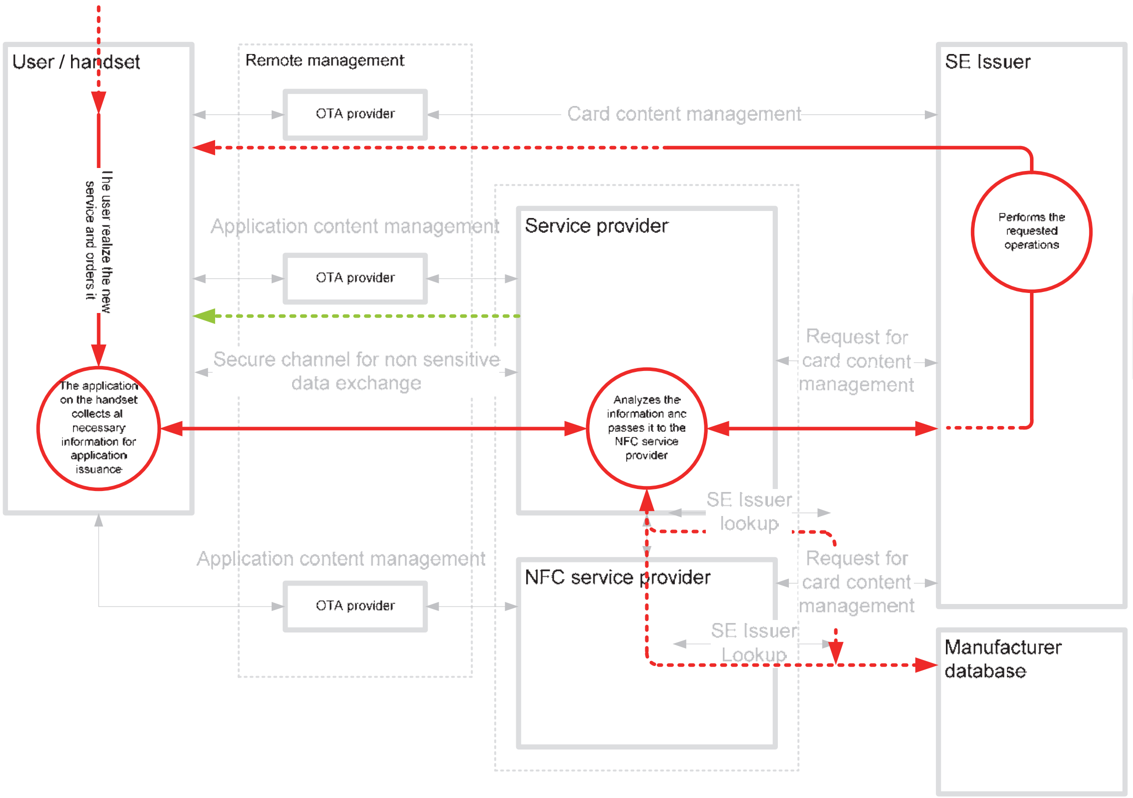

User / handset
The user realize the new service and orders it
The application on the handset collects al necessary information for application issuance
Remote management
OTA provider
Card content management
Application content management
OTA provider
Secure channel for non sensitive data exchange
Application content management
OTA provider
Service provider
Analyzes the information anc passes it to the NFC service provider
SE Issuer lookup
NFC service provider
SE Issuer Lookup
Request for card content management
Request for card content management
SE Issuer
Performs the requested operations
Manufacturer database

Fig. 3. Overview of the card content management process

Another issue to consider is the SE selection in multi SE environments. Although the currently available NFC handsets support only one Secure Element, we also clearly see the potential that in one NFC handset there may be multiple SEs hosted. We think that including more than one Secure Element provides more flexibility, allows differentiation of security levels and also increases the business potential of the technology. At this point, given a free choice between a SIM storage and another SE, we cannot judge which alternative will be preferred by the Service Providers. There may be a number of technical, security and business issues which will influence the decision.

The actual choice between the SEs will partly be influenced by technical factors, but currently unknown business conditions will have a major impact on these decisions. If a simple algorithm should drive the selection, the following issues need to be considered in the sequence listed here:

- SE capacity availability;
- Security level of Secure Element;
- Controllability of the Secure Element;
- Cost;
- Business considerations/existing business relationship between the parties;
- User preferences.

Last but not least, the customer support is a crucial issue on which attention is needed. As described among the roles listed, the present model introduces a new TSM to support the customer in situations where the management of multiple applications stored in the SE(s) may be just too complex or time consuming. The best example for such a situation is when the handset is lost or when migration is necessary from one SE to another one. Instead of letting the User do this task alone, which is practically blocking and reordering each and every application again, a simple request to the TSM may solve the problem. However, to get to this point, two aspects have to be clearly seen.

First, the User needs to decide that he needs such support for himself, because the Service Providers' various TSMs will not be able to provide him this function, because each of them will only have information about the application(s) it manages. Second, the application(s) need to contain some sort of summary information that, if provided to the TSM, will describe the application in satisfactory details that allows to identify the Service Provider, the User and his technical environment, and also the application itself, but it still does not provide details that could be misused.

4.2 NFC wallet application or the HOST application

In the current pilot operations, the service portfolio contains only a limited number of services (use cases) hard coded into the mobile handset. These implementations do not allow the removal or the insertion of any new or unused NFC service. Without this service portfolio dynamism, these operations effectively limit the penetration of NFC services.

