A Novel Scheme for On-demand Distribution of Secure Element Keys

Vincent Alimi
Normandie Univ, France
UNICAEN, ENSICAEN, GREYC
CNRS, UMR 6072
F-14032 Caen, France
fvincent.alimi@ensicaen.fr

ABSTRACT: *The Trusted Service Manager is a key actor in the Near Field Communication technology ecosystem. It is responsible for the management of secure elements and/or applications life cycle on behalf of Issuers, Mobile Network Operators and Service Providers. The Issuer is the actor owning the keys of the secure element present in an NFC-enabled equipment. Some of them such as personal computer, laptop, or tablet manufacturers can see the key management process as a barrier to the integration of the NFC technology.*

We propose a novel scheme for on-demand distribution of secure element keys. This scheme allows to subcontract the business and technical key management processes to a trusted third party that will distribute on-demand the keys to accredited TSMs.

Keywords: Near Field Communication, Trusted Service Manager, On-demand Key Distribution, Global Platform

Received: 2 June 2013, Revised 8 July 2013, Accepted 13 July 2013

1. Introduction

In order to deploy a mobile contactless service, the Trusted Service Manager (TSM) in charge of this operation must have the keys of the security domain in which the application will be downloaded and installed. In most cases, these keys are provided to the TSM by the Issuer (the entity issuing the equipment containing the Secure Element) according to pre-defined business and/or technical agreements. But in some cases, the Issuer does not wish or cannot ensure the key management or the Issuer does not wish to multiply agreements and key exchange operations with different TSMs.

In this paper, we propose a key distribution scheme that issues on-demand the secure element keys to accredited TSMs. This paper is oranized as follows. Section II gives some background to the reader on the NFC technology and its ecosytem. Section III exposes the problem solved by our proposition. Sections IV and V describe the new scheme for the on-demand distribution of secure element keys. Section VI explains our action in standardization bodies to see the adoption of our proposition. Finally, section VII presents our conclusions.

2. Background

2.1 Near Field Communication

The Near Field Communication technology (NFC), is based on RFID (Radio Frequency IDentification) that, embedded in a mobile device – such as a smart phone, a tablet . . . – allows to work in three modes [7]. (cf. Figure 1). The device can act either as a reader or alter contactless cards and tags, exchange data with another NFC-enabled device through a peer-to-peer communication, or emulate a contactless card.

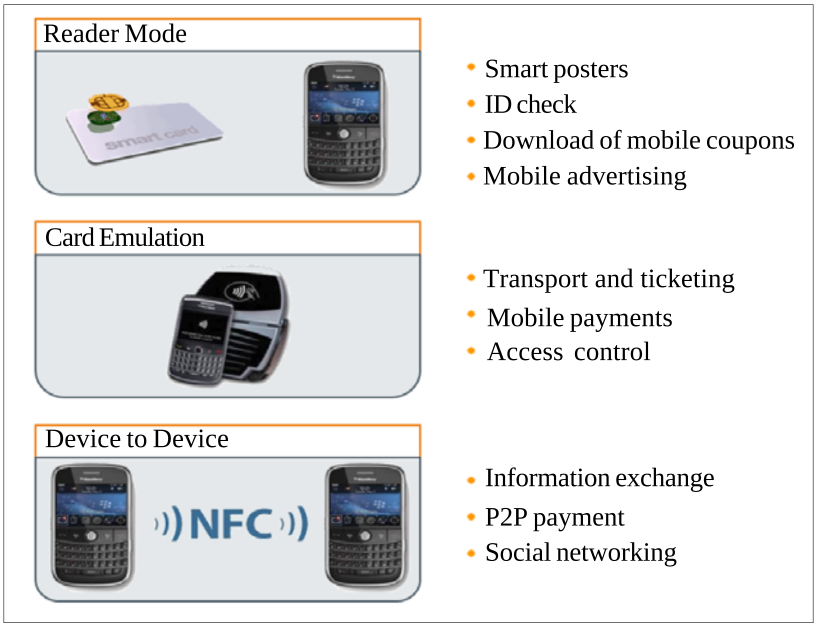

Figure 1. NFC modes

An NFC-enabled mobile device is composed of the three following logical components [2], [8] : the mobile device processor (commonly named Baseband Processor), an NFC Controller and a Secure Element. The baseband processor hosts the device system application (e.g.: applications managing the GSM telecommunication protocol) and third-party applications installed by the user. The NFC controller is responsible for the analog/digital conversion of the signals and for routing the communications to the Secure Element and to the baseband processor. The Secure Element allows the card emulation mode so that a reader or terminal (such as a Point of Sale) does not distinguish a contactless card from a secure element. Figure 2 illustrates the integration of the NFC technology into a mobile device.

