A Role-Based Service Level NFC Ecosystem Model

Kerem Ok, Vedat Coskun, Busra Ozdenizci, Mehmet N. Aydin

Citation:

Ok, K., Coskun, V., Ozdenizci, B., & Aydin, M. N. (2013). A Role-Based Service Level NFC Ecosystem Model. *Wireless personal communications*, *68*(3), 811-841.

Abstract

Near Field Communication is a short range wireless communication technology allowing to communicate mobile devices within close proximity. It provides opportunity for service providers to offer various value added services to customers. NFC technology allows the usage of wide range of applications and eliminates the obligation to carry additional components other than the mobile device such as credit or payment cards, tickets, identification cards or keys. Despite its technological advantages over alternative ones, the NFC business ecosystems and services are yet to take off. The problems mainly arise with the business issues triggered by different and mostly conflicting needs of many actors in the ecosystem and several additional technical issues. In this study, by adopting a role-based service ecosystem modeling, we propose an NFC ecosystem model which perfectly specifies the roles in the ecosystem, and defines set of activities for each role, and communication structure. We analyzed NFC ecosystem in three phases as pre-installation, installation, and service usage. We have defined the activities and communication structure in the first two phases, and finally investigated the service usage phase in three different operational modes of NFC. After giving the details of the proposed ecosystem model, two use cases are given to validate the developed ecosystem model. We complete our study by discussing the requirement satisfaction.

Keywords: *Near Field Communication, NFC Ecosystem, Trusted Service Manager, NFC Applications, Service Providers*

1 Introduction

Near Field Communication (NFC) is a short range, high frequency, and low bandwidth wireless communication technology based on Radio Frequency Identification (RFID). NFC, also being used as a term pointing the ecosystem provided by the underlying technology, combines convenience of RFID in near field with the convenience of the mobile phones. It was developed through NFC Forum which was founded to advance and standardize this technology [24]. NFC communication occurs between two mobile devices within few centimeters; using 13.56 MHz frequency with bandwidth of less than 424 Kbit/s. NFC provides variety of implementations through mobile phones such as payment, ticketing, access control, loyalty, smart poster/advertising, and social networking [1, 7, 12, 20, 23, 27, 28, 31, 33].

NFC communication is performed in half duplex mode meaning that only one of the parties can send data at a time, hence when one device transmits data the other device listens. The device starting the communication is called as initiator, whereas responder to the initiator is called as target. Initiator is an active device which contains a power source, whereas target can be either an active or a passive device.

There are three devices in NFC model which are NFC reader, NFC mobile and NFC tag. NFC tag is a passive RFID device whereas the two others are active. NFC reader is used as an initiator during an NFC communication; NFC tag is used as a target, but NFC mobile can be used either as an initiator or a target based on the application requirements. Depending on how the communication is established between the initiator and the target, three NFC operating modes are developed:

- In reader/writer mode, initiator is the active NFC enabled mobile phone whereas target is an NFC tag. Initiator either writes data to the NFC tag or read data from it (Figures 1a and 1b). This operating mode is compatible with the ISO/IEC 14443 and FeliCa standards for the communication on RF layer.
- In card emulation mode, both devices are active. NFC reader acts as initiator, creates the magnetic field and reads data that is stored in a mobile phone. When NFC mobile is touched to the NFC reader, NFC mobile responds to the request of the active device. This mode is useful for payment and ticketing applications, since corresponding data is stored in the mobile phone and it is read by an external NFC reader (Figure 2). This operating mode gives smart card capability to mobile phones and uses ISO/IEC 14443 Type A, Type B and FeliCa communication interfaces.
- In peer-to-peer mode, two active NFC enabled mobile phones establish link-level communication to exchange data. In this mode, devices work according to master/slave principle. Master initiates data transfers whereas slave answers for master's requests (Figure 3). This mode is standardized on the ISO/IEC 18092 NFCIP-1 (Near Field Communication Interface Protocol-1) standard for the communication on RF layer.

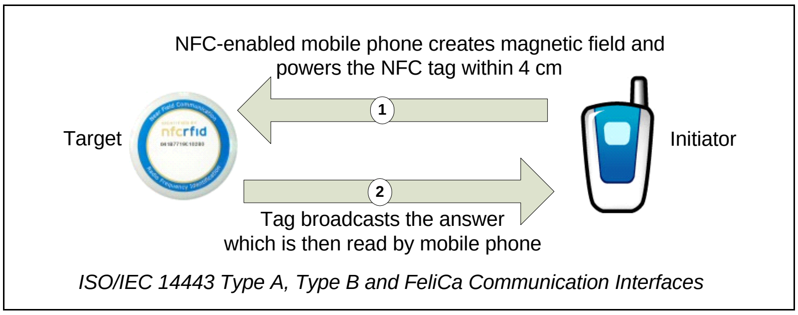
NFC-enabled mobile phone creates magnetic field and powers the NFC tag within 4 cm
1
Target
nfcrfid
Initiator
2
Tag broadcasts the answer which is then read by mobile phone
ISO/IEC 14443 Type A, Type B and FeliCa Communication Interfaces

Figure 1a. Reader Mode

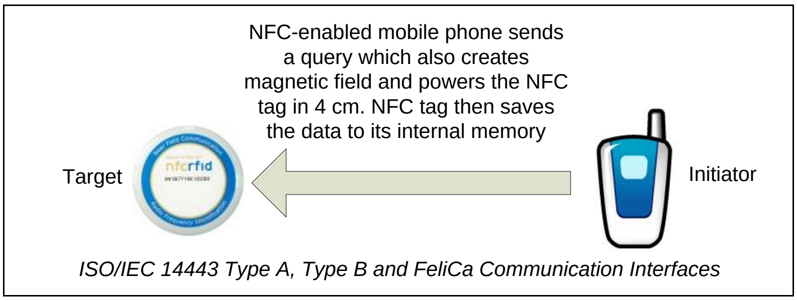
NFC-enabled mobile phone sends a query which also creates magnetic field and powers the NFC tag in 4 cm. NFC tag then saves the data to its internal memory
Target
nfcrfid
Initiator
ISO/IEC 14443 Type A, Type B and FeliCa Communication Interfaces

Figure 1b. Writer Mode

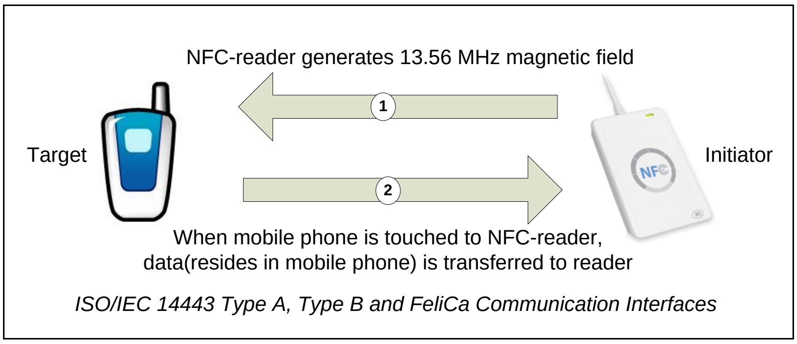
NFC-reader generates 13.56 MHz magnetic field
1
Target
NFC
Initiator
2
When mobile phone is touched to NFC-reader, data(resides in mobile phone) is transferred to reader
ISO/IEC 14443 Type A, Type B and FeliCa Communication Interfaces

Figure 2. Card Emulation Mode

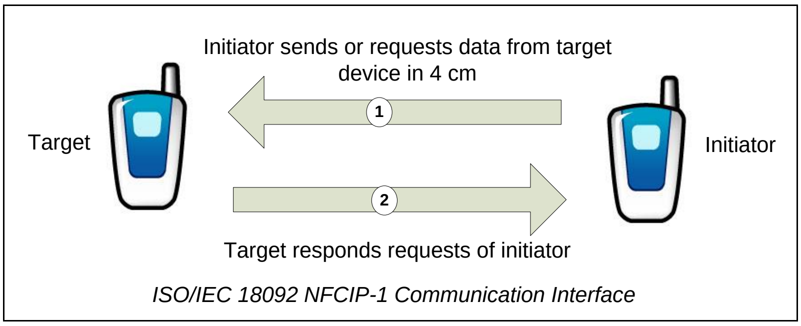
Initiator sends or requests data from target device in 4 cm
1
Target
Initiator
2
Target responds requests of initiator
ISO/IEC 18092 NFCIP-1 Communication Interface

Figure 3. Peer-to-Peer Mode

An important advantage of NFC technology is that it is based on an existing and hence tested RFID technology and also compatible with smart card interfaces; ISO/IEC 14443 Contactless Proximity Smart Card Standard (e.g. Type A which refers for MIFARE smart cards and Type B), Japanese JIS X 6319 standard as FeliCa (i.e. another contactless proximity smart card standard by Sony) and ISO/IEC 15693 Contactless Vicinity Smart Card Standard [5, 6, 24]. This implies that most of the technical essentials are already set with earlier studies. Another advantage of this technology is its simplicity [24]. All that a user needs to do in order to trigger an application installed on the mobile phone is to bring two NFC compatible devices close enough. Depending on the implementation, application may start automatically with NFC push feature. This is what people are inherently familiar with, just as simple and easy as waving your hand to get attention of your friend.

Let’s consider a ticketing application for purchasing a ticket and also involving a payment service for paying for it with NFC technology. To realize a ticketing ecosystem, some roles need to be involved. It involves a card holder as the owner of the mobile phone with an integrated smart card. Transportation Company is the one who carries the tickets from the seller to the user. Bank is the issuer of the debit and credit cards that will be used to pay for the tickets. Mobile Network Operator (MNO) provides Over-the-Air (OTA) service as required. Moreover security infrastructure and its actors are needed in order to enable secure communication and storage. On the other hand, multiple applications from many Service Providers (SPs) are to be installed and hosted on the same smart card. Many SP companies will provide a range of different services; many banks will provide payment options with credit and debit card options; and still a variety of services will be provided in the form of loyalty cards, membership cards etc. Security is at least as important as the functionality, therefore all entities should act in a particular manner and all applications should communicate each other securely in an NFC ecosystem.

As seen in an indiscriminate ticketing case, many roles are involved in NFC ecosystem. Several technical, security, and business issues arise due to requirements and demands of multiple roles. Until now the specifications, requirements, implementations, and other integral parts of ecosystems are partially studied by StoLPan [35], which is a pan-European consortium that aims to establish a secure, interoperable operating environment for NFC enabled applications. StoLPan provided analysis of life-cycle management of NFC applications and relationships between ecosystem roles [25, 36]. StoLPan adopted a complex service scenario for post issuance remote personalization process of applications. The proposed service scenario includes various roles which are classified by themselves as ones with primary roles (User, Secure Element (SE) Issuer, and SP) and support roles (OTA Provider, Certification Authorities (CA), Trusted Service Manager (TSM), Domain Agent). Primary roles are necessary to complete the functionality of the process. Another important study of StoLPan is the analysis of business and technological aspects of managing NFC based applications [3, 4]. The deficiencies of NFC based solutions and technological barriers (handset dependent technology, different interoperable technical OTA solutions and other problems) are discussed and suitable business models and processes are proposed. To handle the deficiencies of NFC technology, StoLPan introduced StoLPan mobile NFC host application which is a middleware implementation that is residing on the SE of the mobile handset [3]. StoLPan mobile NFC host aims to manage multiple NFC applications on the same smart card, and provide collaboration between entities of the value chain. In [2], StoLPan examines NFC ecosystem issues in detail. Diverse business and marketing interests of two major roles, namely SP and MNO are discussed. The requirement for a global host application is highlighted. It is stated that host application provides a transparent environment for the simultaneous operation of various NFC based service applications, by neutralizing specifics of the handset design and taking care of resource, communication management, application management and interoperability. In [17] the requirement of a Platform Manager for OTA management of NFC applications is explained. In [16] Platform Manager's importance is explained and risks of the OTA processes in an NFC ecosystem are extensively discussed.