According to the StoLPaN consortium, in order to quickly spread the adoption of NFC services among end-users, they need a simple way of downloading and removing NFC services to and from their mobile device. People want a dynamic NFC platform on their handset that hides the complexity of changing NFC services. They also want a generic, simple and easy way to manage their NFC service portfolio. Service Providers also need NFC platforms in handsets which can dynamically accept their applications, to minimize the barriers to their services. Secure Element issuers need a platform that help them sell space on their SE in a dynamic manner. Technically, this can be managed by a dynamic NFC wallet (also referred to as HOST) application stored on the mobile phone regardless of the model used and based on a modular architecture that provides a transparent and seamless environment to the Users, the various Service Providers and the Secure Element issuers.

A proof-of-concept prototype of this wallet application, along with a related smart retail scenario demonstration, has been designed and implemented by the StoLPaN consortium (StoLPaN consortium, 2008b, 2009a).

In this section we are describing the technical implementation of the StoLPaN HOST application.

4.2.1 Seamless NFC environment enablers

The StoLPaN project has defined the functional and non-functional description of a dynamic NFC environment and reviewed its potential lifecycle. This complex analysis resulted in the development of a prototype where dynamic application management can be demonstrated and further analysed. The analysis determined three important elements which need to be defined in an open, dynamic NFC environment.

Common issuance processes - The Global Platform defines the smartcard content management procedures implemented in most Secure Elements, explaining how a card issuer can manage card content. However, it does not explain how an application provider can contact the card issuer. This is a clear issue in a dynamic environment. In addition, none of the current standards define how the interoperability of the User Interface elements of the service and the actual hosting of the wallet platform can be assured. Section 4.1 describes a procedure for resolving these issues. It shows how the relationship between a Secure Element Issuer and a Service Provider can be determined using existing protocols and standards and how this offers a communication channel for exchanging wallet compatibility information. An official standard addressing these issues would help the industry to make dynamic NFC wallets commercially available.

Application selection - Once applications are installed on a mobile handset, they are registered in the Card Manager. Each application in this registry is active by default. This means that they are able to respond to a call from the card acceptance device. Today, the decision on which application to use in a defined context, for example which banking card to use for a transaction, is made by the acceptance device, based on the matched priority list of the Secure Element and the acceptance device. Application selection by the user can be fulfilled by creating a single element list of the available applications. The procedure for application selection is not fully defined in any standard or recommendation. What is even more disquieting is the expected growth in complexity caused by introducing multiple service types on one card, the plug and play use of multiple Secure Elements and the presence of multiple wallets in the same system. As a result, application selection is a very complex subject. The current section does not intend to cover the topic in detail, but without a detailed standard on application selection it will be impossible to build a smoothly functioning NFC wallet service.

Application development - Most NFC services have a software element that contains the user interface and/or its structure. This code is hosted on a certain platform (a midlet based wallet core, a Smart Card Web Server implementation or similar) which represents the user interface. The link between the user interface and the application resides in the Secure Element. The developer creates the user interface element and the non-sensitive application logic of the service so that it works smoothly with the hosting platform. This is only possible if the developer knows all the hosting platform interfaces in detail. There are many ways to ease and speed up the developers' work. Out of the many good practices we would like to emphasize two things. One is that the hosting platform should contain many pre-coded modules that the developer can use as building blocks via open APIs. This has the additional benefits that it makes the certification process much faster and controllable. The other is the creation of Software Developer Toolkits to make the use of these building blocks even easier and at a higher quality level.

The development of a well-defined platform can significantly decrease the cost of NFC service development and hence bringing faster penetration of NFC services.

4.2.2 General wallet requirements

Here below are described the general requirements to build up the NFC wallet application:

- **Remote management**: The platform/wallet must provide the necessary functions to enable remote application management. This covers all the functions which are necessary for remote or proximity service delivery and deletion and for the continuous operation of the services as well.
- **NFC events handling:** Several use cases require the handling of RFID/NFC hardware events from the application runtime environment. Therefore, the hosting platform must contain an application programming interface that allows NFC applications to access information on external contactless targets such as RFID tags or other NFC devices.
- **Security features**: The targeted application environment for NFC applications should provide a reusable set of functionality that encompasses the security needs of the

various use cases implementations. It should contain authentication, security policy settings and cryptographic services. In the dynamic service portfolio, each use case implementation must comply with the specification and security rules provided by the wallet manager to ensure a homogeneous wallet environment. This goal can only be achieved through well specified usage of the pre-certified security services embedded in the hosting platform.

- **User Interface** (UI): The wallet/platform should provide a homogeneous NFC user experience with similar design principles and opportunities for accessing all known added value functions. It must be possible to personalize the interface on multiple levels, to reflect the preferences and the specifics of service providers and of the wallet manager.

4.2.3 Solutions for seamless NFC issues – the StoLPaN HOST

In order to define the requirements of different NFC services, the StoLPaN consortium has analysed various use cases from different industry segments. As a result of this analysis, we were able to create the system architecture and to define its boundaries. After detailing the functional description, we made an implementation to check its viability.

When we started our implementation we had to choice the most suitable platform. The selected platform had to be able to support a seamless user experience for downloading, using and deleting NFC services. The platform also needed to support the dynamic wallet concept and, finally, we wanted to create a friendly, open environment for developers.

The conclusion was that embedded chip handsets with MIDP 2.0 support already had all the mandatory features we needed to meet our main objectives. As they are commercially available, we can hopefully state that the features they carry represent the minimum that we will see in all future models. This ensures that our work can be easily reused in the future. Our middleware should work on any future MIDP 2.0 handset based on UICC or embedded chips without modification. For non-MIDP 2.0 based handsets (e.g. MIDP3, Android, SCWS, JC3, etc.), it may be possible to implement the concepts with a short or none software code. This is because it is not necessary to implement a wallet application if the underlying platform provides all the features necessary for a homogeneous NFC application environment.