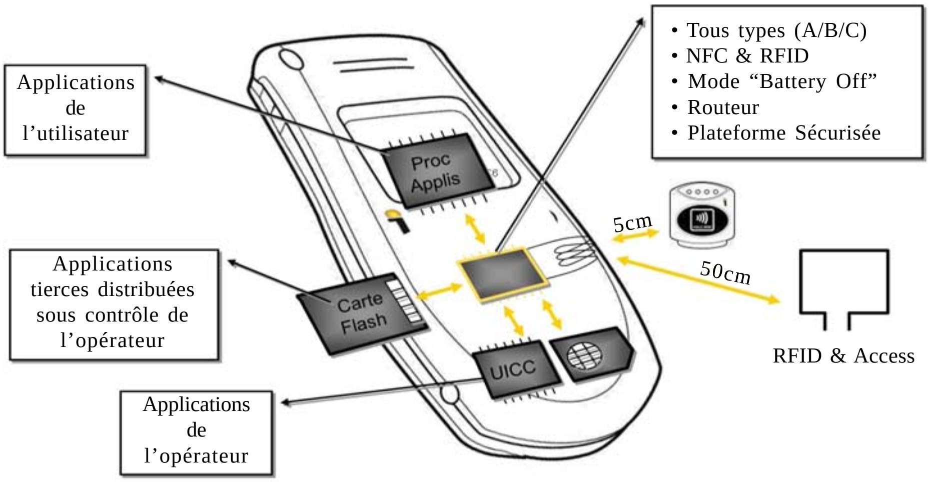

Figure 2. Functional architecture of the NFC technology

2.2 Trusted Service Manager

As illustrated in Figure 3, the NFC ecosystem comprises many stakeholders. One of them, the Trusted Service Manager (TSM)

