

# **White Paper**

## **Alternatives for Banks to offer Secure Mobile Payments**

Mobey Forum represents leading banks having over 331 million customers worldwide, leading mobile device manufacturers and semiconductors in addition to payment processors and mobile service providers. This paper has particularly profited from the contributions of members such as Deutsche Bank, Giesecke & Devrient, Inside Contactless, Nokia, Nordea, Valimo and Venyon. It has been extensively reviewed by the entire Mobey Forum and endorsed by the Mobey Forum board of directors.

## Table of Contents

1.	Introduction: Empowering MFS through Open SEs.....	5
1.1.	Objectives of this paper .....	5
1.2.	Reference points used in this paper .....	6
1.2.1.	Status of the MFS Ecosystem .....	6
1.2.2.	Role of SEs for MFS .....	7
1.2.3.	SE-related roles in the MFS Ecosystem: SE Vendor, SE Issuer, Application Issuer and Trusted Service Manager ..	8
1.3.	Applications for MFS, SE issuance, lifecycle management and TSM pricing models .....	13
2.	Analysis of SEs.....	16
2.1.	Sticker .....	16
2.1.1.	Concept description .....	16
2.1.2.	Business model scenarios .....	17
2.1.3.	Technical enablers and inhibitors .....	18
2.1.4.	Opportunities and challenges .....	18
2.2.	Secure Micro SD Card (Secure $\mu$ SD) .....	19
2.2.1.	Concept description .....	19
2.2.2.	Business model scenarios .....	21
2.2.3.	Technical enablers and inhibitors .....	24
2.2.4.	Opportunities and challenges .....	25
2.3.	Universal Integrated Circuit Card (UICC).....	26
2.3.1.	Concept description .....	26
2.3.2.	Business model scenarios .....	26
2.3.3.	Technical enablers and inhibitors .....	28
2.3.4.	Opportunities and challenges .....	28
2.4.	Embedded Secure Element (eSE).....	29
2.4.1.	Concept description .....	29
2.4.2.	Business model scenarios .....	29
2.4.3.	Technical enablers and inhibitors .....	31
2.4.4.	Opportunities and challenges .....	31
2.5.	Trusted Mobile Base (TMB) .....	33
2.5.1.	Concept description .....	33
2.5.2.	Business model scenarios .....	34
2.5.3.	Technical enablers and inhibitors .....	35
2.5.4.	Opportunities and challenges .....	35
3.	Summary on Open SEs and the outlook for MFS .....	36
	Appendix - Requirements table .....	39
aa.	Prerequisites .....	39
i.	Multi-Application management capability.....	39
ii.	Secure management across the full lifecycle of MFS Apps.....	39
iii.	Interoperability across locations.....	40
iv.	Compliance with applicable law .....	40
bb.	Initial Bank Requirements: Table .....	40
cc.	Operational Bank Requirements: Table.....	43
dd.	Security Bank Requirements: Table .....	44
	List of References.....	45

## List of Figures

Figure 1: Potential Secure Elements for Mobile Financial Services.....	7
Figure 2: The Mobile Financial Services Value Chain.....	9
Figure 3: Key Provisioning Process to Secure Elements .....	12
Figure 4: Service Areas of MFS Applications and Secure Elements .....	13
Figure 5: Conceptual combination of payment and SE issuance processes .....	14
Figure 6: Stickers in the context of the MFS Value Chain and the Stakeholders.....	17
Figure 7: Secure Micro SD in the context of the MFS Value Chain and the Stakeholders .....	21
Figure 8: UICC in the context of the MFS Value Chain and the Stakeholders.....	27
Figure 9: eSE in the context of the MFS Value Chain and the Stakeholders.....	31
Figure 10: TMB in the context of the MFS Value Chain and the Stakeholders .....	34
Figure 11: Overview of Value Chain, Stakeholders and SEs for MFS .....	37