The StoLPaN HOST wallet has a modular architecture and is based on a component model, which is the industry trend: both the next generation of mobile java, and MIDP 3.0's architecture are going to be component based. The component structure enables Service Providers to integrate NFC applications as components in the HOST dynamically and efficiently. In this way, Service Providers only have to deal with their business logic and can use pre-coded platform services for standard functions instead of implementing the whole application with all the related technical concerns of compatibility and portability. The code will be handset agnostic when run on the StoLPaN HOST, as the HOST hides all handset specifics. The StoLPaN Platform provides loose coupling between the individual third party components and the HOST core. As the APIs (that represent this coupling) to the HOST core services are open and available for the programmers, development of new NFC services can be carried out without changing the HOST core platform.

There are two types of components in the StoLPaN HOST:

- **Host Core Components**: they are part of the HOST. These components are required for the HOST to function correctly as they provide low-level functions to the second type of components which are implemented by third parties.

- **Third Party Service Components (TPSCs)**: they are not part of the HOST. They are installed, replaced or uninstalled without disturbing the HOST or other components that are not dependent on the replaced or uninstalled components.

The relations of the HOST, Third Party Service Components (TPSCs), and the Third Party Cardlet Applications (TPCs) are shown in Figure 4.

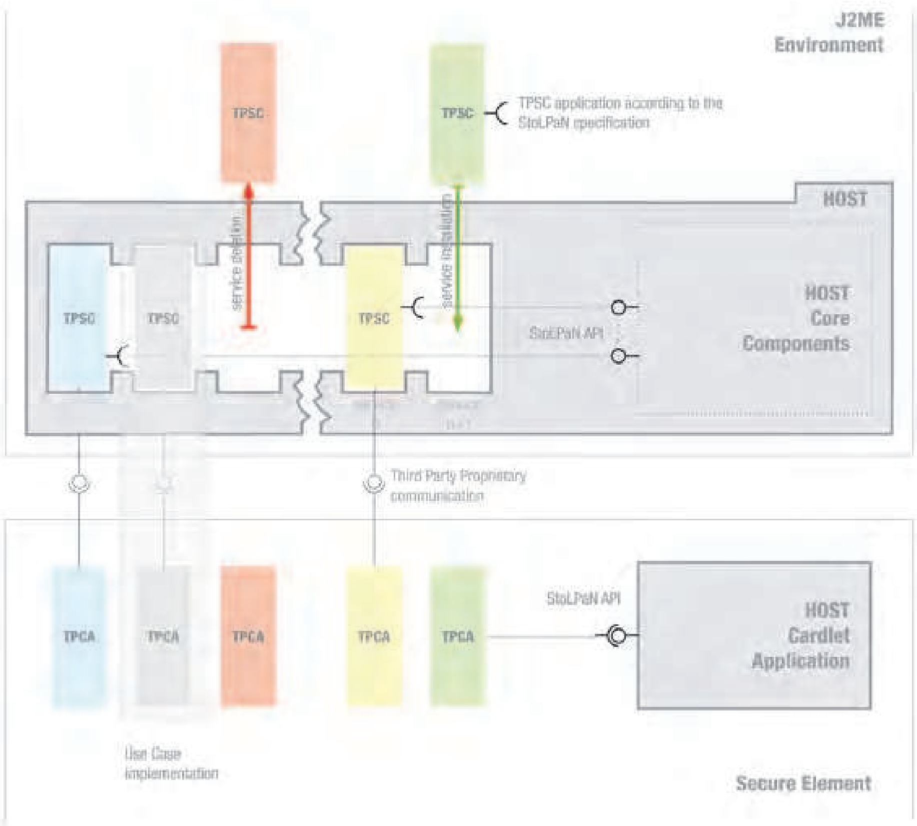


Fig. 4. The HOST structure and the use of Third Party Software Components (TPCs)

Among HOST Core Components, the StoLPaN Cardlet (HOST Cardlet Application) is a smartcard application residing on the default Secure Element in the handset. It mainly addresses shortcomings of the security and smartcard application management in the StoLPaN framework. It provides cryptographic support and can store keys, certificates and authentication schemes such as PIN or password for granting access to applications.

On the other side, the Third Party Service Components realize user interfaces and business logic on the client side for managing third party service-specific workflow and all third party related functions. The Third Party Cardlet Applications contain the sensitive application logic and any user related data in a secure environment provided by the applied Secure Element. The legacy cardlets which were designed for the traditional plastic card environment do not provide added value services such as User Interface support. To adapt these applications for the modern NFC environment, the application developer needs to implement some additional extensions into this cardlet. The Third Party Service Component (TPSC) and the Cardlet application (TPCA) coexist next to each other and realize the Third Party Service for the user. They run on the StoLPaN HOST resources, which makes them handset and platform agnostic.

4.2.4 Summary of the requirements

This section summarizes all the requirements necessary for a transparent application environment, which we believe is the key for NFC's success. We have also shown how we built our own flexible and transparent NFC wallet system (the StoLPaN HOST). This implementation will enable us to further analyse the environment requirements and at the same time create a tangible demo for the public.