Another work on NFC ecosystem is presented in [26]. In the proposed ecosystem, MNOs and SPs are identified as primary roles in the ecosystem, whereas users, chipset manufacturers, NFC handset manufacturers, NFC component manufacturers, and TSM are identified as secondary roles. In [21], ecosystem of an NFC based mobile payment is investigated. SE Issuer and Platform Manager are identified as key functional roles in the ecosystem. Also stakeholders of the ecosystem, three alternative ecosystem scenarios and three alternative SEs are described within the same study.

Even if some partial studies are realized on defining the content of NFC ecosystems, no work has shown a complete ecosystem model in terms of communication structure. In this paper, we propose a complete service level NFC ecosystem model. The proposed ecosystem model highlights the requirements and importance of a neutral, trusted entity as TSM centric deployment of NFC services which allows communication and interest protection of each actor within the ecosystem, and also reduces the complexity of NFC services' business environment. This paper provides the proposed TSM centric ecosystem model with its well defined communication architecture among actors and usage of this new service model in each operating mode clearly.

We think that major contributions of this paper are twofold: defining the requirements of NFC ecosystem which are not defined explicitly so far, and also designing a TSM centric NFC ecosystem model that adopts role-based service level communication structure. Some ecosystem related studies are already mentioned above; however the communication structure is not detailed at a service level. Another major contribution of this paper is the proposal of centralized application pool under TSM's roof for efficient application management which is given in section 4.3.1. Application pool brings many advantages for an NFC ecosystem and they are highlighted in the related section.

In this very first section, the basics of NFC, its ecosystem definition, and the importance to provide a complete solution for the NFC ecosystem together with the partial solutions so far are given. Section 2 gives the research backgrounds that will be used in the ecosystem study together with the technical framework. Section 3 describes our research approach on ecosystem modeling. In section 4, the detailed requirements of an NFC ecosystem, the roles of the ecosystem model together and actors' communication are explained. In section 5, the generic model of service usage phase for each NFC operating mode is given and then the use cases to test the proposed ecosystem modeling follow. In section 6, we evaluate our work by discussing functional requirements of the proposed model. Finally, we conclude our work with conclusion and future researches in Section 7.

2 Research Background

NFC services will be publicly available to all mobile phone users, and therefore it should be designed to be used by vast number of users. OTA transfer, smart card management (installation, and maintenance of applications), and personalization are important issues for each NFC application. In this section we give background information of the related technologies and latest studies.

2.1 Secure Element and Over-the-Air Technology

Applications those require secure usage should be installed to the SE of mobile phone. When a user wishes to use more than one application, each one will be installed onto the same SE on the same smart card. SE provides the security including confidentiality required to support business models [8]. In a successful NFC ecosystem, each mobile phone definitely needs a SE in order to install and store applications.

Several studies have already been conducted to analyze SE alternatives for NFC technology. In [29], four SE alternatives are evaluated as Baseband processor, Embedded Hardware, Secure Memory Card (SMC), and Universal Integrated Circuit Card (UICC). In [21], SE alternatives are assessed among UICC, SMC, and embedded chip. It is clearly stated that UICC has many advantages over other alternatives. On the other hand SMCs are developed which enable NFC and RFID read/write capabilities in non NFC enabled mobile devices and also have embedded SE [32]. Moreover iCarte is developed for iPhones which also enables same functions for iPhones [14]. These developments will likely to lead users to multiple SE alternatives, at least UICC and SMC.

With the emerging new NFC services, accommodation and remote management of applications (i.e. installation, personalization, update, termination, card block, unblock, re-issuance, PIN reset, change, parameters update) on the SEs' of mobile devices via OTA technology became important concern. Currently, UICC based SEs appears to be the most popular way of promoting NFC services using OTA technology. With OTA technology, new NFC applications can be delivered to a UICC via OTA and managed easily, regardless of time and place [34]. However; access to embedded SE and SMC can only be accessed from the outside over the air through a J2ME midlet using a special API JSR#177 [36].

2.2 GlobalPlatform Specifications

GlobalPlatform is a cross industry membership organization comprising more than 50 organizations as of today, ranging from payments and communications industries to government sector and vendor community. Involved companies are the pioneers to promote a global infrastructure for smart card implementation across all possible industries. Their goal is to enable interoperable technical specifications necessary to support smart cards and appropriate smart card system management for Card Issuers (CIs). GlobalPlatform provides a card specification which is currently accepted as a proper card model and offers secure and flexible multi-application card content management (i.e. loading, installation, extradition, registry update, and removal of card content) functionality during a card's life-cycle.

We highlight GlobalPlatform as major SE and smart card specifications. These specifications are necessary to support three types of SEs for NFC technology which are

UICC, embedded SE, and SMC. GlobalPlatform Card Specifications also provide the necessary functionality for our proposed ecosystem model in terms of secure storage of keys, key management, and distinct security domains of card architecture. GlobalPlatform Card Specifications are comprised of a number of logical and physical components those aim to provide application interoperability and security in an issuer controlled environment [8, 18].

When we study the actors in the GlobalPlatform Card Specifications, we see Card Manager as central administrator of the smart card, CI, and Application / Service Providers which are the companies (banks, mobile network operators etc.) those have a business relationship with the CI. In accordance with [9], CI is the controller of the smart card which holds ultimate responsibility of the smart card, and is also responsible from the security of the smart card together with other responsibilities as well.

GlobalPlatform is designed to provide maximum flexibility to the CI as well as its business partners regarding card content management which includes loading, installation, extradition, registry update, and removal of card content. Due to this flexibility, CI can delegate card content management functions to an Application/Service Provider - delegated management content loading - with or without authorization. At this point, appropriate content management policy on smart cards has become a fundamental concern; flexible, easy, safe and dynamic structure of a policy is required, rather than neither completely closed nor completely opened multi-application smart card policies [30]. In our proposed ecosystem model, in order to defend against potential vulnerabilities of the ecosystem, most of the role and functions of CI is mostly transferred to the TSM who is a neutral and trusted party. Therefore SE is controlled by TSM with the transmission of its Master Key from CI, which will be described in section 4.

Another major component of GlobalPlatform is the notion of security domains. Each entity has its own security domain (Issuer Security Domain (ISD), Application Provider Security Domain (APSD) and Controlling Authorities' Security Domain (CASD)). Security domains of GlobalPlatform act as on-card representatives of off-card authorities and have their own security architecture [18, 19]. They are responsible for cryptographic functions, key handling, key generation, and secure channel protocol implementation.

In most of the SEs, there will be multiple applications running on the same platform at a given time and those applications need to share intended data with each other. Our proposed ecosystem will provide those features with the security implementations. In order to manage application domains in SEs, an NFC loyalty system called NFC Loyal is developed in [27]. This system enables sharing transaction data among payment and loyalty applications which are previously installed and configured by the NFC enabled mobile device owner. This beneficial model is completely based on GlobalPlatform Card Specification that provides appropriate framework to enable NFC Loyal.

Another important specification provided by GlobalPlatform is the "GlobalPlatform Messaging Specification" which defines a set of standard messages for data exchange between entities in a smart card environment [10, 11]. In order to provide a standard infrastructure and to avoid proprietary solutions and therefore to exchange information seamlessly, promote standard interactions between players, as well as facilitate easy integration of new players in smart card ecosystem. It examines interoperability at three major levels; business data (i.e. common vocabulary), business process (i.e. role, responsibilities, process and constraints) and data exchange (i.e. data structure, integrity and security of information, error handling etc.).

GlobalPlatform proposes three card content management models; simple mode, delegated mode and authorized mode. Simple mode is completely card issuer centric model, whereas delegated mode and authorized mode are more TSM centric models. GlobalPlatform Messaging Specification supports all these three deployment models [10, 11].

These models cover application loading and personalization processes on UICC based SEs. Figure 4 illustrates these three models when UICC based SE option is used for deployment of NFC services. Today MNOs play an important role as UICC issuer and even they may act like a card manager. MNO holds the essential keys on the card. Thus SPs and other entities such as TSM are mainly dependent on the CIs. It is possible to see that MNOs can delegate the card content management processes by delivering a management token to the TSM, or TSM can perform card content management without authorization. These deployment models are also applicable to other SE options such as embedded hardware, SMC on NFC mobiles [11].

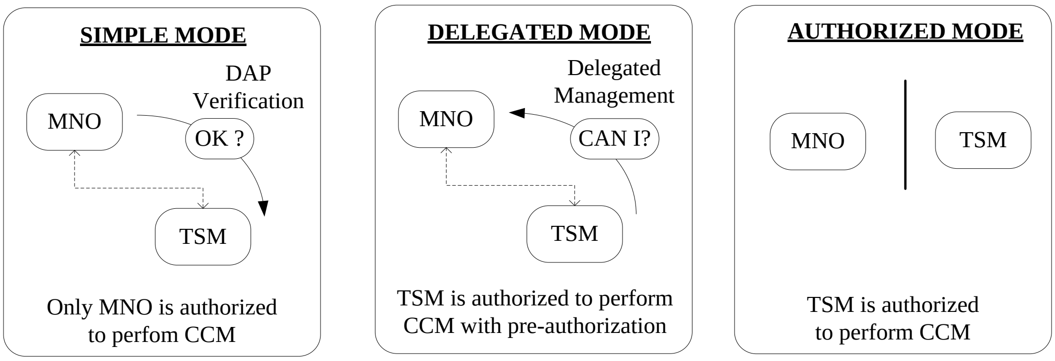
SIMPLE MODE
DAP Verification
MNO
OK ?
TSM
Only MNO is authorized to perfom CCM
DELEGATED MODE
Delegated Management
MNO
CAN I?
TSM
TSM is authorized to perform CCM with pre-authorization
AUTHORIZED MODE
MNO
TSM
TSM is authorized to perform CCM

Figure 4. Application Management Models on UICC based SE [10]

3 Research Approach

This research adopts role-based modeling as a technique to analyze actors and their relations in an NFC ecosystem.

It is defined in [37] that, the functions and activities of a business entity may overlap with other entities over time in an ecosystem model, but most of the roles do not change or do not overlap. Since NFC ecosystem studies are still in development progress, it will be difficult to change them according to an evolving business model when entities and their relationships are modeled directly. However the roles being the aggregation of common activities (all operational functions played by the role) will have very limited changes. Thus, the technique, role-based service ecosystem modeling [31] we used allows examining the roles and activities of each role in detail. In this modeling technique, each business entity may act as an independent agent and it can play one or more roles according to its own business model over time.

