



Dynamic management of multi-application secure elements



StoLPaN – NFC mobile services standards consortium



The Consortium consists of

No.	Participant Name
1	Motorola Ltd.
2	SafePay Systems Ltd.
3	Deloitte Ltd.
4	Budapest Tech, John von Neumann Faculty of Informatics
5	Auto-ID-Labs St. Gallen
6	BULL Ltd.
7	Consult Hyperion
8	Fornax Plc.
9	NXP Austria Gmbh.
10	University of Technology and Economics
11	Banca Popolare di Vicenza
12	Libri Bookstores Ltd.
13	Baker & McKenzie
14	Consorzio Triveneto S.P.A.
15	SUN Microsystems Ltd.
16	T-Systems Hungary Ltd.
17	NXP Italia Spa.
18	Motorola Gmbh.
19	Cattid

Contents

1. Glossary	4
2. Preface	5
3. Executive summary	6
4. Issues to consider	7
4.1 Card issuance	7
4.1.1 Complexity of the mobile NFC ecosystem	7
4.1.2 Traditional card issuance and management	7
4.1.3 Dynamic multi-application card content management model	8
4.2 Need for interoperability	8
4.3 Service distribution	8
4.4 Limitation of trial operations	8
4.5 A GSM analogy - unveil what needs to be done	9
4.6 Conclusion	9
5. Basic requirements	10
6. Our proposed solution	11
7. Roles	12
7.1 Primary roles	12
7.1.1 User	12
7.1.2 Secure Element Issuer	12
7.1.3 Service Provider	12
7.2 Support roles	12
7.2.1 OTA provider	12
7.2.2 Trusted Service Manager / Trusted 3rd Party (TSM)	13
7.2.3 Application Issuer	13
7.3 Conclusion of the roles considered	13
8. The proposed card content management process	15
8.1 The technical process	15
8.1.1 The start	15
8.1.2 Information requirement, data exchange	15
8.1.3 Data check and SE selection	16
8.1.4 Card Issuer determination	16
8.1.5 Post issuance process	16
8.2 Other issues to consider	18
8.2.1 How to find the right card issuer – card issuer reference	18
8.2.2 Multi SE environment – SE selection	18
8.2.3 Customer support	19

1. Glossary

3G	3 rd Generation mobile network
CA	Certification Authority
CPLC	Card Production Life Cycle data
EBPP	Electronic Bill Presentment and Payment
GP	Global Platform
GPRS	Global Packet Radio Service
GSM	Global System for Mobile
MNO	Mobile Network Operator
MSISDN	A number uniquely identifying a GSM subscription
OTA	Technology to manage Secure Elements remotely
SD	Security Domain
SD Card	Mass storage 'Secure Digital' memory card
SE	Secure Element
SIM	Subscriber Identity Module
TSM	Trusted Service Manager, Trusted Third Party (TSM, T3P)
UAP	User Agent Profile
URL	Universal Resource Locator

The StoLPaN consortium is co-funded by the European Commission's Information Society Technology (IST) program.

This document reflects only the authors' view and the Commission is not liable for any use that may be made of the information contained therein.

2. Preface

The StoLPaN project, with the support of the European Commission's IST program and the consortium behind it, will detail the commercial and technical frameworks required to deliver third party applications securely into Secure Elements (SEs) in an NFC-enabled mobile handset, irrespective of the handset type or the support infrastructure. These frameworks will be submitted to the relevant trade bodies for adoption and demonstrated in a Host Application developed by the project team.

This document is the first in a three part series of white papers presenting a proposal for the post issuance procedures for multi-application SEs. The second paper will discuss application management in a single platform multi-application environment. Lastly, we also plan to release a white paper about the NFC value chain, possible business models, key legal issues and other challenges of the multi-application NFC operation.

In this paper we describe the technical model for dynamic card content management of SEs placed in a mobile handset. All the rules, processes and interactions are also valid in case the same process should be realized for a personal or handheld computer equipped with SEs.

In the proposed model, we have tried to avoid the use of technology-specific terms as much as possible. The goal was to describe in simple terms, a set of reliable, transparent logistical and technical processes for the various business interactions that provide the tools for dynamically managing individual service portfolios, even with international scope.