This application environment concept, together with the application distribution principles explained in section 4.1, creates a complete description for an open NFC application environment. The advantages of the dynamic wallet approach can only be exploited if it is ready for rapid applications development. This requires open interfaces and libraries supported by an SDK for developers. The StoLPaN consortium is ready to cooperate on any further analysis of the related behaviours and requirements and to support any related standardization effort.

4.3 Demonstration of the StoLPaN solution in a smart shopping environment

So far in paragraphs 4.1 and 4.2 we presented the StoLPaN view of the utilization of the NFC technology and its contribution to the NFC market. In this section we will describe the retail demo application implemented by the consortium.

4.3.1 Overview of the retail industry scenario

In the past decades, the retail industry did not position itself as a great innovator when it comes to improving the customer's shopping experience through the implementation of new services and technologies. Instead, the most prevalent innovations were bigger packages for lower prices, for example in the range of products of hard discounters such as Aldi and Lidl. In the meanwhile, several technologies with the potential for significant innovations in the customer shopping process have matured and became available, e.g. mobile scanning barcode devices, new point-of-sale concepts, and radio frequency applications. Thanks to these technologies, retailers now have the opportunity to offer their customers additional services, such as self-scanning, self-checkout, information terminals, personal shopping assistants, and new, convenient methods of payment.

Studies (Benyó et. al. 2009, Wiechert et. al. 2009b) have revealed that the best thing a retailer can do to better serve its customers is to save their time. This includes the time that customers spend waiting at the checkout area and the time they spend waiting for a store employee to be available or to find a product that meets their needs. New checkout concepts and information devices can help retailers to shorten the lines at the checkouts and can help customers to become more independent from store personnel, for example through easy access to data on available products.

To enable mobile payment in retail commerce, support devices need to be designed and developed and the traditional business procedures need to be remodelled. The StoLPaN consortium is developing a mobile, contactless payment solution based on NFC mobile phones. With the help of these NFC mobile phones, customers will be able to pay offline via NFC, where compatible terminals are available, and over the air, where they are not. Asides the support for payment based on credit cards, debit cards, and an electronic purse, the project also includes the support of other concepts, such as e-tickets, loyalty cards, access ID, and e-prescriptions to be saved on the mobile phone.

The StoLPaN shopping process implements an individual information terminal combined with an individual POS, thus establishing a user friendly, efficient shopping environment.

The goal of the StoLPaN project is to create a pleasant shopping environment for the customers, while increasing efficiency of operation for the retail store operators. The core finding of the project, the basics of the StoLPaN shopping and payment process, is the personalization of the shopping experience, the delivery of personal services to someone's shopping cart and the removal of check-out and payment counters.

The new StoLPaN shopping and payment concept encompasses diverse functionality, including product information, loyalty programs, promotional programs, coupons, and payment. The smart shopping concept presented in this section has been developed in such a way that allows step-by-step migration from the traditional barcode based solutions to the new contactless, RFID based systems and services.

4.3.2 The StoLPaN shopping processes

As it was identified in our earlier studies (Benyó el.al. 2007, Wiechert et. al. 2009b), the various commercial sectors have significantly different shopping processes. It is however possible to identify some basic commonalities which can be summed up as a "generic customer shopping process" used across all retail sectors. This *generic customer shopping process* consist of the following steps:

1. choice of products,
2. registration of products,
3. payment,
4. security control (optionally including the deactivation of products),
5. procurement of product information (content, availability, pedigree, price),
6. general assistance (what, where, how, …?),
7. use of the loyalty programme (collection and redemption of rewards).

Also, as it will be detailed in the following sections, we decided to split these steps into *core process* and *optional services*. While the core process consists of those steps indispensable for the completion of the shopping process, the optional services are not necessarily preconditions. The breakdown into these two areas is the following:

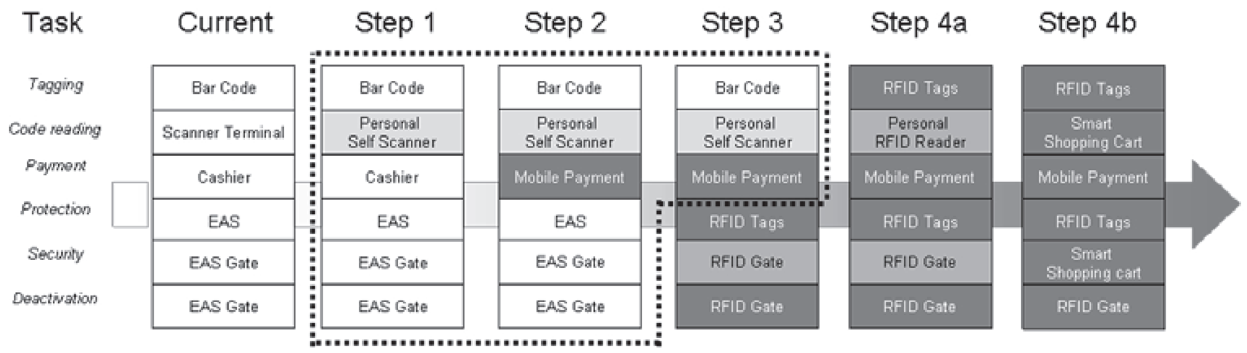
- Core process:
  - choice of products,
  - registration of products,
  - payment,
  - security control (optionally including the deactivation of products).
- Optional services:
  - procurement of product information (content, availability, pedigree, price),
  - general assistance (what, where, how, …?),
  - use of the loyalty programme (collection and redemption of rewards).