In order to attain the activities and roles, the requirements of the NFC ecosystem are needed to be defined. So, we first identify the operational needs of an NFC ecosystem. After gathering the ecosystem requirements, we define and describe activities and roles to satisfy those requirements. Then the service ecosystem modeling is performed iteratively that consists of required roles and activities (Figure 5). In the proposed ecosystem model, we present three phases (pre-installation, installation, and service usage) as seen in Figure 6, since operational activities and involved roles differ in each phase. Moreover, we present the generated generic service usage model for each operating mode. The service usage phase needs to differ in each mode since performed communication structure differs by mode. Finally, we test the viability of the model by applying two use cases.

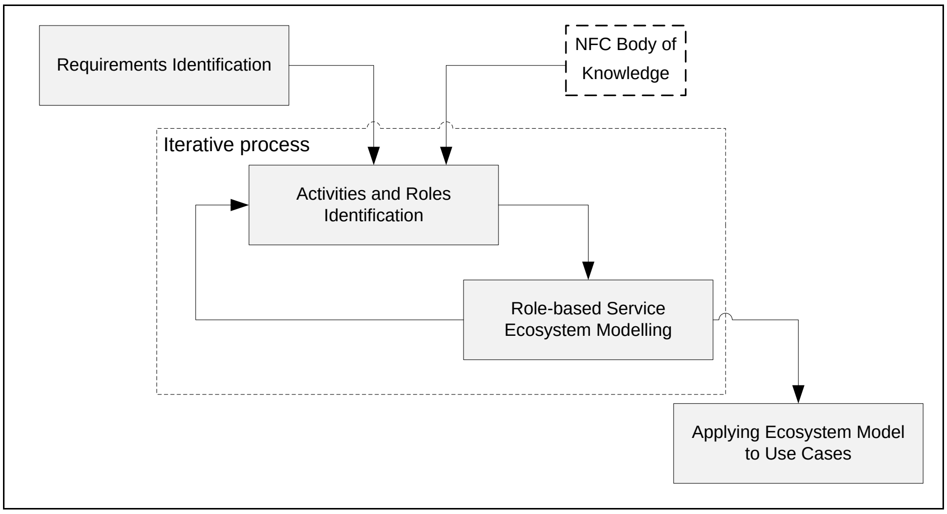
Requirements Identification
NFC Body of Knowledge
Iterative process
Activities and Roles Identification
Role-based Service Ecosystem Modelling
Applying Ecosystem Model to Use Cases

Figure 5. Research Approach

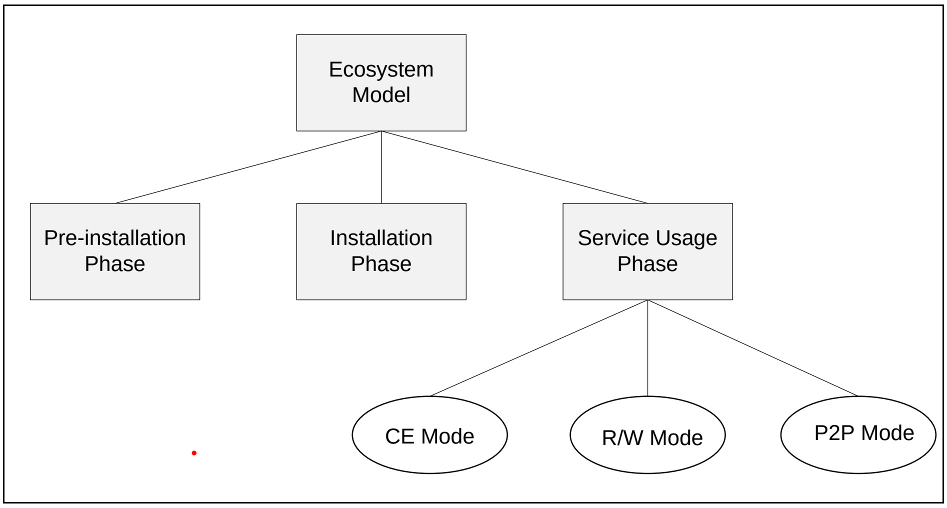

Figure 6. Ecosystem Modeling Phases

4 Role-Based NFC Service Ecosystem Modeling

Starting from this section, we describe our proposed ecosystem model. In this section, we first define the requirements of an NFC ecosystem, and the roles in a concrete fashion that are involved in the proposed ecosystem. Then we describe the ecosystem model with its communication structure.

4.1 Ecosystem Requirements

Related studies on NFC ecosystem are already given in introduction section. Despite some studies are performed, we have observed that even the requirements of an NFC ecosystem are not defined explicitly so far. After an extended review of current ecosystem studies and problems that arise, we define requirements of an NFC ecosystem as following:

- **Competitive environment between SPs:** There will be corporate companies as SPs as well as local or newly established firms. In order to attract new and innovative services to make users happy, a competitive environment among SPs is required to be set up.
- **A neutral entity to manage and secure the ecosystem:** Each company's intention is to gather as bigger profit as possible, so they would try to gain positions of higher importance in the ecosystem. A neutral role is needed to manage and secure the ecosystem that all other entities can trust to it and agree on it.
- **A neutral entity to support SPs and users:** A neutral role is needed in order to support SPs and users by securely downloading applications to mobile phones. This neutral role should be able to personalize and manage locking, unlocking and deleting functions on the SE, based on the requests of users and SPs. It should be able to provide management keys of applications to SPs [26, 36].
- **Each SP to manage its own application in SEs:** Many SPs can install their applications to mobile phones after which they need to share the same smart card. Management of the cards needs to be handled in such a way that many SPs can access their applications securely without interfering each other [4, 25].
- **Compatibility with major SEs:** There are major SE alternatives as described in section 2. We take GlobalPlatform as the smart card and SEs standards provider. According to our opinion, ecosystem should be compatible with these major SEs those are based on GlobalPlatform Card specifications.
- **Business agreements:** Agreements between entities should be signed in order to satisfy trust requirements of the parties involved in the ecosystem.
- **Communication security:** The communication between actors should be secured in a well developed ecosystem.
- **General security:** Devices (tags, readers, SEs), short range communication of the technology and backend systems should also be secured as part of the NFC ecosystem. Details of general security issues are given in the section 4.2.

4.2 Security Requirements

No system is complete unless the adequate security services are defined and detailed in parallel to the system design. In this regard, we consider the following security issues related to NFC based systems:

- Security concerns related with NFC tag
- Security concerns related with NFC reader
- Security concerns related with SE
- Security concerns related with short range communication
- Security concerns related with middleware and backend systems

When talking about NFC ecosystem, we must heal all the associated risks as well.

4.2.1 Security Issues on NFC Tag

NFC tag is actually an RFID tag; hence the security concerns are identical. The attacks against NFC tags can be categorized as:

- *Tag Cloning and Tag Impersonation* are about creating an identical copy of a legitimate tag to be used for malicious purposes.
- *Tag Content Changes is* changing the content of the tag for a malicious purpose which can be performed by various attacks such as spoofing attacks,

manipulating tag data, denial of service (DOS) attack etc. The spoofing attack examples are URI and URL spoofing, phone call spoofing and SMS spoofing which potentially result in theft of services or identity.

- *Tag Replacement and Tag Hiding* is sticking a malicious tag on top of the original tag or replacing the original tag with a malicious tag is enough to let the system work as the attacker desires. In case of sticking a new tag; it is possible to disable the old tag. Another method to attack passive tags is to break the write protection of the tag and overwrite it with malicious data.

NFC tags can be partially protected using techniques such as encryption.

4.2.2 Security Issues on NFC Reader

NFC reader is similar with the RFID reader therefore their security concerns are similar as well. The major attacking methods to NFC readers are removal or destruction of them and impersonation.

4.2.3 Security Issues on SE

Mainly, the most important attacks on the SEs are the side channel attacks. Side Channel Attack is observing a side channel while information is being processed. This means that an attacker seeks to derive information by observing how the characteristics of a smart card change as it process different information. Some examples of side channel attacks are listed as timing analysis, simple side channel analysis, and fault induction attack as defined in [15]. According to the same study, the countermeasures that can be implemented to prevent side channel attacks include constant execution, random delays, and randomization.

4.2.4 Security Issues on Short Range Communication

An obvious threat for the wireless media is eavesdropping. The short range communication requirement imposes some prevention mechanism, but a risk still exists when high capacity devices can be used by the attackers. The main question is how close an attacker needs to stay, in order to retrieve a usable RF signal; but unfortunately, there is no exact answer to this question since there are many parameters those affect the answer [13]. As the data is intercepted, other more advanced techniques such as man-in-the-middle (MIM) attacks can be performed as well. Other similar techniques might be data corruption, data modification, data insertion, relay attack, or replay attack as the data is intercepted.

One effective and obvious solution may seem to create a secure channel using encryption techniques [13], which increases the cost for communication. Advanced attacks are also harder to perform when high data rates are used.

4.2.5 Middleware and Backend System Security

An NFC based system contains NFC readers, NFC mobiles and NFC tags in technical terms. But a complete NFC system includes servers to store and manage data such as banking servers, credit card middleware, authentication subsystems, etc. Hence, security of an NFC system is not complete unless the security of all ingredients of the complete system is provided. Databases may be extremely sensitive if they contain valuable information such as credit card numbers. Companies may even lose the confidence of consumers unless they prevent the damage or quickly correct it. The business sections of newspapers and magazines have reported many stories regarding the companies which suffer major setbacks by losing customers due to an IT related failure.

4.3 Roles

After defining the requirements, we have identified following roles in the ecosystem to satisfy those requirements.

- **Trusted Service Manager** is a neutral and trusted party. In our ecosystem model, we propose one central TSM that all parties can trust.
- **Card Holder (User)** is the owner of the SE as well as the mobile phone.
- **Service Provider** is the party wishing to offer an NFC service to its customers by deploying an application on the SE. There can be many competing SPs in the ecosystem and each SP can have many applications and services that wish to deploy.
- **Card Issuer** is the issuer of the SE.
- **Certification Authority** is an authority that is recognized by everybody to issue digital certificates.
- **OTA Provider** is the party that is responsible for establishing secure end-to-end communication.

4.3.1 Trusted Service Manager

TSM, which is one of the major roles, has the most strategic importance in proposed ecosystem. Its main function is to establish and manage a trusted environment by providing a secure network between MNOs, SPs and card holders. Integrating TSM into the ecosystem enables secure communication and interest protection of each entity, and also reduces the complexity of business models.

One can find various models which do not include TSM as an actor, but we contend that TSM brings many opportunities to the ecosystem such as coordination, simplifying, enabling or facilitating communication effectively. TSM provides a single point of contact for users, MNOs and SPs as financial institutions, banks, transit authorities, retailers and others who want to provide NFC enabled payment, ticketing, or loyalty services to customers (Figure 8).