## List of Abbreviations

<b>μSD</b>	Micro SD
<b>2G / 3G</b>	2nd Generation / 3rd Generation
<b>AI</b>	Application Issuer
<b>App</b>	Application, here for mobile devices
<b>API</b>	Application Programming Interfaces
<b>B2B</b>	Business to Business
<b>B2C</b>	Business to Customer
<b>BOM</b>	Bill of Material
<b>CC</b>	Common criteria for Information Technology Security Evaluation
<b>CPU</b>	Central Processing Unit
<b>CSIM</b>	CDMA Subscriber Identification Module
<b>EMV / EMVCo</b>	Europay-MasterCard-Visa, EMV is a Trademark; Specifications and requirements are called EMV specifications / requirements. Definition body for these is EMVCo.
<b>eSE</b>	embedded Secure Element
<b>FI</b>	Financial Institutions
<b>GB</b>	Giga Bite
<b>ID</b>	Identity
<b>LCM</b>	Life Cycle Management
<b>MCP</b>	Mobile Contactless Payment
<b>MNO / MVNO</b>	Mobile Network Operator / Mobile Virtual Network Operator
<b>NFC</b>	Near Field Communication
<b>OBC</b>	On Board Credentials
<b>ODM</b>	Original Design Manufacturers
<b>OTA</b>	Over-The-Air
<b>OTP</b>	One-Time-Password
<b>P2P</b>	Peer-To-Peer (also Person-To-Person)
<b>POS</b>	Point-Of-Sale
<b>SD</b>	Secure Digital
<b>SE</b>	Secure Element
<b>SEI</b>	Secure Element Issuer
<b>SEPA</b>	Single Euro Payments Area
<b>SEV</b>	Secure Element Vendor
<b>SIM</b>	Subscriber Identity Module
<b>SMS</b>	Short Message Service
<b>SP</b>	Service Provider
<b>SWP</b>	Single Wire Protocol
<b>TMB</b>	Trusted Mobile Base
<b>UI</b>	User Interface
<b>UICC</b>	Universal Integrated Circuit Card
<b>UMTS</b>	Universal Mobile Telecommunications System
<b>USIM</b>	Universal Subscriber Identity Module

## Executive Summary

Security is one of the fundamental elements of any payment solution. Financial Institutions increasingly seek to mitigate the risk of fraud in order to protect their customers and hence their own payment franchise. Enhanced security on plastic cards requires a so-called "Secure Element (SE)" - like a chipcard - to store the bank's payment credentials (security keys) and other critical data. One example is the introduction of "Chip and PIN" (EMV chip-based security) on cards in Europe to replace magstripe-based systems.

While the direction for plastic cards seems clear, the Industry is looking for ways to secure Mobile Payments at a comparable level. The question is then, which SE in the mobile handset is available to facilitate the mass-market introduction of secure mobile payments?

Mobey Forum has taken this topic as a subject of the current White Paper. It elaborates on the question how different Secure Elements (SEs) can enable Financial Institutions (FIs) to offer Mobile Financial Services (MFS) and hence empower the take-off of the MFS ecosystem. It is targeted at business managers in Financial Institutions. For them, it strives to clarify the business implications of the various technical SE alternatives. Therefore:

The paper presents a brief status analysis of the MFS Ecosystem and the Stakeholder positions in the MFS Value Chain. This includes a short introduction of the SE-related Stakeholder roles in the MFS Ecosystem (SE Vendor, SE Issuer, Application Issuer and Trusted Service Manager) as well as a comment on the various Applications for MFS, the SE issuance process, the lifecycle management and potential Trusted Service Manager (TSM) pricing models. (Chapter 1)

Based on this conceptual framework, the paper elaborates on the potential roles of the different SEs for MFS. The analyzed SEs are: Stickers (active and passive), Secure Micro SD Cards, Universal Integrated Circuit Card, Embedded Secure Element and Trusted Mobile Base. For each of the SEs, a concept description, different business model scenarios, technical enablers and inhibitors and opportunities and challenges are presented. (Chapter 2)

The paper concludes with a summary about the various SE alternatives for MFS and presents a brief outlook on the next steps for the MFS industry. (Chapter 3)

It is complemented by a detailed appendix on the requirements towards SEs for MFS (Appendix).

In brief, the paper finds that each FI now needs to decide which position it wants to claim in the MFS Value Chain – to become an SE Vendor, SE Issuer, Application Issuer or a combination of these? As a consequence, the FI will be able to choose the adequate SE alternative and decide which process of key provisioning shall be implemented. Furthermore, the choice of a precise MFS Value Chain position and SE technology will help the FI to identify the most interesting partners to establish joint business models and trigger a quick diffusion of MFS.