3. Executive summary

Managing an NFC service in a mobile multi-application environment is very challenging for Service Providers and SE issuers. This is a dynamic 'n' to 'n' relationship, where partners may not have prior knowledge of each other; have limited control over the service environment in which their application is to run; and where the business model and value chain is completely different from those in their usual practices. The StoLPaN model provides a solution for dynamic application management that can be uniformly applied in local as well as in global operations, both between parties with steady contractual relationships and between ad hoc business partners.

One of the main challenges of the new mobile NFC service environment is that current card issuance models cannot support the dynamic post issuance personalization process. This is because Service Providers:

- Have absolutely no control over the cards – referred to as Secure Elements (SEs) in this document – on which their applications are stored, except for deciding whether or not to use them
- Have no control over other applications stored in the same SE
- May not know their clients personally, or have the opportunity to contact the SE or the user physically.

The existing, and primarily expected, technical diversity call for early standardization of the post issuance and personalization process. Otherwise, isolated solutions will prevail and the technology will be incapable of serving the projected several hundred million users and thousands of Service Providers adequately.

To ensure the necessary openness and interoperability, the new logistical and technical model fulfils the following criteria:

- Open relationship between Service Providers, SE Issuers and Users
- Technical transparency for Service Providers
- Service homogeneity for Users

One single logistical process can be created – covering loading, personalization and life cycle management of applications – that is technologically agnostic and supports all SE types, even multiple ones, in communication devices. The process also ensures that both user and Service Provider need not rely on 3rd party services, unless they prefer to outsource certain activities.

In this environment the user can enjoy the services of multiple Service Providers, and can decide which Service Providers and services to use.

The process describes a homogenous system which supports SE issuers such as Mobile Operators in promoting their services to Service Providers, facilitating growth and improving business conditions.

This homogenous system also improves business conditions for Service Providers by achieving technical compatibility with platforms of various SE issuers. The result is free access to the customer base of multiple SE issuers, and improved economics of developing NFC services.

4. Issues to consider

4.1 Card issuance

4.1.1 Complexity of the mobile NFC ecosystem

The service environment

- Potentially, many Service Providers could place their applications on the SE in mobile handsets
- The SE is an 'external condition' for all Service Providers – its technical parameters cannot be influenced
- Potentially, there are multiple card issuers in every country
- Users (customers) are mobile and may wish to use NFC services even if they are abroad
- Some Service Providers are global and prefer to have uniform solutions for application deployment and operation, irrespective of the specific market
- Users may wish to change the service portfolio they use dynamically, even after the issuance of the SE, adding a service here and there and cancelling another one when no longer needed
- The various service applications have their own specific requirements, but they still need to share the same SE and must coexist and perhaps even interoperate

In the mobile NFC world, there are many constraints unknown to either Service Providers or SE issuers in their current operations. It presents a new way of doing business: in which no-one can substantially influence the service environment, and cooperation is necessary between even unknown partners. A transparent logistical model and a technical solution are needed that can ensure uniform procedures for the parties involved. This makes it unnecessary to negotiate and describe the details of each and every interaction, and allows even previously unknown business partners to seamlessly realize the procedures for application deployment and management. Without such an approach the NFC ecosystem will not prevail, resulting in an unsatisfactory business model that is unable to provide user-friendly, valuable services for customers.

4.1.2 Traditional card issuance and management

In the traditional issuance process of contact and contactless cards, the card environment and the services loaded onto them are well specified and known in advance. The whole technical and logistical process is strictly controlled. Usually it is not possible – or even necessary – to manage card content throughout the card's lifecycle. After the card is distributed, the Service Provider typically loses any control over it.

In today's multi-application environment, the applications and their Service Providers are known to each other: card management and all commercial issues are contractually regulated well in advance. The stored applications and the Service Providers involved are usually static, and will not change during the card's life cycle. Technically the cards do allow content download after issuance, but this is rarely done. Examples of contact and contactless services on traditional cards are those provided by public transportation companies, or banks with diverse payment methods.