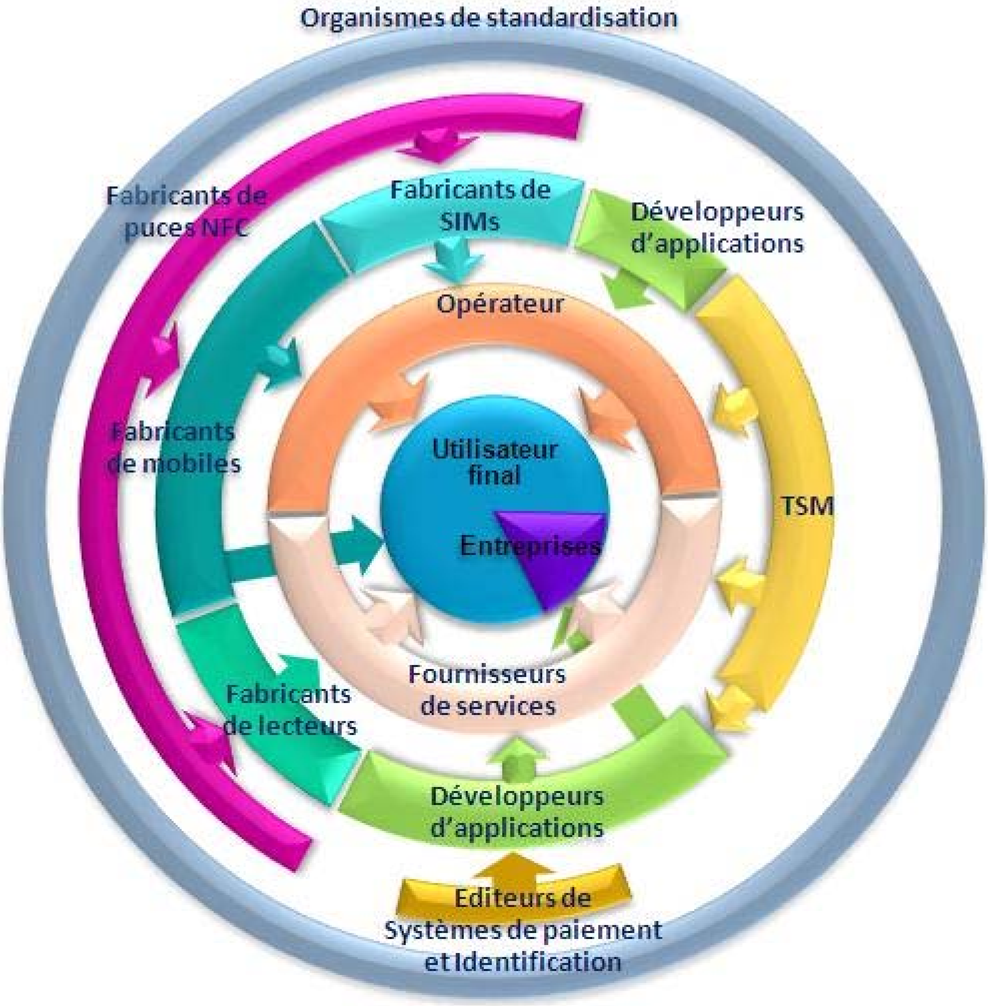

Figure 3. NFC ecosytem

has an important role. It is responsible for securely managing secure elements life cycle, install and personalize applications on behalf of Mobile Network Operators (MNOs), Original Equipment Manufacturers (OEMs) and Service Providers. As such, the TSM needs to own the set of cryptographic keys that protect the secure element, more precisely a logical part of the secure element called Security Domain.

3. Problem Statement

Let us detail the different steps required for the deployment of a mobile service from the subscription to the installation of the application on the secure element by a TSM.

1) The end-user subscribes to a mobile service.

2) The service provider entrusts the deployment of the mobile service to the TSM.

At this stage, in most of the cases, the TSM queries the secure element capabilities to its Issuer. Now, let us make the following assumptions:

- Regardless the secure element management mode, it is assumed that the TSM has the associated privilege.

- For business and/or technical reasons, the secure element issuer subcontracts the keys management to a trusted third party.

Based on these assumptions, the next steps of the mobile service deployment are the following:

3) The TSM identifies the trusted third party owning the secure element keys.

4) The TSM queries the secure element keys to the trusted third party.

5) The trusted third party generates the secure element keys by derivating the master key with the secure element identification data provided by the TSM.

6) The generated keys are sent to the TSM.

7) The TSM can now open a secure communication channel with the secure element.

8) The TSM processes a key rotation, i.e. it pushes its own keyset into the secure element.

9) The TSM runs the mobile service deployment by sending a commands script through the previously open secure channel.

Yet, an issue is preventing this scenario from occurring. Indeed, the secure element contains only the data allowing to

identify the following actors:

- The chip and operating system manufacturers with the Card Production Life Cycle data,
- The secure element issuer with the Issuer Identification Number, IIN.

As the secure element does not contain (cf. GlobalPlatform Card specifications [4]) information allowing to identify the trusted third party, the TSM cannot proceed to step 3. We propose in this paper a methodology to identify this actor and allowing to distribute on-demand the secure element keys to the TSM.

4. Propositions for the Third-Party Identification

We have seen in the previous section that the GlobalPlatform specifications do not include any mechanism allowing to identify other entities than the manufacturers and the issuer. To circumvent this issue, we propose two solutions described in the next sections.

4.1 Solution #1: Extend the card recognition data

In this solution, we propose to extend the GlobalPlatform Card Recognition Data in order to store the identifier of the trusted third party. Card recognition data format is given in Figure 4. Since the card recognition data is limited to 127 bytes, this identifier must be short, i.e. a few bytes. Therefore, this assumes the existence of a central directory matching the short identifier and the URL of the trusted third party's web server.