# 1. Introduction: Empowering MFS through Open SEs

## 1.1. Objectives of this paper

The objective of this document is to describe and review the different SE solutions for Mobile Financial Services (MFS) enabling the respective Applications (Apps), e.g. for mobile contactless payments, mobile banking, remote mobile payments and other services, allowing a variety of open business models to kick-start the MFS market. The solutions evaluated in this paper include the following:

- **Stickers (see Section 2.1):** Contactless cards, manufactured in form of a Sticker that can be personalized and processed through the existing banking infrastructure. Customers can place the Sticker on their phone for NFC payments. There are Active and Passive Stickers. The static Stickers that do not have any connection to the phone are called Passive Stickers. Recently, technology solutions have been introduced that will establish a connection between the Sticker and the phone user interface (UI) through Bluetooth. These are called Active Stickers since there is a connection to the phone operating system and user interface, which makes the Sticker to become an integrated part of the phone.
- **Secure Micro SD card (Sec.  $\mu$ SD; see Section 2.2):** In the context of this document SD (Secure Digital) refers to memory card products that hold an embedded chip which can be used as a SE. These SD products may or may not hold a Near Field Communication (NFC) antenna in addition. In this paper, reference is mainly made to Secure SD cards in the form factor of Micro SDs.<sup>1</sup>
- **Universal Integrated Circuit Card (UICC, see Section 2.3):** A generic and well standardized a physical and logic platform for Smart Card Applications. The UICC is issued by one party who will usually include at least one Application on the card. UICC cards have been used typically by Mobile Network Operators (MNOs) who have included a USIM (UMTS/3G SIM) Application on the Card to authenticate the user in a 3G network.<sup>2</sup>
- **Embedded Secure Element (eSE; see Section 2.4):** A security component, which is embedded in a mobile device and is capable of storing and handling business and personal information in a secure manner.<sup>3</sup> This dedicated Smart Card chip is embedded to the mobile Handset at the time of manufacturing.
- **Trusted Mobile Base (TMB; see Section 2.5):** Is a secure isolated section on the core processors (CPU) of mobile devices from various Vendors into which various secure Applications can be provided flexibly and over-the-air (OTA). The TMB is linked to a secure User Interface (UI). The TMB cannot be considered to be a full-fledged SE at the moment, but based on today's information has the full potential of becoming a Secure Element in the future. The TMB can also assist in achieving required security level together with the other SE alternatives.

<sup>1</sup> Note: Given that the mobile device has an SD card slot, Micro SD, Mini SD and "normal" SD can all be used, e.g. via adaptors.

<sup>2</sup> Note: This paper focuses as UICC as next technology in the SIM context. The transition from SIM Cards to UICCs is related to the introduction of 3G networks. Therefore approx. 20-25% of the installed SIM base are UICCs at present, for up to date percentages on UICC market share, see e.g. [www.gsmworld.com](http://www.gsmworld.com)

<sup>3</sup> PrimeLife 2008: D 6.2.1 Infrastructure for Trusted Content, p. 20

This paper reviews the above mentioned solutions with regards to their capabilities, their business impact and their security<sup>4</sup> in order to present the Stakeholders of the MFS Value Chain with an overview of alternatives for the implementation of MFS with Secure Elements (SEs), e.g. for mobile contactless payments or other MFS utilizing SE to assist in identification or transaction confirmation.

It does so in a step-by-step approach, presenting the different SEs on a well funded base of references. By building an overall understanding, it intends to support:

- The conceptualization of business models for MFS<sup>5</sup>
- The decision-taking process of the Stakeholders along the MFS Value Chain
- The empowerment of market take-off

The business model scenarios described in this document reflect the main current trends in Mobile Financial Services and do not intend to be final. In general, the here presented technologies allow for a large number of collaborative settings between the Stakeholders along the MFS Value Chain. Today, the Ecosystem around the Value Chain is still very fragmented and complex. By explaining how different SE technologies will empower the Value Chain and the Stakeholders in it, this paper aims to detail alternative approaches, promote collaboration and hence assist in reducing the Ecosystem complexity which currently slows down market take-off.