4.1.3 Dynamic multi-application card content management model

The new dynamic multi-application NFC service environment requires new logistical and technical solutions because current card issuance and content management models and practices are inadequate. In the dynamic post issuance and personalization process, Service Providers will:

- Have absolutely no control over cards on which their applications are stored, except for deciding whether or not to use them
- Have no control over other applications stored on the same SE
- May not know their clients personally, or have the opportunity to contact the SE or the user physically.

4.2 Need for interoperability

Industries working with NFC technology are striving to achieve technical standards and interoperability at the basic, underlying technology level. At least the same level of interoperability needs to be achieved on the more complex application level too, where it is still missing.

The present environment with proprietary service applications, unique logistical solutions do not provide the right conditions.

For services and applications there are many independent players involved. Their decisions are primarily driven by considerations that are not NFC specific, therefore they only accept transparent, financially sound solutions.

4.3 Service distribution

There are several players involved in the NFC value chain, but their roles and form of cooperation are poorly defined. This means distributing any NFC service application requires special, individual agreements between the partners involved. With relationships ill-defined, Service Providers face new logistical challenges every time their application is loaded onto their users' SEs.

4.4 Limitation of trial operations

Most key Service Providers in the smart card industry have started, or plan to start, their own pilot systems. They want to gain experience with NFC technology and to prepare themselves for the commercial rollout of NFC services. In these trials, key industry stakeholders implement local, proprietary solutions and concentrate on only one or a few selected use cases, usually with preloaded applications.

While these trials may serve the purposes of usability assessment, they are hardly adequate for evaluating the complex service environment – which is projected to involve several hundred million users and thousands of Service Providers within a few years.

4.5 A GSM analogy - unveil what needs to be done

By now GSM is a widely adopted standardized international system for mobile communication with a huge number of users. The great advantage of this system is not only the interoperability resulting from the cross-border roaming capability, it also has advantages in terms of service development and economics.

The high penetration of GSM systems offers a solid foundation for the fast development of new functionalities, new designs and new services. In a similar environment for NFC in which a sufficiently large customer base can be targeted and reached, a Service Provider could develop a new experience efficiently.

Even if only in a limited way, the standardization of both NFC application download procedure and platforms would let the NFC community act as one, just as in the GSM world. This would improve NFC business conditions dramatically.

4.6 Conclusion

To support quick proliferation of NFC services the industry has to achieve a homogenous, dynamic service environment which would, even after issuance of the cards, allow any service to be loaded onto any SE and managed throughout the application's lifetime.

The present document introduces a logistical and technical process that provides a solution for these requirements.

5. Basic requirements

User

In an ideal NFC environment users can download any NFC application onto their handsets or PCs. It is also expected that, if a user purchases a new handset or changes their mobile Service Provider, etc., they will have no difficulties in transferring applications from one device to the other.

Users want homogeneity. They should not face compatibility issues or have to worry about any technical information for application use or download.

The NFC industry is on its way to deliver this experience to the user. **The first basic requirement for this goal is to provide technical compatibility between the services and the hosting environments.**

Service Provider

From the Service Provider's perspective, the logistical model for dynamic post issuance and remote personalization should be both handset vendor and SE environment transparent. The differences between the end-user environment and the used architecture should be hidden. This allows Service Providers to follow the same procedures and use the same applications irrespective of any technical differences in the host environment.

There will be numerous players involved in the dynamic post issuance and remote personalization process. It cannot be expected that all parties know each other or have established commercial relationships. **The multi-application mobile environment establishes the requirement that the technical model supporting the dynamic post issuance procedure for NFC services should be capable of detecting any and all environment specifics, and should eventually hide any technical incompatibility from the players involved.**

6. Our proposed solution

This white paper introduces a logistical process that contributes to the creation of a truly global, interoperable NFC service environment based on a **standardized dynamic card content management process**.

Firstly, let's clarify what is meant by card content management. There are two types of content management:

- Card content management includes creation/deletion of new security domains, application loading and personalization of the smart card application. It also contains the deletion of applications and domains on request.
- Application content management covers the product/portfolio management of the Service Provider.

This paper focuses on card content management, while the complementary application content management process will be discussed in a later document.

The solution is described with reference to a secure element. This SE can be a SIM card, an embedded chip or an SD card. The concept discussed in this paper also provides the algorithm for a selection process involving multiple SEs deployed in the same handset.