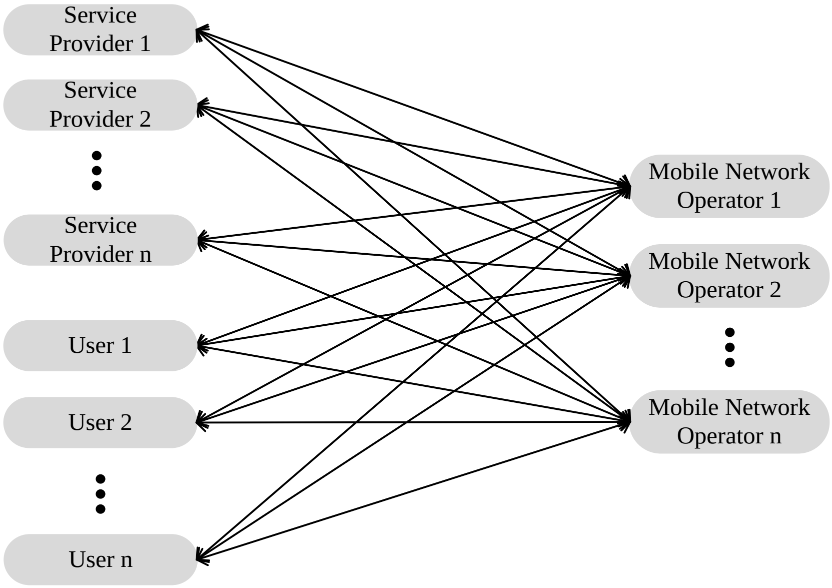
Service Provider 1
Service Provider 2
Service Provider n
User 1
User 2
User n
Mobile Network Operator 1
Mobile Network Operator 2
Mobile Network Operator n

Figure 7. A Complex NFC Ecosystem without TSM

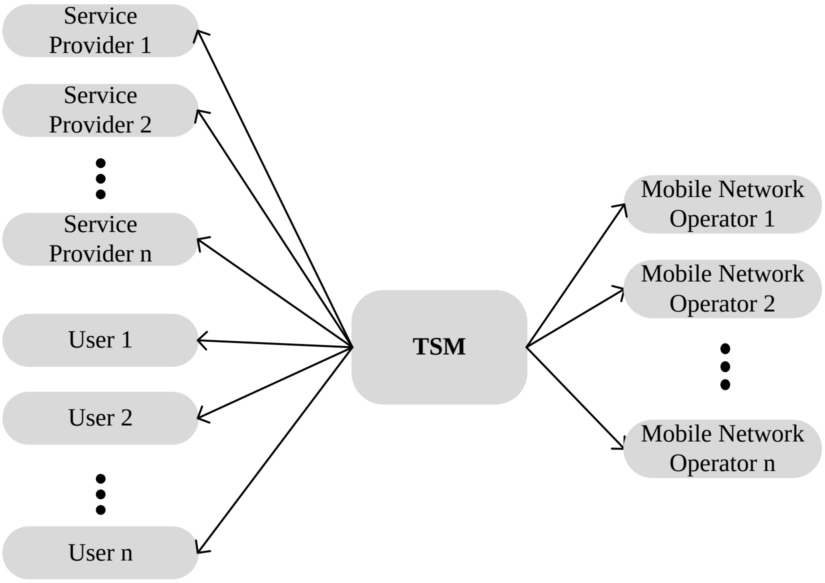
Service Provider 1
Service Provider 2
Service Provider n
User 1
User 2
User n
TSM
Mobile Network Operator 1
Mobile Network Operator 2
Mobile Network Operator n

Figure 8. Ideal NFC Ecosystem with TSM

TSM is primarily responsible for securely provisioning and managing the life-cycle of the NFC based applications and provides a flexible OTA solution for NFC application life-cycle management. It authorizes applications prior to it is downloaded to mobile phones. TSM should also be able to manage (delete, update, lock, unlock) the applications those are installed to SE, on behalf of card holders and SPs. Its trustworthiness is critical to manage and control multiple applications in one SE, and hence makes concurrent applications execute on the same SE.

In order to control the SE exclusively, TSM requests SE's master key from CI as will also be detailed later. Master key is unique for each SE that can be used to exclusively control that related SE. Master key enables many functionalities by the owner such as creating security domains in SE, controlling each security domain, installing applications to SE, as well as some additional functionalities [21, 22]. In our proposed ecosystem, TSM is the owner of the master key as the trusted party. TSM requests this key from CI and as the master key is transferred to TSM, it can start handling SE functions.

It can be challenging for SPs to adapt NFC to their business processes without any further help. TSM plays an important role by providing the necessary technology support and services to SPs. TSM also guarantees confidentiality between SPs and MNOs during application installation; pre-issuance (service delivery) and post-issuance. Only one central and neutral TSM will manage contractual relationships between many MNOs, financial institutions and other SPs.

When NFC services will start to spread, there will be many SPs and thus many NFC applications will be offered to users. However users should not deal with spam-like applications and security thoughts. They should be able to use install and use any NFC service easily. In order to provide more secure and efficient application management, we propose using an application pool managed by TSM which will provide a central location for application housing. Applications uploaded by SPs will be offered to users, and users those tend to use one of those applications will be able to download it from a centralized location.

The advantages to use a centralized application pool under TSM's roof are:

- **Checking the needs of applications; convenience:** The security requirements of the applications need to be satisfied prior to the application installation. In the proposed application pool, TSM is the party for checking the security and convenience of the applications. Any insecure and inconvenient applications is not accepted and not published in the application pool.
- **Easy update of applications:** Handling application updates will be much easier. If there is a newer version of the application in the application pool, system will update the application in SE.
- **It is easy to place a tag for anyone:** The ecosystem requires installation of the application after the user touches her mobile phone to an NFC tag containing the download information. Since SPs will be able to place NFC tags into anywhere such as restaurants, stadiums etc., users should trust to this way of application installation. Providing application pool as the trusted central location for application installation, the users will be convinced about the security of the system.
- **Application search:** Users will be able to search the application pool via host application which is pre-installed on smart cards and manages other NFC applications. SPs will also benefit from this application pool, since users will be able to install applications without the need of SP, and SPs will not be kept busy by answering the requests of each user.
- **Cost deduction for SPs:** SPs will not need to provide necessary technology infrastructure for application housing, which will minimize the cost that the SPs will suffer.
- **Preventing spam-like applications:** End users will not need to deal with fake applications. Users' security concerns should be minimized, because they hold their private and sensitive information such as credit card data in the SE. They should be able to install applications without any hesitation.

As described above, a centralized application pool is critically necessary. Both SPs and the users will benefit from this centralized application installation.

4.3.2 Card Holder

The main actor of the NFC ecosystem is of course card holder being the owner or the SE, smart card, and the mobile phone. She initiates the NFC service by touching her mobile phone to a tag or another NFC device, and starts using the benefits of the ecosystem afterwards. Card holder also decides:

- Which application is to be installed,
- Whether a proposed application is to be installed or not.
- Which application to use among different alternative applications
- How to configure any application that are installed previously,

Since selection of NFC applications depend on card holders' preferences, their security and other concerns should be minimized in order to attract them. Application pool is one of the things to handle these concerns.

4.3.3 Service Provider

SP is the one who creates applications, offer them to the card holders by uploading it to the application pool, and tries to get a bigger share from the ecosystem. SPs are mostly corporate companies serving huge amount of people such as banks, transportation companies, and retailers. In rare situations they can be local or small firms who want to deploy a service to a small group of people.

When an SP desires to make an application available to users, it needs to submit their application to TSM. After TSM checks and approves validity of the application, it publishes the application into the application pool after which users can use it. This process will be described in section 4.4 in detail.

4.3.4 Card Issuer

CI is the authority that produces and issues the SEs. Due to existence of many SE alternatives, there is high probability that there will be many CIs which means a strong competition environment in the NFC ecosystem. CI's important advantage is that it is the authority who owns the master key of the SE. Master key is produced at chip personalization phase, and it can either be produced by the chip manufacturer or chip personalization bureau [21, 22]. In order for TSM to control the SE, this master key should be transferred to TSM as the user decides to use NFC services.

We have already mentioned UICC and the NFC enabled SD card as two important SE alternatives. The CI actually differs according to which alternative is used by the user. If the user chooses UICC as the SE, MNO of the user will be the CI. In the contrary, when user chooses NFC enabled SD card, corresponding SD card manufacturer will play CI role.

According to the GlobalPlatform Card Architecture, SE has its own security domain called as ISD. ISD represents the Issuer's interests in the smart card, holds keys, and performs cryptographic operations in order to verify any requests for changing the card content. GlobalPlatform provides maximum flexibility for CIs regarding Card Content Management. The one who has the master key of the card can delegate Card Content Management functions to an Application/SP.

4.3.5 Certification Authority

CA is a trusted party that is responsible for issuing digital certificates. In the NFC ecosystem, CA is the party that issues secure digital certificates. SPs need to obtain digital certificates for themselves from CA. Also each user needs to obtain her digital certificate for authentication. These qualified digital certificates are issued according to the described PKI Technology.

4.3.6 OTA Provider

OTA is the name for Over-the-Air communication technology that enables secure wireless communication between two end parties. It provides transmission and reception of application related information in a wireless communication system [36]. As already mentioned, OTA enables remote download, installation and management of applications such as updating, activating or deactivating an application on smart cards [4, 36]. Thus, OTA providers play a crucial role during remote application download and management. Providing flexible and interoperable OTA solution is a key requirement in the NFC ecosystem.

Some MNOs on the world are capable of providing OTA communication using their current technology infrastructure. TSMs can also provide this service if the required OTA infrastructure is set up in TSM's framework. Since TSM also handles card content management functions, the more proper solution is to set up OTA platform in TSM infrastructure.

4.4 How Proposed Ecosystem Works

In this section we describe our proposed ecosystem processes. In the proposed NFC ecosystem the following two assumptions are accepted.

- **GlobalPlatform Card Specifications are valid:** As described in [8], GlobalPlatform provides valuable, interoperable SE and smart card specifications which are universally recognized and implemented as well. Currently most of the CIs produce smart cards based on these standards. In order to provide the ecosystem model based on universally recognized standards, smart cards that are used along with the ecosystem should have been compatible with GlobalPlatform standards.
- **Card Manager is pre-installed on smart cards:** An NFC host application is needed on smart cards in order to set up security domains for the user and application personalization on smart cards. This application also stores TSM's root certificate in it. It updates itself whenever an update command is issued by TSM. We assume that the global card manager host application is already developed; its security is verified, and is also pre-installed onto smart cards.

As described earlier, our ecosystem model consists of three phases; pre-installation phase, application installation phase, and service usage phase.

1. **Pre-installation phase:** In pre-installation phase, required entities should obtain their certificates and sign their business agreement. It is simply the preparation of SPs and users for application installation to smart cards. This phase mainly consists of obtaining digital certificates, signing business agreements, and submitting service applications to TSM. Pre-installation phase is depicted in Figure 9a and its details are described afterwards.

2. **Installation phase:** Installation phase includes installation of service applications to the SE. Business agreements of the related service applications are signed between user and TSM prior to the installation. Another important process in this step is the transfer of user's smart card's master key from CI to TSM. This phase is depicted in Figure 9b and its details are described afterwards.
3. **Service usage phase:** Service application is already installed to the SE, thus the application is ready to be used by the user. Roles involved in this phase can be seen in Figure 9c which includes all of the three NFC operating modes. Each NFC operating mode has a different service usage model and it is further described in section 4.5.