## **1.2. Reference points used in this paper**

A brief explanation of reference point of this paper applies for the sake of clarity:

### **1.2.1. Status of the MFS Ecosystem**

The first Mobile Contactless Payment (MCP) pilot started 2003, and since then there have been many pilots testing the NFC Payments.<sup>6</sup> By now it has been proven that the technology works and consumers love it.<sup>7</sup> However, even globally, there are only few commercial services on the market. The MCP industry is now in an “Ecosystem Building” phase. The definition of money flows and detailed roles of the Stakeholders continue to be the main discussion points, especially in collaborative business models. It seems that there are severe challenges in reaching a consensus, particularly regarding the renting or “selling” of the required SEs or SE spaces amongst the key Stakeholders. However, only a collaborative mindset and actions would enable building a business case for all parties. Furthermore, the complexities and inter-dependencies of the MCP Ecosystem have proven to be even higher than earlier expected. This slows down the implementation of collaborative models. This status is equally valid for all business models which require the usage of an SE and relate to different domains of MFS – be it mobile contactless payments or other financial transactions.<sup>8</sup>

<sup>4</sup> Note: The purpose of the report is not to state security requirements or assess the security of the different SEs but rather relate to the key aspects

<sup>5</sup> Note: This paper does not address the regulation discussion. Rather, it points towards the entities which will need to derive the certification and security requirements, depending on the nature of the respective Application

<sup>6</sup> Note: See e.g. GSMA (2008) and MobeyForum (2009a)

<sup>7</sup> Note: See MobeyForum (2009b)

<sup>8</sup> Note: If the SE is not required, then implementation is very straight forward for the individual party and no liaising with other parties along the Value Chain is needed.

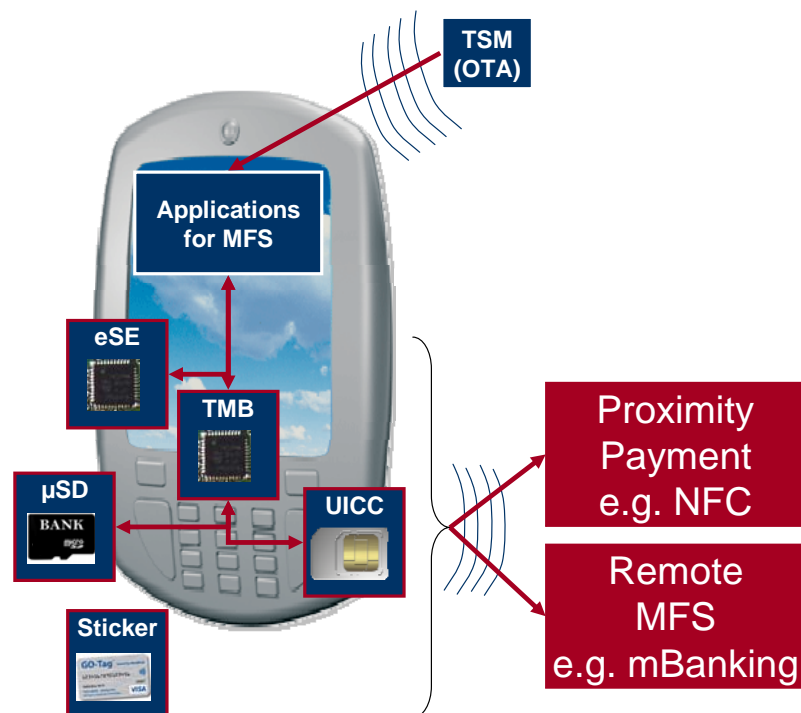
Therefore, understanding the characteristics of the various Secure Elements (SEs) will play an important role for the different Stakeholders along the Value Chain of the mobile industry in general and MFS in particular. Whoever dominates the respective SE will have a strong position to build trusted services around the SE, in all possible definitions of MFS.

### 1.2.2. Role of SEs for MFS

A Secure Element (SE) is a platform where Applications can be installed, personalized and managed, preferably over-the-air. It is a combination of hardware, software, interfaces and protocols that enable the secure storage and usage of credentials for payments, authentication and other services. Conceptually, SEs can be categorized into three areas:

- Removable SEs (e.g. Stickers, Secure Micro SD cards and UICCs)
- Non-removable SEs (e.g. embedded SEs)
- SEs from a combination of software programs on dedicated hardware (e.g. Trusted Mobile Base).<sup>9</sup>

The following figure shows the different SEs that are eligible within the concept of MFS and are covered in this paper:



**Figure 1: Potential Secure Elements for Mobile Financial Services**

<sup>9</sup> Note: In the case of the TMB, the SE consists of a physical module, e.g. a partition of the CPU and software embedded into this physical module (e.g. a secure operating system). For a detailed elaboration on the different categories of SEs, see Mobey Forum (2005), p.4f.