4.2 Solution #2: add a tag to the Security Domain data

In this solution, we propose to add a tag, i.e. a data container, to the GlobalPlatform Security Domain data. This tag contains a URL pointing directly to the trusted third party's web server. The URL would be of the form http://service.mytsm.net/secureelementmanagement/v1/index.htm. Storing a URL is a better option than storing the IP address because it is more flexible. Indeed, the URL uses DNS services and thus makes transparent a possible change of the trusted third party network topology.

4.3 Comparative study

Table 1 summarizes the advantages and disadvantages of each solution. It appears in Table I that the best solution is to add a tag in the security domain data. It can store a complete URL and is a direct link to the trusted third party. The URL is accessible via a GET DATA command that does not require the establishment of a secure channel.

5. Proposed Architecture

5.1 Key server

The server implemented by the trusted third party exposes a Web Service that publishes methods available to TSMs.The connection and authentication between the TSM and the trusted third party are realized through the establishement of a VPN (*Virtual Private Network*) based on SSL (*Security Socket Layer*) or its successor TLS (*Transport Layer Security*) in the client authentication mode as described in [1]. The messages exchanged comply with XML (*eXtended Markup Language*) and SOAP

Tag	Explanation	Length	Value	Presence
‘66’	Tag for “Card Data”	variable - see note 1	Data objects identified in 7816-6, including tag ‘73’	Mandatory
‘73’	Tag for “Card Recognition Data”	variable	Data objects listed below	Mandatory
‘06’	Universal tag for “Object Identifier” (OID)	variable	(globalPlatform 1) OID for Card Recognition Data, also identifies Global Platform as the Tag Allocation Authority	Mandatory
‘60’ ‘06’	Application tag 0 ‘OID’ tag	variable variable	(globalPlatform 2) OID for Card Management Tyoe and Version-see note 2	Mandatory
‘63’ ‘06’	Application tag 3 ‘OID’ tag	variable variable	(globalPlatform 3) OID for Card Identification Scheme-see note 3	Mandatory
‘64’ ‘06’	Application tag 4 ‘OID’ tag	variable variable	(globalPlatform 4 scp i) OID for Secure Channel Protocol of the Issuer Security Domain and its implementation options- see note 4	Mandatory
‘65’	Application tag 5	variable	Card configuration details -see note 5	Optional
‘66’	Application tag 6	variable	Card / chip details - see note 6	Optional
‘67’	Application tag 7	variable	Issuer Security Domain’s Trust Point certificate information - see note 7	Optional
‘68’	Application tag 8	variable	Issuer Security Domain certificate information - see note 8	Conditional

Figure 4. GlobalPlatform Card Recognition Data format (Source : GlobalPlatform)

(Simple Object Access Protocol).

5.2 Secure Element Proxy

In [5], GlobalPlatform defines a mechanism for remote administration of a Secure Element using the HTTP (**Hypertext Transfer Protocol**) protocol. In particular, this specification describes an application called Administration Agent or Proxy and whose role is to unwrap APDU (**Application Protocol Data Unit**) commands received from the server in an HTTP envelope and route them to the Secure Element.

5.3 Distribution flow

The flow of the proposed on-demand distribution of secure element keys is illustrated in 5. The different steps are detailed hereafter.

Step 0 : The TSM and the trusted third party must exchange a transport key *KEK* (*Key Exchange Key*).

Step 1 : The TSM triggers a remote administration session. The Proxy application opens a TLS connection with the TSM as defined in [5].

Step 2 : The TSM requests the Proxy application to provide him with the following secure element related data:

- URL of the trusted third party,
- Secure element identification data (KEYDATA, tag ‘*CF*’),
- Information about the secure channel keyset (tag ‘*E*0’),
- Counter of secure channel sessions (*Sequence Counter*, tag ‘*C*1’). This counter is maintained by the security domain. It is used in step 6 for the session keys computation.

Step 3: By using the URL, the TSM opens an SSL/TLS connection with the trusted third party.

Step 4: The TSM invokes the method `WSGetDifersifiedKeys` with the secure element related data and the *KEK* index as parameters.

Step 5: The trusted third party generates the secure element diversified keys (K_{ENC}, K_{MAC}, K_{DEK}) and returns them to the TSM.

Step 6: From the diversified keys and the sequence counter, the TSM generates the session keys and opens a secure channel with the secure element.