The proposed logistical and supporting technical model will offer solutions for the following challenges:

- Dynamic post issuance
- Dynamic personalization
- Clear automated flow of logistical interaction of players involved, including international relations
- Definition of optional support functions for Service Providers
 - OTA service provisioning
 - Trusted Service Management (TSM)
- Homogenous user experience for all applications
 - issuance
 - application management
- Introduction of optional customer support
 - Trusted Service Management (TSM)

It is the industry's task to describe standards for the NFC domain that, if followed, provide a transparent environment for both Service Providers and users. Currently there are few commercial handsets on the market, with only trial and pre-commercial NFC services operating, making it the ideal 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 and the development of uniform solutions. If not correctly implemented, the result will be a more complex and expensive NFC service environment.**

7. Roles

While the proposed card content management process is quite complex, it is also very flexible and includes various roles/functions. **We have identified the functions necessary to complete the process, but the actual players in these roles will always be situation driven.** This means that for each and every personalization instance there will be a unique combination of partners involved.

7.1 Primary roles

The complete service scenario cannot be performed without these roles, however one single player may assume more than one role in the process.

7.1.1 User

The User is the person selecting the application/service and can initiate the request for post issuance and personalization. The user may own the application they wish to download into the SE, or may just use it based on whatever contractual arrangements are in place. These distinctions are important from a legal perspective – control and liability issues – but are transparent for the logistical process itself.

7.1.2 Secure Element Issuer

The issuer of the SE has control over the SE. Control means the right to decide how the SE's storage capacity is used. To exercise these rights the SE Issuer needs to possess the secret key(s) which allow general control over SE management. **The SE Issuer can define the rules governing SE storage space – including who can use it, when and under what conditions. The SE Issuer may also deploy card content onto the SE.**

7.1.3 Service Provider

A Service Provider is anyone wishing to deploy / manage a service application or data element on the SE. No distinctions should be made between Service Providers as long as they comply with the industry's standard security protocols and SE Issuer's specific business conditions. Service Providers are primarily large service operators, like banks or transport operators with ticketing applications. Further examples are retailers, with loyalty and other programs, and authorities using various ID cards, etc.

7.2 Support roles

To provide a fully functional, economic and convenient service the following roles must be considered.

7.2.1 OTA provider

The key value added feature of the post issuance and personalization procedure is the opportunity to perform this activity remotely, over the air (OTA). OTA is a service, but it is also a common name for various communication technologies that enable secure data transfer between an SE and a back-office architecture. From our perspective the technical implementation of OTA services is transparent and does not affect the proposed solution.

7.2.2 Trusted Service Manager / Trusted 3rd Party (TSM)

If placed into an electronic device, NFC technology will be able to support value added services that are not possible – not even considered – in traditional card-based contact or contactless applications. Having performed their activities for years, Service Providers may not be ready or able to change their working methods or the functions they provide. But they may still want to participate in the new mode of service operation: by enhancing the services they offer without changing existing core processes. This conflict is solved by involving a TSM, who can provide the technology and service support necessary for realizing these objectives.

Users also face a challenge presented by many applications being available on one SE, or even, in a more complex situation, multiple SEs. The services need to be managed and protected. This can be a time consuming and potentially difficult activity that many users do not want to bother with. However this could be supported by a Trusted 3rd Party.

The two roles, TSM for the Service Provider and TSM for the User, have different requirements that call for an EBPP-like model, in which there are user consolidator TSMs and Service Provider consolidator TSMs who, by necessity, interact with each other. The roles are not exclusive: the same TSM may act in either position for different parties.

It is important that we treat the TSM strictly as a service support function and not as an entity whose task would be to solve technical imperfections in the service provisioning.

7.2.3 Application Issuer

The application issuer provides the application which implements and fulfils the business requirements of smart card Service Providers. Application issuers can guarantee secure interoperability between card and card-acceptance device. Sometimes, the Service Provider is also the application issuer.