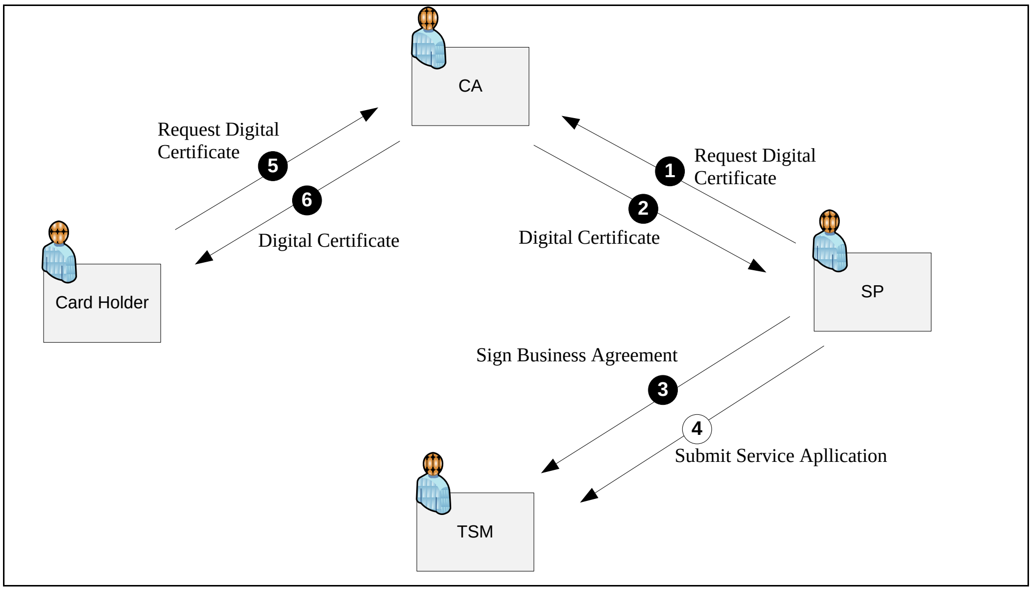

Figure 9a. Ecosystem Communication in Pre-Installation Phase

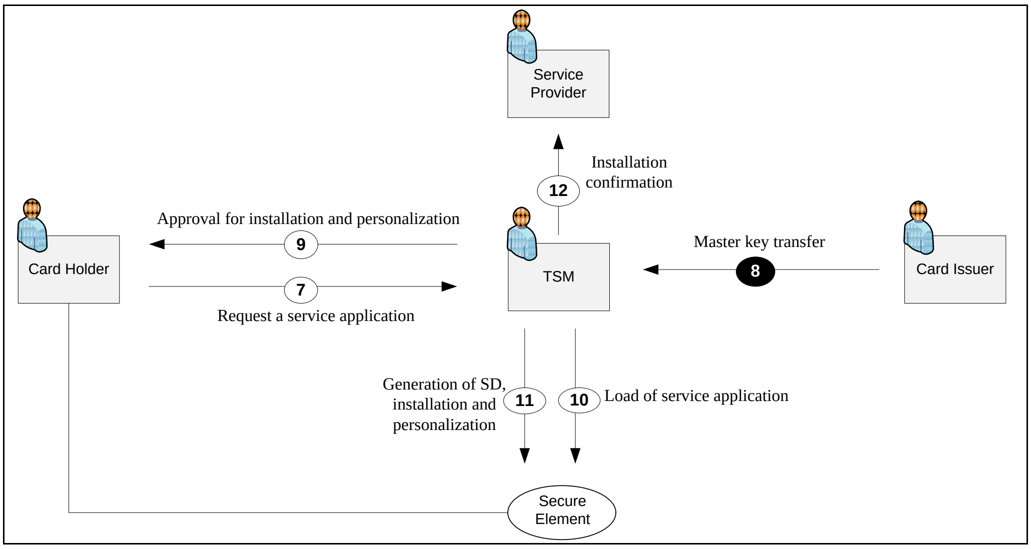
Service Provider
Installation confirmation
12
Approval for installation and personalization
9
Card Holder
TSM
Master key transfer
8
Card Issuer
7
Request a service application
Generation of SD, installation and personalization
11
10
Load of service application
Secure Element

Figure 9b. Ecosystem Communication in Installation Phase

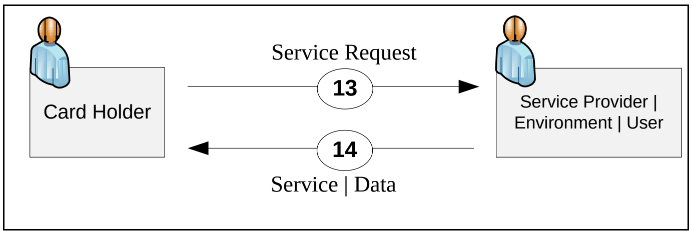

Figure 9c. Service Usage Phase

Black filled circles are needed one-time only and white filled circles are repeated for each application.

1. **Digital certificate request by SP:** SP requests its digital certificate from a CA if it didn't obtain it earlier.

2. **Digital certificate transfer to SP:** CA prepares the certificate and sends it to SP. Each SP obtains digital certificate only once, use it whenever it needs.

3. **Business agreement between SP and TSM:** SP needs to sign business agreement with TSM before deploying an application to users' mobile. SP signs business agreement and sends the agreement to TSM.

4. **Submitting an application:** SP sends an application together with the application's service agreement to TSM. When TSM verifies the application and confirms the agreement, it publishes the application into its application pool and applications can be downloaded by the users afterwards. This step also recurs for each application that SP wants to deploy to users.

5. **Digital certificate request by user:** User requests her digital certificate CA if she didn't obtain it earlier.

6. **Digital certificate transfer to user:** CA prepares the certificate and sends it to the user. User should obtain its certificate one-time and renew when it expires.

7. **Service application request:** User requests a service application from TSM via NFC service tags or manually using NFC host application (searches TSM's application pool database). When user tries to get a service from a SP, host application automatically requests confirmation from the user to request the corresponding application from TSM, if that service application is not already installed in smart card. Then, user is requested to sign the application's service agreement by the host application. Service agreement is afterwards sent to TSM.

8. **Master key transfer:** TSM requests master key of the SE on the user's mobile (if it did not receive before) from CI in order to take control over the SE. TSM requests this master key during the very first application installation phase to the SE. This step is valid for only SE applications and required one-time only for each SE.

9. **Approval for installation and personalization:** After the application is loaded to the user's mobile phone, TSM gets approval from the user for installing the application to the mobile and personalize the service.

10. **Loading service application:** As user approves the installation of the requested service application, it is OTA downloaded to the user's mobile.

11. **Generation of security domain, installation and personalization:** The SE receives a "CREATE SSD" command, after which Supplementary Security Domain (SSD) is created by the ISD. Loading and personalization of all applications are performed using GlobalPlatform content loading commands [8]. After creation of security domains of applications and personalization, applications can be loaded and installed through "INSTALL [for load]" command and one or multiple "LOAD" commands. Installation is personalized through "INSTALL [for personalization]" command and consecutive "STORE DATA" commands. Alternatively, depending on the TSM's policy, the SP may get exclusive access to its application and assigned Security Domain, allowing it to manage its own application without interaction from the TSM which process is called "delegated card content management". This step is valid for only SE applications.

12. **Confirmation to SP:** Once the requested operations are performed and the required data is loaded onto the mobile phone, SP receives a confirmation response. (If installed application is a SE application) SP receives specific keys from the TSM to access its application's security domain on the user's SE.

13. **Service request:** User requests service from SP/User/Environment by touching her NFC enabled mobile phone to an NFC tag. The entity handling user's request differs based on the NFC mode as it will be discusses in the next section.

14. **Provide service or transfer data:** When respondent entity receives the service request from the user, it responds to this request by providing either service or data. Service usage differs in each NFC mode as it will be explained in section 4.5.

4.5 Service Usage in each NFC Operating Mode

Service usage phase involves the usage of installed applications and services on the SE as described earlier. Usage of services in each NFC operating mode differ from each other, because each service runs on a specific mode and the interaction of the user with NFC objects and also involvement of roles differs in each mode as well. Additionally, applications can be stored and executed either in SE or in mobile phone's storage area. Applications stored in SE are called as SE applications which require secure storage and execution area. On the other hand, interface applications are the ones which run inside mobile's storage. This type of applications are generally used for both reader/writer and peer-to-peer modes. Moreover, an interface application is indeed needed for each SE application in order to interact with it and display information to the user (e.g. after a credit card transaction), since SE applications run inside SE cannot manage any displayable object. Despite that most of the SE applications are card emulation mode applications, reader/writer mode and peer-to-peer mode applications can also use SE applications to store valuable data.

In card emulation mode, user uses her mobile phone as a smart card, and interacts with an NFC reader. Generally SP owns the NFC reader which is possibly connected to the Internet as well. So user connects to her SP through an NFC reader. In reader/writer mode, user interacts with an NFC/RFID tag and uses her mobile phone as an NFC reader. In this process, SP is not directly included, because NFC tag is a passive device which acts as simple data storage media. If tag stores a URL or a web service address, a web service can assist user to connect to SP. Also an NFC tag can be used to run a SP's application automatically using NFC push feature. In Peer-to-Peer mode, user interacts with another user through her NFC enabled mobile phone. In this mode SP is able to provide service to users through its service application such as sharing a ticket or a coupon. SP is not directly active in the process, meaning that users do not communicate with SP. However when users want to use the shared object in this operating mode, SP will be included in the process as the validator of the object. We will give details of the service usages of each mode in this section and after which we will test the service usages with use cases.

4.5.1 Reader/Writer Mode

In reader/writer mode, SP is not directly included in the process. However if the data stored in tag is designed to be used for additional services over Internet, SP can make user to connect to it. Figure 10 shows the framework for service usage of this mode.

1. **Service Request:** User requests service by touching her mobile phone to an NFC tag. As the tag receives the energy, it uses the energy to reply the request.
2. **Data Transfer:** The data that resides in the tag is transferred to mobile phone.
3. **Processing within device:** When data is transferred to mobile phone, it can be used for several purposes such as running an application with push registry feature, displaying data to user, or processing data for additional purposes etc.
4. **Additional Service Usage (optional):** This step is optional and takes advantage of the mobile phone's capabilities. When data is processed within mobile phone, it can be used for further operations through Internet such as connecting to SP by opening a web-based service.

4.5.2 Card Emulation Mode

As stated above, card emulation mode is the only mode that directly connects SP and user through SP's NFC reader and user's mobile phone. Figure 11 depicts the framework of the service usage in this mode.

1. **Service Request:** User requests service from SP by touching her mobile phone to NFC reader. Required data is transferred from mobile phone to SP through NFC reader.
2. **Background Services:** SP runs required background services. Examples to these services are credit card authorization, and ticket validation.
3. **Service Usage:** SP returns a service to the user such as opening a turnstile, printing a paper ticket etc. It can also send some digital data to user such as a coupon, ticket etc.