This split up is important for the design of the StoLPaN Personal Shopping Assistant (PSA) prototype, because we want to enable people to be able to benefit of the full pallet of services enabled by NFC, but also reserving them the right to renounce to these services (e.g. use of a loyalty card) if they wish to do so. We plan for our solution to be just as easy to use, while giving the technology friendly use many more options.

The implementation of the StoLPaN solution will be possible with different Auto-ID solutions, namely barcodes and RFID tags. While the barcode solution is likely to be more popular with retailers, because of its lower cost compared to a tag based solution and the fact that almost all products are already equipped with barcodes, this position might change in the future. In fact, RFID based solutions offer many more potentialities, such as automatic check-outs, automatic inventory counts and the possibility to identify product instances instead of product types.

Our interviews with retailers have shown that they definitely appreciate the option of a partial or step-by-step implementation of NFC and RFID based solutions. The StoLPaN consortium will thus integrate this possibility. However, a partial implementation bears the risk of losing a part of the anticipated efficiency gains, because the necessary expenditures would result in a lesser return on investment.

The StoLPaN project is targeting a smooth migration path for the NFC/RFID technology into the retail environment as shown in Figure 5. In each of the different tasks covered by the StoLPaN solution the existing technical and business state-of-the-art implementation is considered as the base for the next step. Therefore the StoLPaN solution is taking a conservative investment saving approach.



Task	Current	Step 1	Step 2	Step 3	Step 4a	Step 4b
Tagging	Bar Code	Bar Code	Bar Code	Bar Code	RFID Tags	RFID Tags
Code reading	Scanner Terminal	Personal Self Scanner	Personal Self Scanner	Personal Self Scanner	Personal RFID Reader	Smart Shopping Cart
Payment	Cashier	Cashier	Mobile Payment	Mobile Payment	Mobile Payment	Mobile Payment
Protection	EAS	EAS	EAS	RFID Tags	RFID Tags	RFID Tags
Security	EAS Gate	EAS Gate	EAS Gate	RFID Gate	RFID Gate	Smart Shopping cart
Deactivation	EAS Gate	EAS Gate	EAS Gate	RFID Gate	RFID Gate	RFID Gate

Fig. 5. Steps of migration from traditional shopping to shopping with the aid of applications using RFID/NFC technology

Taking into account the technical constraints as the limitation of the StoLPaN shopping experience, the following objectives are considered for the step-by-step migration path:

- delegate many functions to the customer’s mobile handset to avoid the need for individual support devices;
- delegate many functions to the retail back office to avoid the need for expensive technology built into the smart shopping cart.

The first step is characterized by the introduction of a personal self-scanner, this could be a dedicated barcode scanning device, a personal shopping assistant or even the customer's mobile phone. The customer will be able to scan his items by himself and, before leaving, the payment procedure will be done at a fixed payment terminal which can be assisted by a cashier. In the following step the personal self-scanner will morph into a closed loop payment terminal enabling the customer to pay where and whenever he wants. Even in this step, barcode will be the main identification technology for objects in the store.

The step three can be seen as an intermediate step for moving from barcode to RFID tagging. As this approach will happen for high value goods first the security related tasks are mainly affected. Finally steps 4 a/b uses RFID tagged products as the base for providing the StoLPaN solution to the customer. Whereas the customer can still use a handheld device to scan its purchase (4a) and pay using the same method as developed in step 2, the final vision is a completely automatic checkout using a smart shopping cart being able to read all the tagged products inserted by the customer. In this step the cart will incorporate also the payment terminal functions by being wireless connected to the back office using the retailers WLAN network.

4.3.3 The StoLPaN support devices

The StoLPaN process is built on the use of various support devices. These modules enhance customer service as well as facilitate the use of new technology and enable the seamless migration of the StoLPaN services from a barcode based environment to one where the most of the products are carrying smart labels.

The StoLPaN shopping environment consists of multiple components:

- The smart shopping cart is the temporary storage area for products to be purchased.
- The on-board computer (Personal Shopping Assistant, PSA) provides the necessary user interface for customer interaction and facilitates the remote data exchange with the back office.
- The StoLPaN back office coordinates the front-end devices and provides for the data exchange and the integration with the legacy systems of the retail operation.

Let's see how these components have been implemented by the StoLPaN consortium.

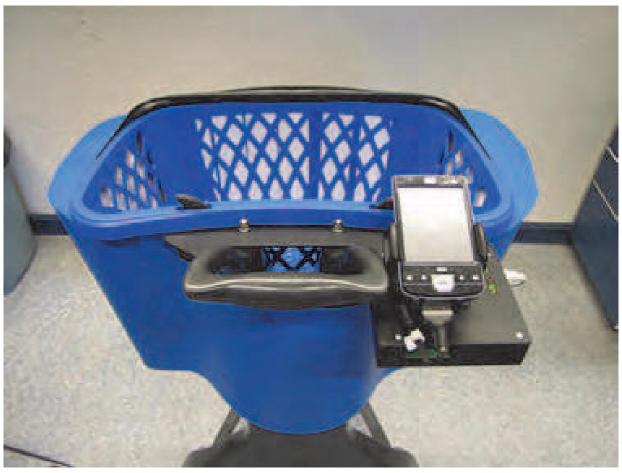


Fig. 6. Smart shopping cart

Smart shopping cart - It is a regular cart equipped with 3 pieces of UHF antennas, an RFID reader, a small computer (PDA) with display and battery (Figure 6).