SEs assure security in these service processes, especially in Mobile Financial Services. Hence, all SE discussions in this paper relate to Applications that are provided with additional security via the SE. These are different to the widely diffused Applications of, e.g., mobile banking that rely on for instance java midlets or other downloadable applications and base their security on external (from phone) mechanisms.

Beyond their role for Application security and trustworthiness, SEs are branding devices, representing the SE Issuer (and potential partners) on the SE form factor and enabling the branding of SE-based Apps via the mobile device's display. SEs also often enable issuer-based policy decisions on the functionality of the Mobile Device and may influence, directly or indirectly, the way the user interacts with the device.<sup>10</sup>

At present, the use of a SE is only mandatory for the EMV-based contactless payment area, based on the EMVCo<sup>11</sup> requirements. However, a SE may be used also for other MFS areas like mobile banking or payments, particularly in Applications where the End Consumer manages and transfers larger amounts of financial resources via his mobile device.<sup>12</sup> Herein, the SE can also be used as a storage and processing platform for the identification of individuals and their credentials.<sup>13</sup>

### 1.2.3. SE-related roles in the MFS Ecosystem: SE Vendor, SE Issuer, Application Issuer and Trusted Service Manager

Four main Stakeholders along the Value Chain of Mobile Financial Services bear an essential role in making the overall system work:

- **The SE Vendor (SEV):** The physical producer of the SE. This can be chipset corporations (esp. for TMBs), Handset providers (esp. for eSEs) and other SE producers, e.g. in the domain of Stickers, Secure Micro SD cards, or UICCs.<sup>14</sup>
- **The SE Issuer (SEI):** The entity that sources the SE from the SEV, controls the SE's root keys, brands the SE and provides it to the End Consumer. The SEI can also open the SE to additional AIs, e.g. SEIs can be MNOs, Banks, Transport Authorities, or Customer Loyalty Programs or even TSMs that provide this service to Application Issuers. Alternatively, SEIs can also be independent companies that wish to empower MFS and claim a position in the newly developing MFS Ecosystem.
- **The Application Issuer (AI):** The party that offers an SE-related Application to the End Consumer for its own business purposes, e.g. a Bank, Transport Authority, or Customer Loyalty Program.<sup>15</sup>

<sup>10</sup> Note: This paper assumes that the user experience is consistent across the different SE alternatives when it comes to actual usage of the Application. In the understanding of "mobile integrated Applications" the user experience should not differ largely between the different SE that leverage the Operating System of the mobile device. Passive Stickers without a link to the OS, however, will have a less interactive user experience. However, UICC may differ here based on the potential SE Issuer decisions referred in the text.

<sup>11</sup> Note: In particular in EMV-based proximity payments.

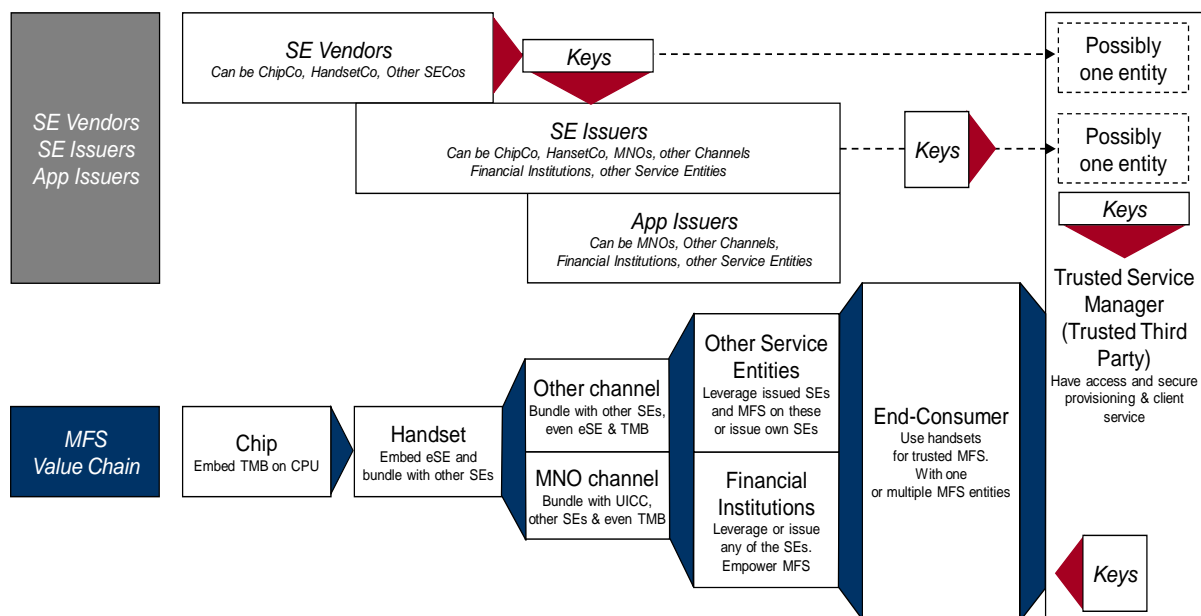
<sup>12</sup> Note: Management of transfer of higher volume financial resources is also possible without employing an SE. To manage their risk in MFS, however, Financial Institutions are increasingly expected to apply SEs.