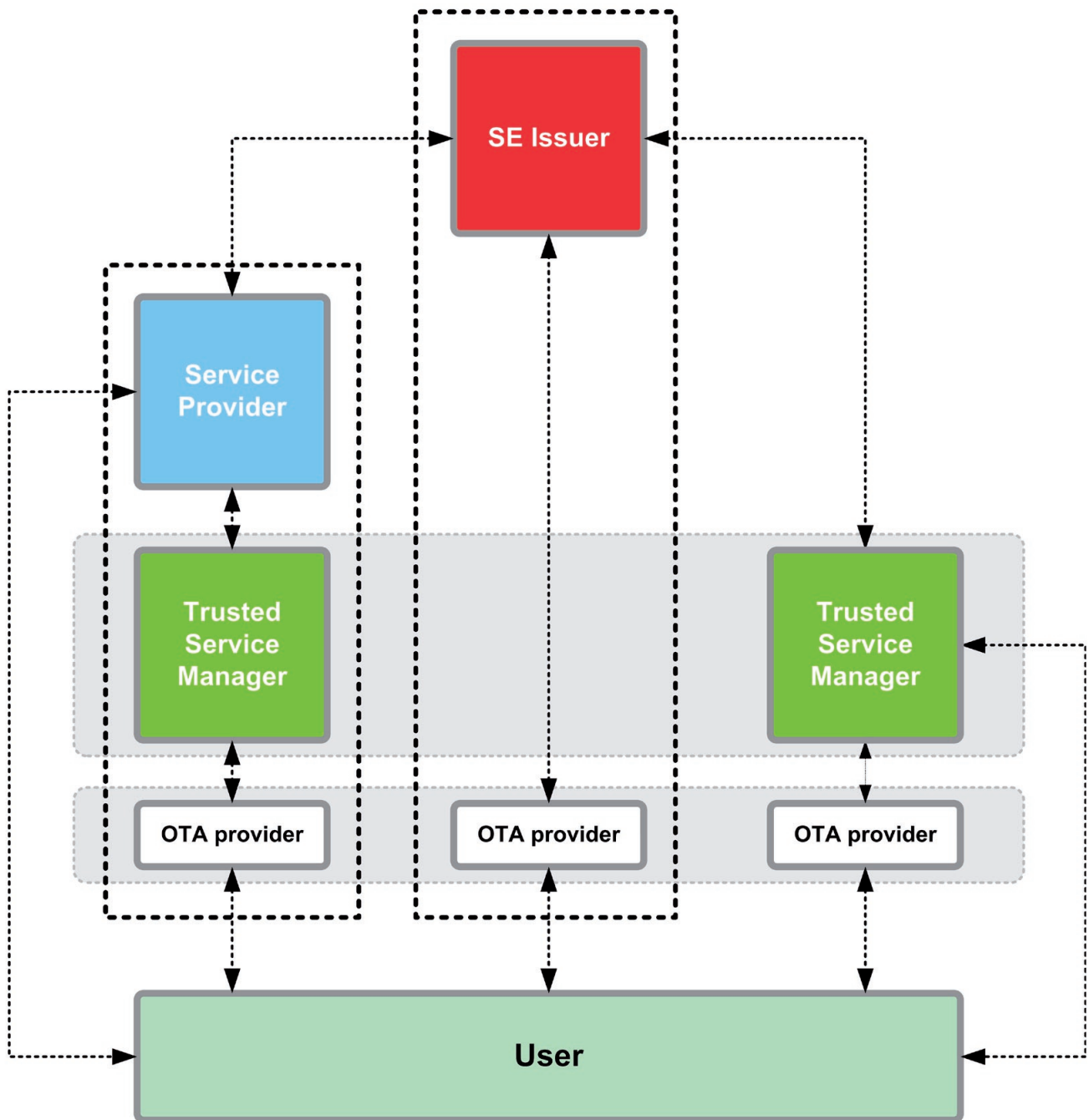
7.3 Conclusion of the roles considered

In reality many Service Providers will offer contactless services and require online application management support. There will also be many SE issuers, and most probably a number of other players.

Some roles have to be filled: for each and every post issuance personalization interaction, there is always a User for the service, and always an SE Issuer providing access to the SE.

Although involving additional players in the support roles is optional, there is nothing to prevent multiple players being involved in one single transaction, all acting in various capacities for the User, the Service Provider and the SE Issuer.

While support functions are required, involvement of additional players is not necessary since under specific conditions simple technical infrastructures can perform OTA and TSM activities.