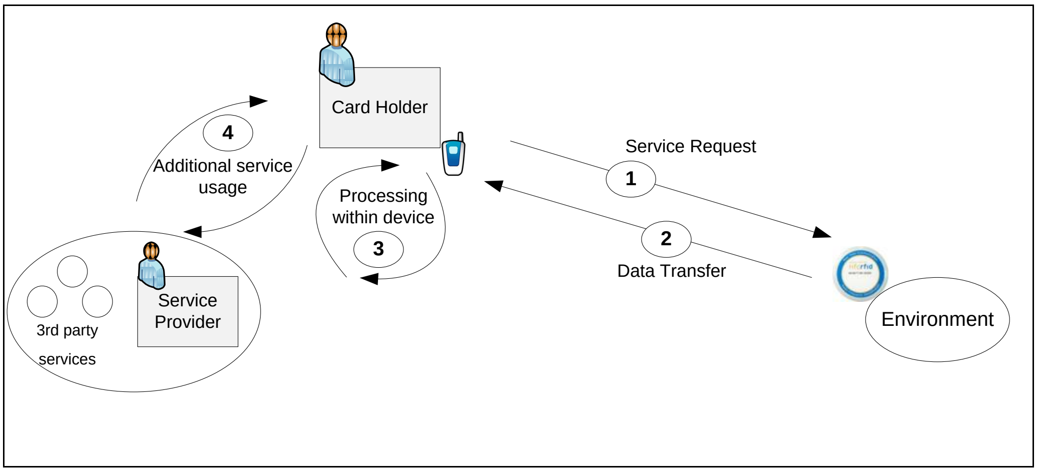

Figure 10. Service Usage Model of Reader/Writer Mode

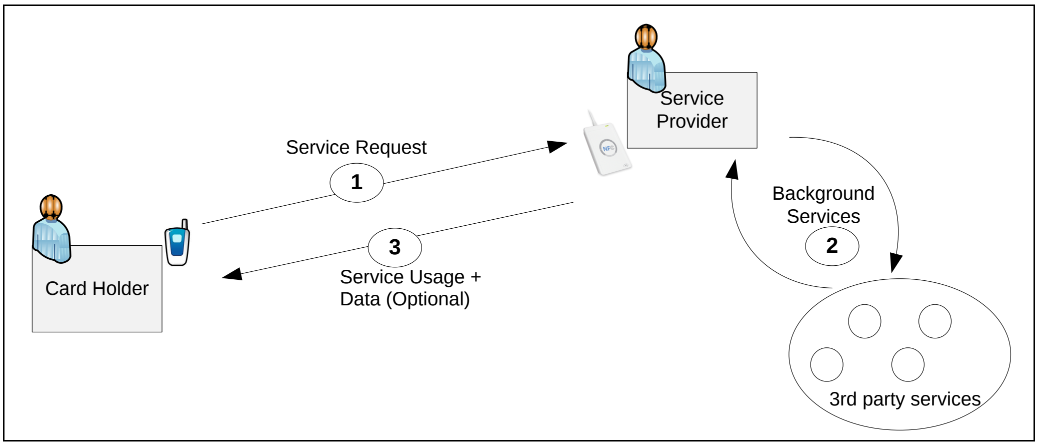

Figure 11. Service Usage Model of Card Emulation Mode

4.5.3 Peer-to-Peer Mode

In this mode two users can communicate with each other using their mobile phones. SPs are not involved in this mode; however they can be active if the shared object is used for further operations within mobile phone. In Figure 12, the service usage model of this mode is given.

1. **Data Request/Transfer:** Master and slave devices request/transfer data from/to each other.
2. **Additional Service Usage (optional):** When data is shared between mobile phones, these data can be used for additional purposes over Internet such as saving received business card to a database over Internet after a successful share.

In this part of the section, we described the frameworks for each NFC mode for service usage phase, because the interaction required in each NFC mode requires different services to be defined for each mode. In the next part, we test these frameworks with use case scenarios. Also we emphasize that our proposed ecosystem model is a generic model and the service differentiation in each mode does not affect our proposed model.

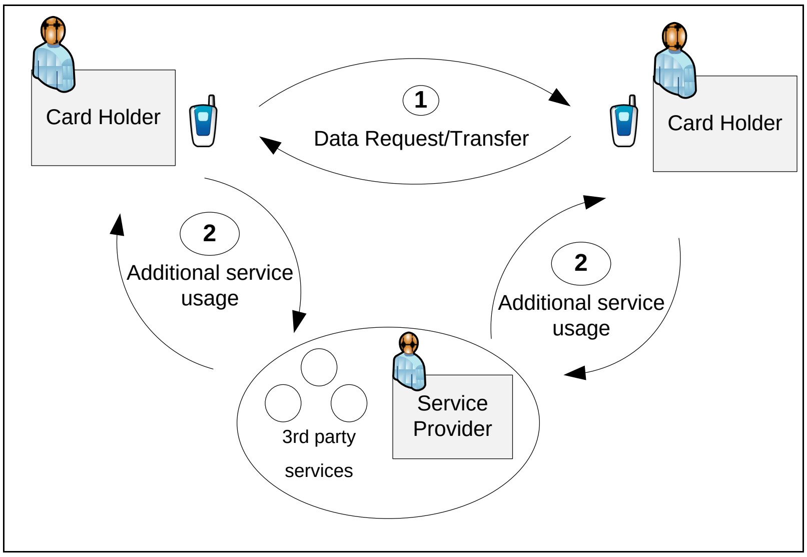

Figure 12. Service Usage Model of Peer-to-Peer Mode

5 Use Cases

In the previous section we have described the proposed ecosystem architecture and service usage phases for each operating mode. Now, we want to test the viability of our proposed model together with its service usage phases in the light of two use cases. These cases are meant to address NFC operating modes. The first use case is the combination of NFC ticketing [7, 23] and NFC payment [20, 28] applications which also includes the secure communication of two different applications in smart card. Two different NFC operating modes (Reader/Writer mode and Card-emulation mode) are used in the application. The second use case is a social networking application which is described in [12, 33]. This application also uses two different NFC operating modes (Reader/Writer mode & Peer-to-Peer mode). Hence, all of three NFC operating modes will be satisfied when both use cases are applied.

5.1 NFC Ticketing Use Case

Most important applications of NFC are e-ticketing and payment applications which are also emphasized many times in NFC's official website [24]. In [23], a complete e-ticketing application is developed and tested, and compared with other e-ticketing solutions. According to this application, user buys her ticket from event's web site using her computer and easily passes through turnstiles without waiting in the line. If she has an NFC-reader connected to her computer, she transfers her e-ticket to her mobile phone by touching them using card-emulation mode. Otherwise she transfers her e-ticket at "SYNC points" at event site. After she transfers the tickets to mobile phone, she can pass through entrance terminal by waving her mobile phone [23]. Actually this e-ticketing application is lack of payment method which can only be done through a computer via event's web site. There is not any other payment method presented in the paper that the fee can be paid with the same mobile device, without the need of a computer.

On the other side, an e-ticket application is presented in [7], where the ticket is bought via smart poster environment using reader/writer mode. In this application when user touches her mobile phone to NFC tag, an automated SMS is sent to SP provider and e-ticket is transferred to mobile phone. However in [20, 28] payment with NFC enabled phones are presented and discussed along with other payment technologies. The technological improvements on NFC technology such as intercommunication of applications and host application's capability to manage multiple NFC applications enabled using two NFC applications together with possibility of exchanging data between applications. In our use case, we test a scenario that both uses payment and ticketing applications. Firstly payment application pays a ticket fee. Then ticketing application provides obtaining the e-ticket to mobile phone. Ticketing application communicates with payment application and gets payment confirmation.

Our Scenario: User wants to buy her e-ticket for a movie by touching an NFC tag, attached to a poster advertisement and easily pass through turnstiles without waiting in the line. As she touches to the tag on the smart poster, the data that resides in the tag is transferred to mobile phone. Ticketing application runs on the mobile phone automatically with the push registry data, and event-id data is also transferred to the phone. Mobile phone displays movie's information using event-id. If user wants to buy the ticket after reservation, she can do this by using one available payment service that is previously installed to the SE at the mobile. Upon payment of the ticket fee, user is forwarded to ticketing application and it receives e-ticket from ticketing SP and stores in mobile phone. At event site, user can pass through entrance terminal by touching her mobile phone. When ticket is confirmed, turnstile is opened. In this scenario, user is able to pay and buy with her mobile phone with eliminating the need for an additional method for payment.

Used Operating Modes: Reader/Writer mode & Card-emulation mode. Reader/Writer mode is used prior to payment to get event data from NFC tag. Card emulation mode is used at the entrance terminal to use stored e-ticket.

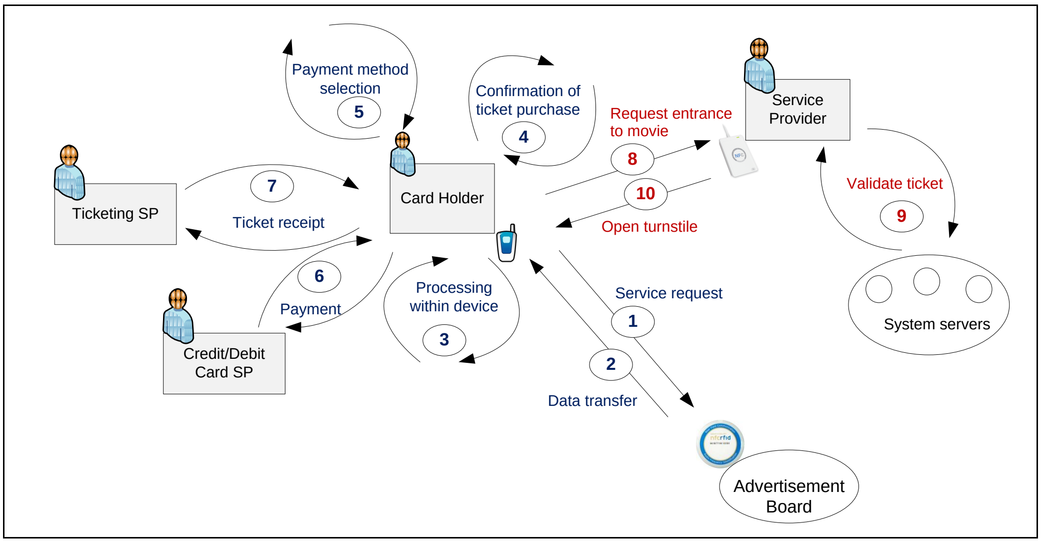

Figure 13. Service Usage Model of NFC Ticketing Use Case

Following steps are performed in NFC ticketing which consist of the service usage model of the first use case.

1. **Service request:** User touches her mobile phone to the tag that is on the smart poster.
2. **Data transfer:** Data is transferred from NFC tag to the mobile phone which includes push registry and event id data.
3. **Processing within device:** If ticketing application is available on user's mobile phone, the ticketing application automatically runs with the transferred push registry data. If not available, the host application on the SE immediately asks user to request the ticketing application from TSM's application pool. If user confirms, TSM asks user to sign the application's business agreement. Also

these steps are described in section 4.4. After the downloading the ticketing application, installation and personalization of the application are performed by TSM. When ticketing application is ready to use, event information is displayed on mobile phone based on the event id.

4. **Confirmation of ticket purchase:** When event data is displayed to user, she is able to select purchase ticket option from the ticketing application.
5. **Payment method selection:** When user requests to purchase ticket, host application checks if there is any available installed payment application (credit card or debit card). If not, the host application first installs the payment application as described in section 4.4. If there is any available payment application, these are displayed to user and requested to select one. Alternatively user can download another payment application from TSM’s application pool.
6. **Payment:** When payment method is selected, mobile phone connects to the payment application’s SP and pays via OTA. When payment is confirmed, host application leads user to ticketing application.
7. **Receiving ticket:** Ticketing application receives the confirmation of payment, and requests ticket from ticketing SP. SP prepares her ticket at its backend servers and sends to user’s mobile phone via OTA.
8. **Request entrance to movie:** User touches her mobile phone to NFC reader at entrance terminal to open turnstile by using her ticket.
9. **Validate ticket:** User ticket data is transferred to SP by its NFC reader and SP validates user’s e-ticket from its backend servers.
10. **Open turnstile:** SP opens turnstile upon validating the ticket.