<sup>13</sup> Note: For a detailed analysis of the necessary infrastructure for trustworthy, privacy-enhancing and identity conscious mobile services, see PrimeLife (2008) and PrimeLife (2009)

<sup>14</sup> Note: In some cases the SE Vendor is also the SE Manufacturer, but not in all cases. For instance in the case of eSE the handset vendor is the SE Vendor but not the manufacturer.

<sup>15</sup> Note: Other publications might refer to the Application Issuer (AI) as Application Provider. For the sake of clarity, this paper uses the term AI to differentiate even more clearly between App Issuance and Provisioning. This is particularly relevant

- **The Trusted Service Manager (TSM):** An entity that AIs or SEIs may use in different phases of the SE's lifecycle and the Applications' lifecycle to manage the distribution, updating and trouble-shooting. TSMs may be controlled either by an SEI, or by an AI (Financial Institution or Other Service Entity). TSMs may also facilitate the business between numerous SEIs and AIs so that not every AI needs to make an agreement with every SEI, and vice versa. In this set-up, a TSM can even be an autonomous entity (e.g. a private company) or a collaborative entity set-up by different AIs.<sup>16</sup>
- **The Service Provider (SP):** AIs can provision the Applications that they issue on their own behalf to the End Consumer. Alternatively, they can employ a Trusted Service Manager to handle the service. Hence, TSMs and AIs can both be referred to as Service Providers (SPs) that eventually face the End Consumer. Whoever faces the End Consumer and take liability for the offered MFS, is perceived as the SP in this paper. Financial Institutions, Other Service Entities and potentially the TSMs are the most likely SPs of the Applications that empower MFS (see Figure 2 and the below sections on practical examples).



**Figure 2: The Mobile Financial Services Value Chain**

Starting from the point of view of the End Consumer, the following motivations apply along the Value Chain of MFS:

- Financial Institutions and Other Service Entities<sup>17</sup> want to deploy new and additional services to the End Consumer. For these, they will issue new Applications and may use SEs to make them more secure. Both parties are referred to as Application Issuers (AIs) in this paper. From the perspective of these two Stakeholders, the first potential enablers are NFC-enabled Secure Micro SD cards

because the AI conceptualizes the MFS and leverages his business processes to execute it, but might outsource the provisioning and management of the Application to a Third Party such (e.g. a TSM) or use another Service Provider's SE (e.g. an MNO's) to make the Application accessible for his (the AI's) End Consumers. Example: An Insurance company issues an Application and draws upon external partners / outsources all other related aspects to SEI and a TSM.

<sup>16</sup> Note: There are examples where a TSM between Banks and MNO's have wider than a pure TSM role, see e.g. www.bankID.com. Also, the Malaysian Certificate Authority Trustgate holds a trusted position between banks and MNO's. In this role it enables secure remote payments and remote CitizenID by using SIM Cards as SEs.

<sup>17</sup> Note: Other Service Entities can e.g. be transport authorities, merchants, customer loyalty programs, frequent traveler service offerings, Service Entities of governmental nature etc.

and Stickers, as both can be rapidly deployed and flexibly attached to the mobile devices.