Roles in the NFC environment

8. The proposed card content management process

It is unrealistic to expect one concept to satisfy all the service needs and all the preferences of Users and Service providers. Several business models will probably co-exist but, most importantly, **they can all be served and supported with the technical process described below, resulting in a uniform service environment.**

8.1 The technical process

8.1.1 The start

In the visionary NFC world, users find information about services they like in many different ways. For example:

- Upon opening a newspaper, the users see an advertisement promoting a service. There is an RFID tag integrated into the ad, and a simple touch of this smart poster with their NFC-device transfers all the necessary information to initiate registration and service deployment.
- Users may also WAP or browse the net with their phones and when they find something they like a link assists them in initiating a service relationship.
- The same service can also be found using a PC. While browsing, the users open up the ad and enter their phone number, which triggers an SMS containing the service specific information.

The possibilities are endless.

One important remark: the originator of these requests is always the user. This is important to avoid unsolicited pushed service offerings.

8.1.2 Information requirement, data exchange

Having received the service request, before the application can be installed the Service Provider needs to collect information about the target device in order to perform the remote card content management procedure. The proposed service environment has to be evaluated, the SE Issuer identified and the potentially available remote support services defined.

The information required contains details about the:

- **NFC device** (The Service Provider and Card Issuer need to identify the end-user device for providing remote management)
- **Secure Element** (The Service Provider needs the SE's CPLC information to find the target SE's Card Issuer and evaluate its security environment)
- **Secure Element Issuer** (The automated contact information of the Issuer, or a pointer to it, is required)

In the procedure, the reference data is stored on both the SE (in case of multiple SEs, each SE stores its own specific information) and in the handset's operating system.

The stored information is sent to the Service Provider for evaluation. The message generated by an application on the User's device is addressed either to a specific Service Provider address (it could be a URL), or to its associated TSM partner, where it can be processed automatically. This relationship is transparent to users: they do not need to know how the service is delivered.

8.1.3 Data check and SE selection

When assessing the message received from the User's device, the Service Provider can decide whether the User's technical environment satisfies its requirements based on technical, security and financial considerations. For multiple SEs, the Provider can also decide which SE it prefers as a storage space / runtime environment for its application. The received message may also indicate the user's preferred SE, which the Service Provider should take into consideration. After evaluating the technical information, the Service Provider either starts the card content management procedure or informs the User that for some – identified – reason(s) the NFC service application cannot be loaded onto the device.

8.1.4 Card Issuer determination

Once the Service Provider selects the target SE, the Service Provider or its TSM partner can identify the chosen SE's Issuer. The necessary identification information is also contained in the service initiating message sent to the Service Provider from the User's mobile device. This piece of information is the only data element that is currently not available either on the SE or in the mobile phone and necessary for starting the automated card content management process.