In the use case described above, both reader/writer mode and card emulation mode are used. Reader/Writer mode is used while requesting and receiving data from NFC environment, namely smart poster. On the other hand, card emulation mode is used while using e-ticket at entrance terminal. In able to use described service, all required entities are needed to complete the steps through 1 to 12 in section 4.4. If user did not install the required application, she needs to install at 3rd step as described.

Steps through 1-7 are service usage of reader/writer mode. Steps from 3 to 5 form “processing within device step” in the same model. In these steps mobile phone processes required actions and passes to next phase with user’s actions. Steps 6 and 7 are “additional service usage step” described in the generic model of reader writer mode. As described in the model, user connects to a SP via Internet, and uses its services via OTA communication. It has been proved that the generic model of the service usage of reader/writer mode completely fits with the use case.

Steps from 8 to 10 consists card emulation mode service usage. Step 8 refers to “service request step”, step 9 refers to “background services step”, and finally step 10 refers to “service usage step” in the generic card emulation mode service usage model. In “service request step”, user requests to enter event in the use case. After validation of ticket, in “service usage step”, SP opens turnstile which results in entering the event. It is seen that the service usage of both reader/writer and card emulation mode fits with the described generic service usage model of those modes.

If we try to test pre-installation and installation phases, steps from 1 through 3 in pre-installation phase are required for a company to be a recognized SP. If SP is already giving an NFC service, it means that SP has already completed these steps. On the other hand step 4 is needed for SP to deploy its application to users such as a ticketing or payment application. SP should have been completed these steps, otherwise users will not be able to use SP's NFC services. If a SP is already providing NFC service, the only need to deploy a new application to users is to process 4th step in pre-installation phase.

User is also required to process 5th and 6th steps in pre-installation phase in order to use her smart card for application installation and service usage. If any other application is installed before ticketing application, it means that user has already completed these steps. Lastly, for a new application installation, user needs to perform 7th and 9th steps. 8th step is performed one-time by TSM at the very first installation of an application to user's SE. If there is already an installed application in user's SE, it means that this step is already completed too. Finally TSM performs steps from 10 to 12 at application installation. Pre-installation and installation phases do not differ in any operating mode since these phases are independent from applications.

5.2 Hot in the City Use Case

Scenario: "Hot in the City (HIC)" is a mobile social network application which is described in [12, 33]. First feature of this application is that; users are able to make new friendship connections by touching their mobile phones each other. It is also extended to use Facebook platform, however it is not dependent. When two phones touched each other, master device informs the back-end system that the users have created a friend connection. Another feature of the application is users are able to update their status information on the Facebook with the location data. When user touches an NFC tag within the environment (hot spot tag), phone reads data from the tag and sends it to the backend system using HIC. User's location is updated this way, and friends are able to see her location information.

Used Operating Modes: Reader/Writer mode & Peer-to-Peer mode. Peer-to-Peer mode is used while creating new friend connections. Reader/Writer mode is used while reading location data from NFC tags.

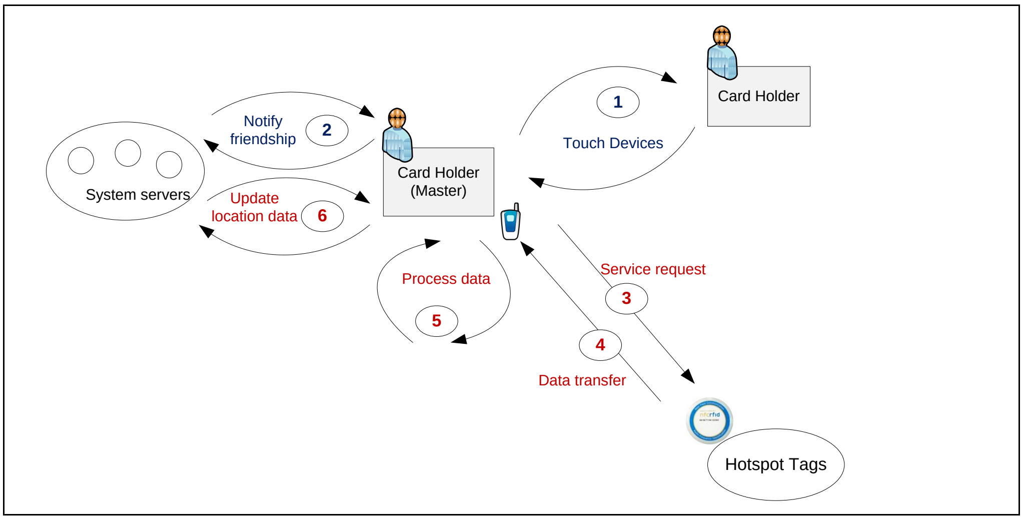

Figure 14. Service Usage Model of Hot in the City Use Case

Following steps are performed in Figure 14 which shows the service usage model of second use case.

1. **Touch Devices:** Users touch two mobile phones each other to start a friend connection and phones send required data to each other.
2. **Notify Friendship:** Master user's mobile phone sends confirmation and notification about connected friendship.

3. **Service request:** User touches her mobile phone to a hot spot tag.
4. **Data transfer:** Location data that resides in the tag is transferred to the user's mobile phone.
5. **Process data:** Data is processed to be sent to backend server.
6. **Update location data:** User's new location data is sent to the system servers and updated. Other users can now see user's new location data using their Hot in the City application.

In the HIC use case both, Peer-to-Peer and Reader/Writer modes are used. Peer-to-Peer mode is used at making friends which are steps 1 and 2. Step 1 ("Touch Devices") is "data request/transfer" step in the generic service usage model of Peer-to-Peer mode. Also "notify friendship" step is additional step described in the same model. It is seen that the Peer-to-Peer service usage of HIC fits with the created generic service usage model.

Reader/writer mode is tested in the first use case; however we tested this mode's service usage in this use case too. Reader/writer mode is used at updating location information at steps through 3 to 6. All steps in this use case fits again with the generic model of this mode. Optional service usage is used in both use cases (6th step in HIC case) however sometimes it is not required. Since pre-installation and installation phases are not dependent to any application, we do not see a need to describe those again.

6 Discussion

We have clearly indicated the requirements of a successful ecosystem, proposed a complete ecosystem model and applied it in use cases so far. We shall briefly highlight important advantages of the proposed model.

First of all, offering an application pool under TSM's roof is firstly proposed in this study and brings so many benefits to both users and SPs. From users' point of view, they will search new service applications easily via TSM's host application's interface. This will eliminate looking for SP websites. They will also easily update application without so much effort, again via host application. Another advantage is eliminating spam-like applications. Since TSM will check the security requirements and convenience of applications hosted in application pool, users will not deal with fake applications. From SPs' point of view, they will not need any investment to provide application housing and installation infrastructure, since TSM will handle this subject. It will minimize the cost that SPs will suffer especially for local or small firms.

Secondly, in the proposed model, TSM is the neutral actor that handles OTA communication. So, TSM makes the required investment for OTA infrastructure. Instead setting up multiple OTA management platforms by many SPs or/and many MNOs, a common OTA platform under TSM's roof seems an ideal solution. On the other hand, management of SE without an OTA platform is impractical; multiple applications cannot be managed and can only be a temporary solution for a period of time for an SP.

Thirdly, our proposed model's foundation is based on the GlobalPlatform's smart card specifications, OTA deployment models and messaging specifications. We highlight the GlobalPlatform specifications in this paper because they provide highly interoperable, feasible and applicable solutions for NFC services over the world. The proposed model in this paper is based on GlobalPlatform's full authorized deployment model where full delegation is given to TSM, as well as on the essentials of messaging specification. We provide a complete TSM centric NFC service deployment model where none of the actors are dependent to an actor, and all actors benefit from the trustworthiness role of the TSM.

Thus, this proposed model can be also applied to all SE options; embedded hardware, SMC and UICC. The major novelty of this study as the application pool infrastructure under TSM's roof provides more secure and efficient life-cycle management of NFC applications and SEs when compared with existing TSM centric models.

However there is not any existing opportunity to validate our proposed model in a real environment because:

- Real environment should be set up which can only be performed by CIs including MNOs and other issuers, SPs and OTA providers,
- Entities are not yet well prepared for an NFC ecosystem model. This is conditional to some factors such as spread of NFC enabled mobile phones among users and dealing with usability problems,
- A neutral entity for handling TSM functions needs to be formed if not exists, otherwise it should be agreed among other actors.

The limitations of validating the proposed model are important and make it nearly impossible to test the model. However we have tried to test the model by applying use cases. We think that the validation of this study is sufficient under current limitations.

6.1 Requirements Discussion

We have already defined and indicated nine requirements of an NFC ecosystem in previous sections. In this section, we discuss those requirements.

1. **Competitive environment between SPs:** Each company wishing to play SP role can get role of a SP only and exclusively, and is forbidden to play another role in the ecosystem such as CI, or TSM etc. This is required to provide fair competitive media. Since corporate companies cannot play any other role besides the given boundaries, the competitive environment between all SPs will be satisfied.
2. **A neutral entity to manage and secure the ecosystem:** The ecosystem is set up based on a trusted and neutral role; TSM. TSM handles administrative functions of the ecosystem. Since it is a neutral entity and all other entities should agree on it, the conflicts between entities should be minimized and a trusted environment should be set up. An NFC environment with one and only TSM removes the compatibility issues to deal with which arises with multiple TSMs. User only need to search for applications in one place. All entities should only make agreements with one TSM. It is important to select one TSM which will be respected by all players in the ecosystem, which is obvious.
3. **A neutral entity to support SPs and users:** SPs and users may need technological support in the ecosystem. In the proposed ecosystem, SPs do not need to manage the operations on the SE. TSM will manage those installing, locking, unlocking and deleting functions; SP will get the required keys only after application installation; and SP will be able to access the application's secure domain using that key. TSM is also able to give technological support to SPs when they need it. On the other hand, users will be able to get support from TSM, so that users' trust will be satisfied. In case of losing the mobile phone, users will be able to get support from TSM and TSM will delete all the applications and related data in the SE.
4. **Each SP to manage its own application in SEs:** Managing an application on the SE is a critical issue for SPs. They need to be able to control the application, where all applications shares the same SE. Thanks to GlobalPlatform Card Specifications which provides an entity to delegate card content management

functions to another entity [18]. In the proposed ecosystem, TTP transfers application's secure domain's specific keys to particular SP. Thus each SP will be able to manage the same card content in same SE, with the condition that each one can link to only its own applications.

5. **Compatibility with major SEs:** As it has been described earlier, there are many SE alternatives such as Baseband processor, Embedded Hardware, SMC, and UICC. A user can select either one. Proposed ecosystem is compatible with the SEs, with the condition that it should be produced along with GlobalPlatform Card Specifications, since card content management functions in the ecosystem are proposed according to those specifications. Any SE that does not fulfill GlobalPlatform Card Specifications cannot be managed of course. We think that this is not a restrictive issue, because most of the SEs are already developed obeying these specifications [8].
6. **Business agreements:** Business agreement set in the proposed ecosystem includes Business Agreement, Service Agreement, and User Agreement. The first two agreements are required to be signed between TSM and SP whereas the last agreement is need to be signed between TSM and card holder. When an agreement is signed, it proves that related entities agree on the agreements, and a misuse will be penalized. The first agreement shows that a SP can provide an NFC service, the second agreement shows that SP can deploy its application to SEs and can give service for particular application, and the third agreement shows that user agrees to get service for particular application. We think that business agreements are very important parts of the ecosystem in order to increase trust.