Step 7: The TSM generates the management scripts, encapsulates them in an HTTP envelope and sends them to the Proxy application. The Proxy de-encapsulates the APDU commands and route them to the secure element (out of scope).

In the next section, we explain our action within the standardization bodies EMVCo and GlobalPlatform to see this new key distribution scheme adopted by all actors of the NFC ecosystem.

	ADVANTAGES	**DISADVANTAGES**
Card Recognition Data	Short data storage Read with GET DATA command	Limited size Requires a directory
Tag	Direct pointer Size not limited Read with GET DATA command	–

Table 1. Comparison of the Proposed Solutions

6. Validation

We believe that this on-demand distribution scheme is a key element for the widespread adoption of NFC technology. Historically, the first devices in which the NFC has been integrated are mobile phones. For these devices, the ecosystem actors are used to the key management process as it is well established and standardized. But if we consider that any device can be equipped with NFC technology, then the manufacturers of equipment like laptops or tablets will have to integrate the key exchange with the TSMs in their manufacturing process. Our solution allows these manufacturers to subcontract the keys management to experts and the NFC ecosystem to be open to all kind of manufacturers.

To see our proposition adopted by the NFC ecosystem, we wanted it to be approved by the GlobalPlatform consortium.

The presentation of our scheme took place during a meeting of the *GlobalPlatform Mobile Task Force* [3]. The presentation was quite well received and it was agreed that a new tag containing the URL of a trusted third party will be integrated in the next version of the Amendment C specification [6].

Furthermore, the EMVCo consortium has the mission of defining and maintaining the specifications of the chip-based payment system EMV (Eurocard, Mastercard, Visa). EMVCo is currently defining a profile detailing the features supported and not supported by EMVCo for the certification of payment applets hosted by an embedded Secure Element. In this context, we think that EMVCo will require that the keys of the security domains hosting payment applications are exchanged between a certified TSM and the certified entity who has loaded them into the secure element. In other words, the issuer of NFC-enabled equipments embedding a secure element will no longer be a link in the key management chain. Therefore, our proposition linking a TSM and a trusted third party received a positive echo from EMVCo.