8.1.5 Post issuance process

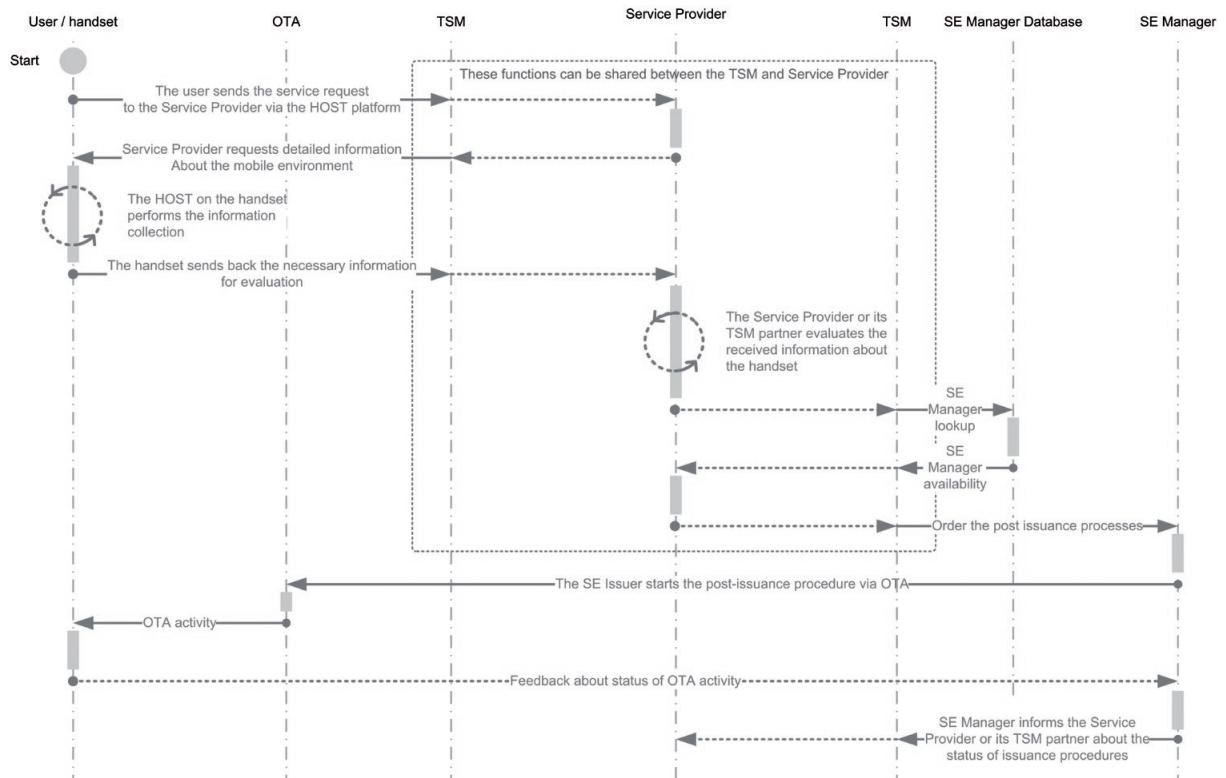
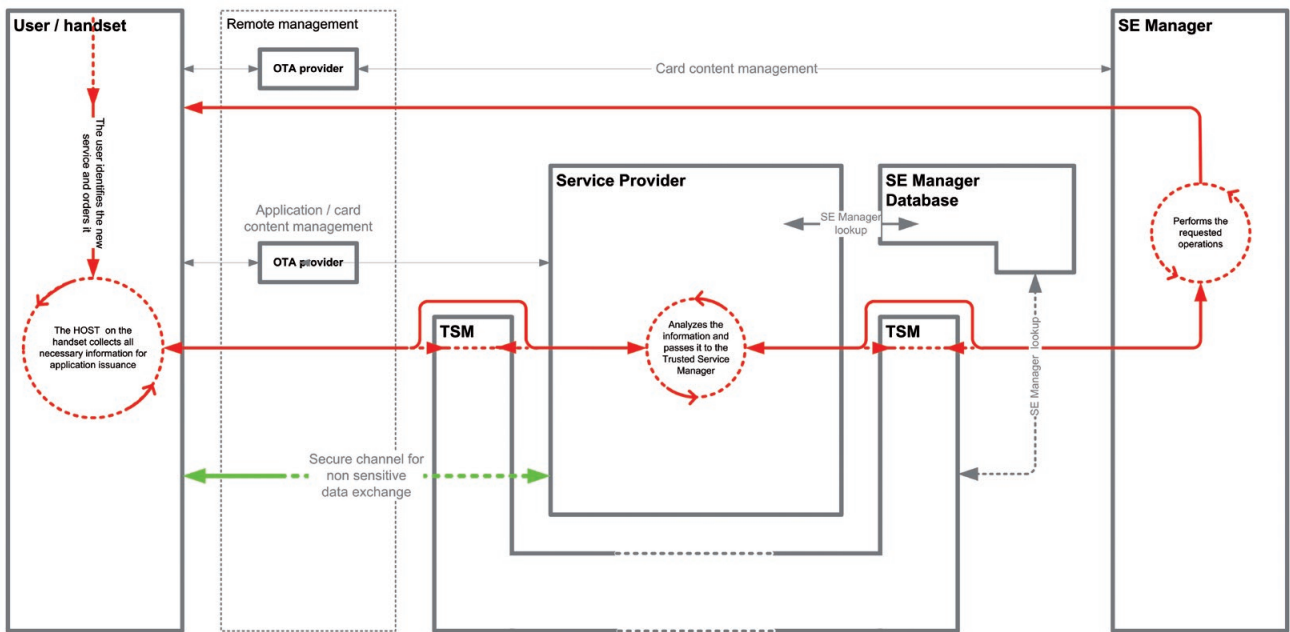
Based on the information received, the SE Issuer can perform the requested post issuance processes. These include the generation of security domains, application loading installation and deletion. The Issuer also generates specific keys for the Service Provider to ensure exclusive access to the new security domain and application.