It has a sophisticated antenna system that can read the RFID tags (EPC Class1 Gen2) on the products, found in the shopping cart in any position. The system consists of three switched high gain antennas, on the left and the right side, and at the bottom of the cart. At anytime only one antenna is active, while the others are operating as microwave absorbers. The cart is mounted with absorber in the front side to avoid reading tags outside the cart. The antenna system ensures that the whole volume of the cart can be read reliably at the 125mW radio frequency power level (European Standard Mode). Reading is reliable even with large number of tags. (The maximum number of tags to be handled can be adjusted in the collision algorithm). The UHF RFID reader reads the tags on the products inside the cart. We use the reader, according to the European standard, in 862-870MHz band, similarly the antenna system is designed according to the European regulations. The output power level can be programmed in the power range 9-24dBm at 50 Ohm. The system has an anti-collision algorithm for several RFID tags in the cart. The reader engine has a programmable serial interface for easy programmability from the local computer on the cart. The RFID reader has a serial to USB interface which connects it to the local on-board computer. From the local computer software the devices can be seen as serial devices and can be managed easily. The present program scans the cart with 500ms switching time at 12dBm radio frequency power level. The shopping cart has a high capacity battery. Using this battery the system can operate continuously more than 12 hours.

Personal Shopping Assistant (PSA) – The StoLPaN PSA will create a differentiated shopping experience and will increase customer loyalty as well as revenues. Nowadays retailer can no longer compete on price alone. In order to sustain and improve profitability in this highly competitive environment, retailers need to differentiate themselves from other stores, to strengthen customer loyalty and to increase overall sales. To survive in today's highly competitive environment, stores must achieve a new level of service excellence, eliminating long lines at the checkout counter and long waits for price and inventory checks. The StoLPaN PSA will provide a unique retail experience to promote customer loyalty as well as streamline everyday processes to maximize the productivity of retail associates, providing better control over labour costs while freeing up time to provide more personalized customer service. Customers can begin their enhanced shopping experience by simply swiping a loyalty card or by touching it with the mobile phone to unlock and activate the StoLPaN terminal. Afterwards, the customers are free to move throughout the store performing a wide variety of tasks — from scanning purchases to self-checkout and finally payment. Since the StoLPaN PSA can gather key data about customer's purchasing behaviour and decisions, the device enables the development of real-time push 1-to-1 promotions to shoppers. Wireless LAN connectivity delivers up-to-the-minute information on customers, while the StoLPaN architecture eases integration with current Point of Sale (POS) and Customer Relationship Management (CRM) systems, turning each customer visit into actionable business intelligence. In turn, shoppers benefit from more practical and valuable promotions that offer savings on regularly purchased products — increasing the likelihood of consumption.

From a technological point-of-view, the PSA is a general purpose PDA with a 4 inch 480x640 pixel display, with SD I/O port and WIFI interface, with a Windows Mobile operating system. (Presently an HP IPAQ214 is used, but any other types of small PCs could suit the purpose).

The computer serves the following functions:

- has a touch screen to allow the customer to select the various functions;
- has an NFC dongle (WD1010 connected to the SD i/o port) to communicate with the NFC handset or to read the contactless cards of the user;
- receives the antenna signals from the carts and converts them to a protocol manageable by the back office;
- communicates over secure WIFI with the back office;
- stores product information downloaded at the beginning from the back office to speed up response to the customer on specific queries;
- displays information received either through the NFC interface or through WIFI from the back office.

StoLPaN back office - The StoLPaN back office has its own business logic to manage the front-end shopping devices, as well as it provides the necessary interfaces for the legacy retail systems. It requests – using web-services – any information that is available and stored in the legacy. The back office is capable to communicate simultaneously with multiple legacy systems and to provide/request different data to/from the specified architectures.

The management of the individual virtual shopping cart is provided by the StoLPaN back office, as well as the operation of the integrated security architecture that checks whether products leaving the store are identical with the products paid for.

Smart security gates - The security gate is a shopping cart-wide, cart-length corridor with an UHF antenna system on the top, at a height of about 1.3 meter. Customers need to push the smart shopping cart through the corridor while they are passing through at its side. The antenna on the top of the gate can read the cart content and can retrieve the payment information of the respective cart from the back office. If the cart content matches the payment information the customer may leave the store without any further interruption, while if there is any discrepancy the security personal is alerted. In case of simpler architectures the security gate is replaced by a handheld security terminal to be carried by the security guards. Guards can make random spot checks on any of the carts leaving the store. The terminal provides the payment information on any of the carts they want to check which they can compare with the actual cart content.

4.3.4 Services

The StoLPaN smart shopping solution supports the following functionality:

1. **Loyalty sign-in -** Customers with loyalty cards or loyalty credentials in the NFC handset can sign in with the PSA. This greets the customer with his name and provides any relevant information (e.g. the number of bonus points available for use, personalized promotional offers or even a shopping list the customer has generated at home) the back office is providing as a response.
2. **Product pricing** - Upon placing the tagged products into the cart the on-board computer shows the running total of the purchase. There may be multiple prices shown, original price in one column and discounted price in another column.
3. **Product information -** When placing a product into the cart, it can be selected for further detailed information, for example detailed product description or the list of accompanying or related product, etc. Using the specific Query menu any products included in the store data base can be searched.
4. **Product location** - As part of the product information the exact location of a product in the store can be shown on the display of the PSA.
5. **E-coupons – discounts** - The PSA can read e-coupon information from vouchers or from the NFC handset. The PSA forwards the information to the back office and the response is the new reduced promotional price information or the rejection of the coupon including the specified reason.
6. **Payment** - The smart shopping cart with its PSA can substitute a cashier counter and can act as a POS terminal. There are three types of payment solutions supported by the StoLPaN implementation.
   - Cash payment: upon selecting the cash icon on the PSA, the invoice information is forwarded to a dedicated cashier desk and the customer is advised to proceed to that given counter. In this scenario products are not counted and scanned again by the cashier, payment is made based on the invoice generated and forwarded by the StoLPaN back office.
   - Card payment: upon selecting the bank card icon the customer is requested to present his bank card. The payment is processed by the retail back office as a Card-Not-Present transaction.
   - Loyalty payment: if the loyalty payment option is selected, then payment is made by using the pre-registered payment instrument of the customer. In this case the payment transaction is performed either as a regular card payment process, or using the available amount of loyalty points.