6.3 Role Model of Proposed NFC Service Ecosystem

It is already described in section 3 that the proposed ecosystem is based on role-based service ecosystem modeling. The roles, activities of each role, and communication structure are modeled in service level. A business entity can play one or many roles and it can even change according to evolving business models over time. Table I summarizes roles, their overall high-level activities and current potential players in NFC ecosystem.

Table I. Role Model of Proposed NFC Service Ecosystem

Role	High-level Activity	Potential Player (Business Entity)
Trusted Service Manager	• Managing trust in ecosystem • Managing the life-cycle of the NFC applications • Providing necessary technology support • Application pool • Managing agreements	• An independent business entity that all other entities agree on it • Government supporting party
Card Holder	• Owning secure element • Installing NFC applications • Initiating NFC service	• Mobile device owners
Service Provider	• Offering value added service(s)	• Any company that wishes to offer NFC service to its customers (Banks, Transportation companies, etc.)

Card Issuer	• Issuing secure elements • Transferring master key to Trusted Service Manager	• MNOs • Smart card manufacturers
Certification Authority	• Issuing digital certificates	• Any recognized Certificate Authority
OTA Provider	• Providing OTA communication	• MNOs • Trusted Service Manager • Another business entity that have OTA infrastructure

7 Conclusion

NFC is a short distance, high frequency and low bandwidth wireless communication technology that integrates RFID and smart technology with mobile devices. There is a clear need for a secure and interoperable NFC ecosystem model which describes roles, the communication structure between roles and uses multiple NFC applications or services in mobile phones in a secure and compatible way. However a complete NFC ecosystem study referring to its communication essentials has not been performed. To fulfill this need, we presented a complete role-based service level NFC ecosystem design.

In the paper, firstly the requirements of an NFC ecosystem are discovered and given. Then roles involved in the proposed ecosystem are identified. Activities of each role are detailed and communication structure between roles is described. Moreover we analyzed NFC ecosystem in three phases as pre-installation, installation, and service usage phases. We further investigated service usage phase for three different operating modes of NFC. We applied two use cases to test the model. Finally we discussed the requirement satisfaction at the end of the paper.

We assume that this paper will provide a good reference point for academicians and industry that are actively involved in NFC technology. We see that the only limitation of the study is the inability to validate the model under current circumstances, since an actual environment is required.

As a further research direction, a comprehensive study for evaluating the security requirements of the proposed ecosystem is needed. This security evaluation should include both securing the communication between actors and securing the applications in SE. We also foresee building on our findings to study the intercommunication of multiple applications in a secure database management system located in SE, and also to promote loyalty management application with this model. Furthermore, we foresee that the security of the intercommunication of multiple applications is a demanding area.

References

[1] Assa Abloy AB (2008). 'Best NFC Service of 2008' Awarded to VingCard. Resource document. VingCard Elsafe Assa Abloy. http://www.vingcard.com/binary?id=66705, Accessed 10 Aug 2011.

[2] Benyo, B. (2009). Business Process Analysis of NFC-based Services. Proceedings of the IEEE 7th International Conference on Computational Cybernetics, Palma de Mallorca, Spain, 26-29 Nov 2009, pp. 75-79.

[3] Benyo, B., Vilmos, A., Fordos, G., Sodor, B. & Kovacs, L. (2009). The StoLPan View of the NFC Ecosystem. Proceedings of the Conference on Wireless Telecommunications Symposium, Prague, Czech Republic, 22-24 Apr 2009, pp. 1-5.

[4] Benyo, B., Vilmos, A., Kovacs, K. & Kutor, L. (2007). NFC Applications and Business Model of the Ecosystem. Proceedings of the 16th IST Mobile and Wireless Communications Summit, Budapest, Hungary, 1-5 July 2007, pp. 1-5.

[5] FELICA, http://www.sony.net/Products/felica/, Accessed 10 Aug 2011.

[6] Finkenzeller, K. (2010). RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication. John Wiley and Sons.

[7] Ghiron, S. L., Sposato, S., Medaglia, C. M. & Moroni, A. (2009). NFC Ticketing: a Prototype and Usability test of an NFC-based Virtual Ticketing application. Proceedings of the 1st International Workshop on Near Field Communication, Hagenberg, Austria, 24-26 Feb 2009, pp. 45-50.

[8] GlobalPlatform. Available online: http://www.globalplatform.org/, Accessed 10 Aug 2011.

[9] GlobalPlatform (2006). GlobalPlatform Card Specification Version 2.2. GlobalPlatform. http://www.globalplatform.org/specificationscard.asp, Accessed 10 Aug 2011.

[10] GlobalPlatform. (2009). GlobalPlatform's Proposition for NFC Mobile: Secure Element Management and Messaging. http://www.globalplatform.org/documents/GlobalPlatform_NFC_Mobile_White_Paper.pdf, Accessed 10 Aug 2011.

[11] GlobalPlatform. (2011). GlobalPlatform System Messaging Specification for Management of Mobile-NFC Services v1.0. http://www.globalplatform.org/specificationssystems.asp, Accessed 10 Aug 2011.

[12] Haikio, J., Tuikka, T., Siira, E. & Tormanen, V. (2010) 'Would You Be My Friend?' - Creating a Mobile Friend Network with 'Hot in the City'. Proceedings of the 43rd Hawaii International Conference on System Sciences, Hawaii, USA, 5-8 Jan 2010, pp. 1-10.

[13]Haselsteiner, S. & Breitfuß, K. (2006). Security in Near Field Communication (NFC). Philips Semiconductors, Proceedings of Workshop on RFID Security 2006, Graz, Austria, 12-14 Jul 2006, pp. 3-13.

[14] iCarte, Resource document. iCarte. http://www.icarte.ca/, Accessed 10 Aug 2011.

[15] Leng, X. (2009). Smart Card Applications and Security. Information Security Technical Report, 14 (2), 36-45.

[16] Madlmayr, G., Langer, J., Kantner, C., Scharinger, J. & Schaumüller-Bichl, I. (2009). Risk Analysis of Over-the-Air Transactions in an NFC Ecosystem. Proceedings of the 1st International Workshop on Near Field Communication, Hagenberg, Austria, 24-26 Feb 2009, pp. 87-92.

[17] Madlmayr, G., Langer, J. & Scharinger, J. (2008). Managing an NFC Ecosystem. Proceedings of the 7th International Conference on Mobile Business, Barcelona, Spain, 7-8 July 2008, pp. 95-101.

[18] Markantonakis, K. & Mayes, K. (2003). An Overview of the GlobalPlatform Smart Card Specification. Information Security Technical Report 8(1), 17-29.

[19] Markantonakis, K. & Mayes, K. (2004). A Secure Channel Protocol for Multi-Application Smart Cards Based On Public Key Cryptography. 8th IFIP TC-6 TC-11 Conference on Communications and Multimedia Security, Windermere, The Lake District, United Kingdom, 15-18 Sep 2004, pp. 79-95.

[20] Massoth, M. & Bingel, T. (2009). Performance of different mobile payment service concepts compared with a NFC-based Solution. Proceedings of the 4th International Conference on Internet and Web Applications and Services, Venice, Italy, 24-28 May 2009, pp. 205-210.

[21] Mobey Forum. (2008). Best Practice for Mobile Financial Services Enrolment Business Model Analysis. Resource document. Mobey Forum. http://www.mobeyforum.org/content/download/460/2768/file/Best%20Practices%20for%20MFS%20Enrolment%20Business%20model%20analysis%20final.pdf, Accessed 10 Aug 2011.

[22] Mobey Forum. (2006). Mobile Financial Services Business Ecosystem Scenarios & Consequences. Resource document. Mobey Forum. http://www.mobeyforum.org/content/download/343/2164/file/Mobey%20Forum%20MFS%20Business%20Ecosystem%20Summary.pdf, Accessed 10 Aug 2011.

[23] Neefs, J., Schrooyen, F., Doggen, J. & Renckens, K. (2010). Paper ticketing vs. Electronic Ticketing based on off-line system 'Tapango'. Proceedings of the 2nd International Workshop on Near Field Communication, Monaco, France, 20 Apr 2010, pp. 3-8.

[24] NFC Forum. http://www.nfc-forum.org, Accessed 10 Aug 2011.

[25] NFC Forum. (2008). Dynamic management of multi-application secure elements. Available online: http://www.nfc-forum.org/resources/white_papers/Stolpan_White_Paper_08.pdf, Accessed 10 Aug 2011.

[26] NFC Forum. (2008). Essentials for Successful NFC Mobile Ecosystems. Resource document. NFC Forum. http://www.nfc-forum.org/resources/white_papers/NFC_Forum_Mobile_NFC_Ecosystem_White_Paper.pdf. Accessed 10 Aug 2011.

[27] Ozdenizci, B., Coskun, V., Aydin, M. N. & Ok, K. (2010). NFC Loyal: A Beneficial Model to Promote Loyalty on Smart Cards of Mobile Devices. Proceedings of the 2010 International Conference for Internet Technology and Secured Transactions (ICITST-2010), London, UK, 8-11 Nov 2010, pp. 134-139.

[28] Pasquet, M., Reynaud, J. & Rosenberger, C. (2008). Secure Payment with NFC Mobile Phone in the Smart Touch Project. Proceedings of the International Symposium on Collaborative Technologies and Systems, California, USA, 19-23 May 2008, pp. 121-126.

[29] Reveilhac, M. & Pasquet, M. (2009). Promising Secure Element Alternatives for NFC Technology. Proceedings of the 1st International Workshop on Near Field Communication, Hagenberg, Austria, 24-26 Feb 2009, pp. 75-80.

[30] Sauveron, D. (2009) Multi-application Smart Card: Towards an Open Smart Card?. Information Security Technical Report 14(2), 70-78.

[31] Schoo, P. & Paolucci, M. (2009). Do you talk to each poster? Security and Privacy for Interactions with Web Service by means of Contact Free Tag Readings. Proceedings of the 1st International Workshop on Near Field Communication, Hagenberg, Austria, 24-26 Feb 2009, pp. 81-86.

[32] SDID, http://www.sdid.com, Accessed 10 Aug 2011.

[33] Siira, E. & Tormanen, V. (2010). The impact of NFC on multimodal social media application. Proceedings of the 2nd International Workshop on Near Field Communication, Monaco, France, 20 April 2010, pp. 51-56.

[34] Smart Trust. (2009). The role of SIM OTA and the Mobile Operator in the NFC Environment. White Paper. http://www.paymentscardsandmobile.com/research/reports/SIM-OTA-Mobile-Operator-role-NFC.pdf, Accessed 10 Aug 2011.

[35] StoLPaN. http://www.stolpan.com/, Accessed 10 Aug 2011.

[36] StoLPaN. (2011). Description of the Life-cycle management of NFC Applications. Resource document. StoLPaN. http://www.nfc-forum.org/resources/white_papers/Stolpan_White_Paper_08.pdf, Accessed 10 Aug 2011.

[37] Tian, C. H., Ray, B. K., Lee, J., Cao, R. & Ding, W. (2008). BEAM: A framework for business ecosystem analysis and modeling. IBM Systems Journal 47(1), 101-114.

[38] Avispa Project, http://www.avispa-project.org/, Accessed 10 Aug 2011.