To deliver these tasks to the user the Issuer can either use third party Service Providers – OTA providers, certification authorities or TSMs – or may 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 a confirmation response and the specific keys from the Card Issuer to access the security domain.

Alternatively, depending on the Card Issuer's policy, the Service Provider may get exclusive access to its application and assigned Security Domain, allowing it to manage its own application without interaction from the Card Issuer. This requires special management rights, which are described in the Global Platform specifications.

The process described here, **provides the necessary technical information about the user's environment to the Service Provider, allowing an automated process to be launched with the designated card issuer to seamlessly establish a new security domain and load a new application.**



Remote post issuance procedure

8.2 Other issues to consider

8.2.1 How to find the right Card Issuer – Card Issuer reference

A technical cornerstone of the dynamic post issuance card content management process is a set of technical parameters and information, possessed by the User, which can facilitate an automated procedure to establish a new secure domain for any selected Service Provider. If the necessary information is provided to Service Providers as well as to the SE Issuer, they will be able to manage a seamless deployment process.

Most of the information describes the User's operating environment – SE, handset, network, etc. – while some other elements may introduce the User. If this information is extended with the technical description of the Service Provider then all **key service information will be available that is necessary for remote service delivery requirements, and the foundation of a completely open, transparent and homogenous NFC ecosystem.**

According to our proposal the SE will contain a reference (e.g., a URL) to the current Issuer of the specific SE. This could be a pointer to a database which maintains the list of Card Issuers, or even direct access to the Issuer itself.

8.2.2 Multi SE environment – SE selection

Although current NFC handsets support only one SE, there is clearly potential that one NFC handset may host multiple SEs. Including more than one SE provides more flexibility, allows differentiation of security levels and increases the technology's business potential. At this point it is not possible to predict, given a free choice between storage on the SIM or another SE, which will be preferred by the Service Providers. There may be a number of technical, security and business issues which will influence the decision.

Three parties may make the selection decision:

- The SE Issuer – for example, if the Issuer of a SIM card is also subsidizing the handset
- The Service Provider – preference over storage devices due to objective security reasons or financial considerations, if the price of competing SEs differs substantially
- If the selection decision is delegated to Users, their primary consideration could be convenience but, depending on the business model, pricing may drive their decisions too.

The actual choice between SEs will be influenced partly by technical factors. Certain business conditions, presently unknown, may also have a major impact on these decisions. If a simple algorithm drove the selection, the following issues need to be considered in the sequence listed:

- SE capacity availability
- Security level of SE
- Control
- Cost
- Business considerations / existing business relationship between the parties
- User preference

8.2.3 Customer support

As described among the roles listed, the present model introduces a new TSM to support customers in situations where the management of multiple applications stored in the SE(s) may be just too complex or time consuming. The best examples of such a situation are when the handset is lost or when migration is necessary from one SE to another. Instead of letting the User do this task alone, which practically involves blocking and reordering each and every application again, a simple request to the TSM may solve the problem.

To get to this point however two aspects have to be clarified.

First, the User needs to decide that such support is needed. The Service Providers' various TSMs will not be able to make this decision as each will only have information about the application(s) it manages.

Second, the applications need to contain some sort of information summary which, if provided to the TSM, can describe the application in enough detail to identify the Service Provider, the user and its technical environment, and also the application itself, but which does not provide any details that could be misused.



Explore with us

StoLPaN is exploring the business potential created by bringing together new kinds of local wireless interfaces, NFC and mobile communication, and the effects of the combined technology platform on contactless services.

If you are a handset manufacturer, operator or service provider then you can bring valuable insights into our activities. So, please get in contact with us and help explore the possibilities.

For more information, please visit the project website

www.stolpan.com