A future extension of the service can be the introduction of individual pricing. As smart tags on the products identify specific individual products and not just product categories, it is possible to price similar products differently on the base of various factors – like closeness of expiration date, damage of packaging, date of reception, etc.

4.3.5 Barcode and contactless

The original StoLPaN shopping process was developed for smart shopping operations, where all the products are tagged with smart RFID tags. However, as fully operational and completely smart retail operations are still a few years away, the solution has been extended to the traditional barcode based environment. In such an environment, the smart shopping cart does not have antennas, instead the PSA receives a built-in barcode reader. When a product is selected, the customer waves it in front of the reader and when the reading is successful a beep sounds. The process is similar with the loyalty sign-in and coupon redemption features. All the previously described services are available as well. At the back office level, the procedures are identical, no changes are necessary. Actually only the antennas on the cart and the smart security gate need to be added to the StoLPaN smart retail operation upon conclusion of a migration from the barcode based to RFID identification. All other features of the new StoLPaN shopping process can be continued without any modification and loss of investments.

5. Beyond the StoLPaN Project: future challenges for NFC-based services

The StoLPaN project ended in 2009, identifying four key topics for the future of NFC ecosystem (StoLPaN consortium, 2009b). The consortium is still working with Global Platform and NFC Forum to have the Project results endorsed by these standardization bodies.

Beyond the StoLPaN project, the authors have identified three major points that have to be considered for the mass adoption of NFC based applications and services. They are related to the evolution of devices and UICCs, the improvement of OTA communication capabilities, which make use of communication protocols such as Bearer Independent Protocol (BIP) with the overlaying Card Application Toolkit_Transport Protocol (CAT_TP), and finally the use of Smart Card Web Server (SCWS) technology for increasing SIM-based applications' capabilities.

The evolution of mobile devices includes the evolution of the UICC and related SIM logical module too. The capacities of the SIM, as well as the applications supported, improve and increase with the (U)SIM (Universal Subscriber Identity Module), which is used in 3G mobile phones. By increasing its capacity, the (U)SIM can host the Secure Element with the user's personal information along with the keys for data protection. In the (U)SIM the SE has a dedicated area for memory and logical elaboration. As we have already discussed in the paper, according to the Smart Card Alliance and Global Platform (Global Platform, 2006), the SE can be divided in different Security Domains (SD), which are separated and logically distinct domains controlled by different Service Providers.

As each SD can be dynamically managed via wireless networks, users can choose their favored services and personalize the carnet of applications on their mobile phone whenever they wish. This improves the service usability, while the user's satisfaction increases. Moreover, the mobile phone becomes a real multitasking object used to pay, to travel, to get discount coupons of the own preferred brands and to communicate with friends.

As we already mentioned, compared with smart card technology, NFC applications stored in the SE situated on the (U)SIM can be modified also after the issuance of the support thanks to OTA update and management service. In order to increase the amount of information exchangeable via wireless communication, OTA services can rely on new protocols besides SMS: the Bearer Independent Protocol and the overtopping layer named Card Application Toolkit_Transport Protocol. As a consequence of this improvement, it is possible not only to transmit a greater amount of data, but also to establish a more secure and reliable communication. More in detail, the BIP and the CAT_TP are able to open a channel for the transmission of data between the device, the OTA Server and the (U)SIM card. The communication channel can be opened either by the client or by the OTA Server, i.e. by the (U)SIM by means of a command to the host device or by the OTA Server by means of a SMS sent to the (U)SIM.

Finally, the future for mobile applications, even the NFC-based ones, is to use a web-compliant logic also for the user interface. The (U)SIM already offers a suitable space to host the Smart Card Web Server (SCWS), which is practically a web server stored locally on the UICC (Madlmayr et al., 2008). Through this Web Server the user can rapidly access to multimedia contents both static and dynamic. By using NFC in combination with a SCWS (now directly connected on the USIM) user can enjoy a richer, more consistent and more intuitive experience without paying any Internet connection fee, as he can benefit from local contents similar to the Internet ones. Moreover, since the MNO can update and manage the contents remotely, it can increase its offer to the end-user.

6. Conclusions

In this paper the authors presented the services, use cases and the future challenges for Near Field Communication, which is the most customer-oriented one among RFID technologies, as it can be described as the integration of an HF reader into the most popular personal device worldwide, i.e. the mobile phone.

After detailing NFC communication modes (card emulation, peer-to-peer and reader/writer modes) and related use cases such as payment, ticketing and information retrieval, the authors focused the attention on the standardization and interoperability within the NFC ecosystem that NFC based services need to achieve in order to reach mass adoption.

The authors presented the results of the research activities carried out by the StoLPaN consortium during a three-year Project co-funded by the European Commission.