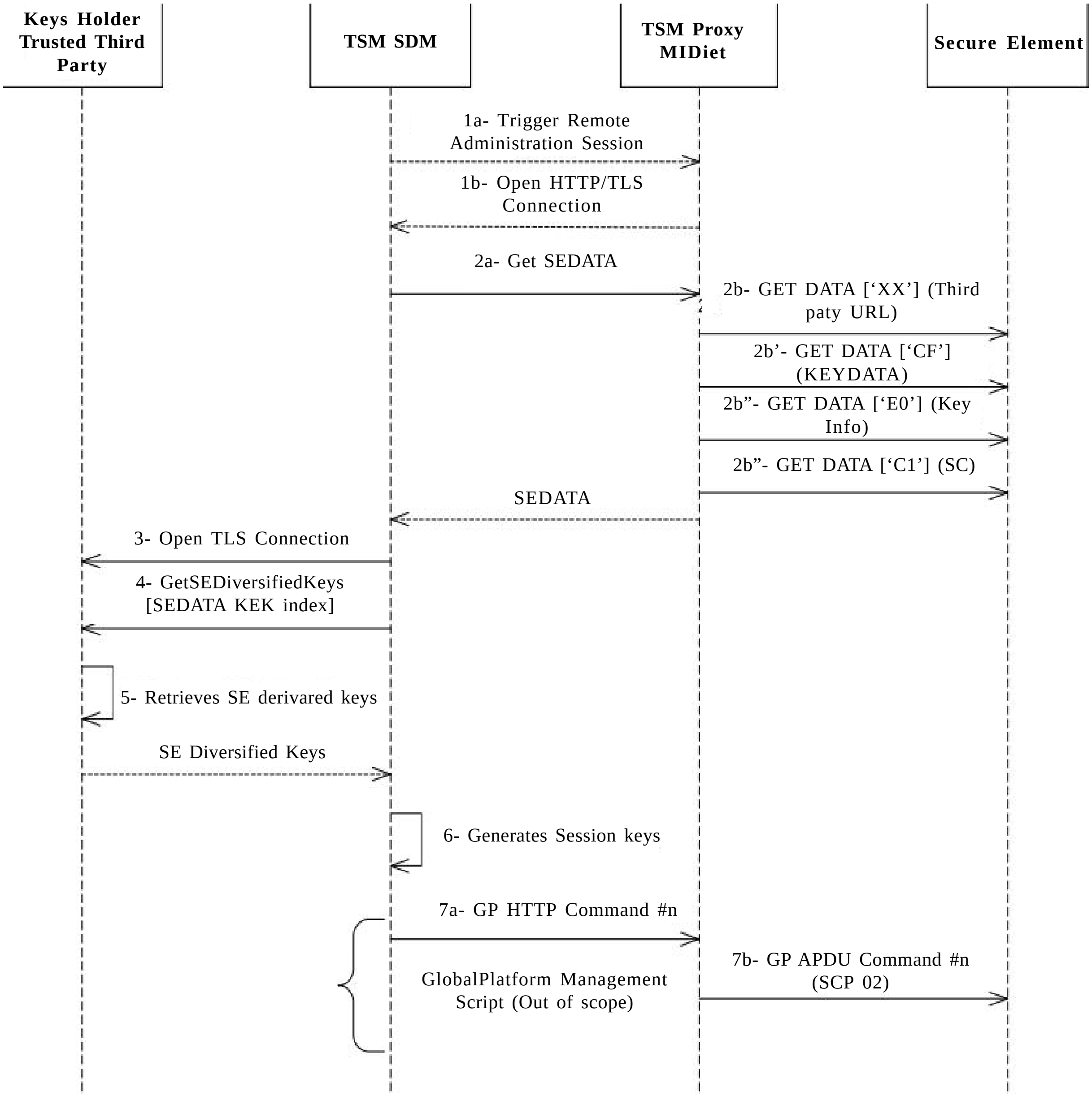
Keys Holder Trusted Third Party
TSM SDM
TSM Proxy MIDiet
Secure Element
1a- Trigger Remote Administration Session
1b- Open HTTP/TLS Connection
2a- Get SEDATA
2b- GET DATA [‘XX’] (Third paty URL)
2b’- GET DATA [‘CF’] (KEYDATA)
2b”- GET DATA [‘E0’] (Key Info)
2b”- GET DATA [‘C1’] (SC)
SEDATA
3- Open TLS Connection
4- GetSEDiversifiedKeys [SEDATA KEK index]
5- Retrieves SE derivared keys
SE Diversified Keys
6- Generates Session keys
7a- GP HTTP Command #n
7b- GP APDU Command #n (SCP 02)
GlobalPlatform Management Script (Out of scope)

Figure 5. On-demand keys distribution flow

7. Conclusion

The on-demand distribution of secure element keys meets a real need and is a major factor for the widespread adoption of NFC technology by manufacturers of electronic equipments. It was presented to the standardization bodies in the field and has received positive feedback. GlobalPlatform will add a new tag in the next version of the specification and EMVCo sees a way to make possible the key management chain of an embedded Secure Element.

References

[1] Lina Alchaal, Vincent Roca. (2004). Managing and securing web services with vpns. *In*: Proceedings of the IEEE International Conference on Web Services (ICWS’04).

[2] Vincent Alimi, Marc Pasquet. (2009). Post-distribution provisioning and personalization of a payment application on a UICC-based Secure Element. *In*: 1st International Workshop on Sensor Security.

[3] GlobalPlatform. About Mobile Task Force. http://www.globalplatform.org/aboutustaskforcesmobile.asp.

[4] GlobalPlatform. (2006). GlobalPlatform Card Specification Version 2.2.

[5] GlobalPlatform. (2007). GlobalPlatform Card v2.2 *Amendment B – Remote Application Management over HTTP*.

[6] GlobalPlatform. (2012). GlobalPlatform Card v2.2 *Amendment C – Contactless Services*.

[7] Gerald Madlmayr, Josef Langer. (2008). Managing an nfc ecosystem. 7th International Conference on Mobile Business.

[8] Gerald Madlmayr, Josef Langer, Christian Kantner, Josef Scharinger. (2008). Nfc devices: Security and privacy. Availability, *Reliability and Security*, *International Conference on*, 0, p. 642–647.