The StoLPaN consortium has worked on overcoming interoperability issues, mainly dealing with application-level standardization, which has not been considered by standardization bodies yet. The consortium elaborated a procedure for dynamic card content management of Secure Elements placed in a mobile handset, identifying key and supporting roles within the NFC ecosystem. Moreover, the consortium has detailed the technical environment necessary for the dynamic management of NFC services, building a proof-of-concept prototype of the NFC wallet application based on a component structure. Finally, StoLPaN has demonstrated the effectiveness and the efficiency of the solution in a smart retail environment, tracing the way forward for the migration from traditional, barcode based, shopping to a smart shopping environment with the support of applications and services that use RFID and NFC technologies.

Beyond the results carried out during the three-year StoLPaN project, the authors have finally identified other three major points that have to be considered for the mass adoption of NFC-based services and applications. These are related to the evolution of the (U)SIM, the improvement of OTA protocols such as BIP and CAT_TP and to the migration to a web-compliant logic for the user interface making use of new technologies such as Smart Card Web Server.

7. Acknowledgment

The authors would like to thank their partners in the Framework of the IST-FP6 project StoLPaN (Store Logistic and Payment with NFC).

8. References

Benyó, B., Vilmos, A., Kovacs, K., Kutor, L., (2007) NFC Applications and Business Model of the Ecosystem. Proc. of the 16th IST Mobile and Wireless Communications Summit. Budapest, Hungary, 2007.07.01-2007.07.05., pp. 1469-1473. Paper 576.

Benyó, B., Vilmos, A., Fördős, G., Sódor, B., Kovács, L., (2009) The StoLPan View of the NFC Ecosystem. Proc. of WTS 2009, 8th Wireless Telecommunications Symposium. Prága, Csehország, 2009.04.22-2009.04.24., 5p., Paper 1569183809.

EPC 492-09, (2010), White Paper Mobile Payments, 1st Edition, Available from http://www.europeanpaymentscouncil.eu/knowledge_bank_detail.cfm?documents_id=402

ETSI TS 102 190 V1.1.1: Near Field Communication (NFC) IP-1; Interface and Protocol (NFCIP-1), (March 2003), Available from http://www.etsi.org

ETSI TS 102 622 V.7.5.0 : Smart Cards; UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI) (Release 7), (June 2009).

ETSI TS 102 613 V.7.7.0 : Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics (Release 7), (October, 2009).

GlobalPlatform, (2006), Card Specification Version 2.2, Available from http://www.globalplatform.org.

GSMA, (2007a), Mobile NFC services, Version 1.0, Available from http://gsmworld.com/documents/aa9310.pdf.

GSMA, (2007b), Pay-Buy-Mobile Business Opportunity Analysis, Version 1.0, Available from http://gsmworld.com/documents/gsma_pbm_wp.pdf.

GSMA (2007c), Mobile NFC technical guidelines, Version 2.0, Available from http://gsmworld.com/documents/gsma_nfc2_wp.pdf.

Innovision Research & Technology plc, (2007), Turning the NFC promise into profitable, everyday applications, In: *Near Field Communication in the real world – part I*, Available from http://www.nfcforum.org/resources/white_papers/Innovision_whitePaper1.pdf

ISO/IEC 14443 : Identification cards – Contactless integrated circuit(s) cards – Proximity cards (Part 1-4), Available from http://www.iso.org.

ISO/IEC 18092 (ECMA-340): Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1), (First Edition, 2004.04.01), Available from http://www.iso.org

ISO/IEC 21481 (ECMA 352): Information technology - Telecommunications and information exchange between systems - Near Field Communication Interface and Protocol -2 (NFCIP-2), (January 2005), Available from http://www.iso.org

Kannainen, L., (2009). Global overview of commercial implementations and pilots of NFC payments during 2009, In : *Smart Card Technology International - globalsmart.com*, 08.11.2010, Available from http://www.mobeyforum.org

Madlmayr, G., Brandlberger, D., Langer, J., Scharinger, J., (2008), Evaluation of SmartCard Webserver as an Application Platform from a User's Perspective, *Proceedings of MoMM 2008*.

Mayes, K., Markantonakis, K., (Eds.). (2008). *Smart Cards, Tokens, Security and Applications*, Spinger, ISBN: 978-0-387-72197-2, New York.

Mobey Forum, (2010), Alternatives for Banks to Offer Secure Mobile Payments, Version 1.0.

NFC Forum, (2006), NFC Data Exchange Format (NDEF) Technical Specification, Version 1.0.

StoLPaN consortium, (2008a), Dynamic Management of multi-application Secure Elements, Public Whitepaper, Available from http://www.stolpan.com

StoLPaN consortium, (2008b), Dynamic NFC wallet, Public Whitepaper, Available from http://www.stolpan.com

StoLPaN consortium, (2009a), StoLPaN Smart Shopping, Public Deliverable, Available from http://www.stolpan.com

StoLPaN consortium, (2009b), NFC Application Distribution – Proposed Business Models, Public Deliverable, Available from http://www.stolpan.com

Wiechert, T., Thiesse, F., Schaller, A., & Fleisch, E., (2009a), NFC based Service Innovation in Retail: An explorative Study. In Proceedings of the 17th European Conference on Information Systems (ECIS)12, Verona, Italy, June 8-9 2009, p12., ECIS2009-0587.R1

Wiechert, T., Schaller, A., & Thiesse, F., (2009b), Near Field Communication Use in Retail Stores: Effects on the Customer Shopping Process. In Mobile und Ubiquitäre Informationssysteme - Entwicklung, Implementierung und Anwendung137-141. Bonn, Germany: Gesellschaft für Informatik e.V. (GI). - ISBN 978-3-88579-240-6.