- Mobile Network Operators (MNOs) and Other Channels of Mobile Device distribution<sup>18</sup> may wish to add MFS to their service offering. Here, they could leverage their position in the UICC (i.e. the MNO), collaborate in shared UICCs or employ other SEs (i.e. the other distribution channel actors such as the Retailers). If these two parties want to issue Applications on their own behalf, they will become AIs as well. Otherwise, they will focus on providing the SE, hence becoming SE Issuers. Alternatively, MNOs can decide not to get directly involved with MFSs and instead leave all MFS offerings to FI – then, MNOs would merely focus on profiting from MFS through the increased mobile service usage (i.e. increased data traffic) or in the role of a merchant for e.g. selling mobile content.
- So far, Handset Vendors have shipped their NFC devices with embedded SEs to empower the MFS Value Chain. In the future, Handset Providers may decide to offer MFS themselves and / or collaborate with others to do so. Also, they may decide to bundle their Handsets with other SEs than embedded ones. If Handset Providers want to be in charge of activating the SEs in their phones, then they may decide to become SE Issuers as well.
- Chip Vendors can integrate additional open SE architectures and platforms into the Central Processing Unit (CPU), leveraging the Trusted Mobile Base (TMB) concept. Hence, they can empower all Stakeholders in the subsequent Value Chain to integrate MFS on a flexible, over-the-air basis. This is expected to fuel and integrate the MFS ecosystem even further in the mid- to long-term. If chipset providers want to be in charge of activating the SEs in their chips, then they will become SE Issuers as well. Otherwise they can leave the issuance process to subsequent parties in the Value Chain.

Therefore, the various SEs have a dominant link to selected Stakeholders along the Value Chain, as those are respectively in charge of the hands-on implementation of the SEs into the mobile device. However, building Stakeholder alliances that collaborate across different Value Chain steps and integrate the different perspectives can be expected to be an important prerequisite for the provisioning of real-life implementations of SE-based MFS.

In practical terms this structure of the MFS Value Chain and the need for collaboration across Value Chain modules can materialize in an almost unlimited number of constellations:

### **Examples of Stakeholder positions along the MFS Value Chain**

In one example, a FI can decide to be SE Issuer and have full control over the SE – hence, even opening it to other Application Issuers for additional Mobile Financial Services. Here, the FI would be able to process the financial transaction for these services via the SE that it issued. Alternatively, it can keep the SE proprietary and not open it for any other AI.

---

<sup>18</sup> Note: These particularly apply esp. in countries where mobile device subsidies by the MNO do not dominate the distribution logics. Market consensus refers to approx 50% of mobile devices being distributed to the market through other distribution channels than the MNOs. For up-to-date figures, refer to industry bodies, e.g. [www.gsmworld.com](http://www.gsmworld.com), or market intelligence providers.

In another example, a FI can decide to merely be the AI, only controlling the specific keys of its own App, but not the root keys of the SE. In this case, the FI is a (depending) B2B-client of the SEI.

Additionally, a TSM can be a B2B partner to the SEV, SEI, and AI, managing the service in a trusted manner for the FI or any other Service Entity.

Alternatively, a SEV and / or SEI can decide to simultaneously also act as a TSM (or vice versa, a TSM as SEI), thus creating the root keys and through the control over these having dominance of the entire SE, managing the SE over its lifecycle and potentially opening (or consciously not opening) the SE to other Service Providers which may then become Application Issuers, paying the TSM / SEV / SEI for access to the SE.

From the End Consumer perspective, AIs, SEIs and TSMs will need to agree on the rules of customer care as the end-user may not know who to call in case of Service problems. This is especially the case when AIs, SEIs and TSMs are different legal entities and brands.

Overall, a Financial Institution or any Other Service Entity can decide to be AI only, SEI and AI or integrated SEI, AI and TSM. This potential overlap of roles along the MFS Value Chain make the set-up of the Ecosystem so complex, but bear large potential for any party that manages to integrate the different motivations and perspectives along the Value Chain into a consistent system offering.

### **SE keys as crucial pivot:**

In any decision concerning the Financial Institutions' or Other Service Entities' positions in the MFS Value Chain, dominance and management over the keys for the SE plays a crucial role: Whoever manages the root keys of the SE, holds the power over the SE and can subsequently structure a business around it.

The enrolment and provisioning processes of NFC Payments, for example, are based on the GlobalPlatform Smart Card standard<sup>19</sup> for all SEs (e.g. UICC, eSE or Secure  $\mu$ SD Card, TMB standardization is ongoing). Although some options slightly differ for the respective SEs, the global provisioning model, processes, protocol and infrastructure building blocks are shared and this allows for consistent investments that are replicable over the different solutions. Figure 3 provides an overview of a generic NFC payment Application issuance model.

GlobalPlatform distinguishes between (SE) Issuers in charge of card content management and Application Providers responsible for Application management<sup>20</sup>. An Application usually gets a unique identifier and is made up of its Executable Code and Data. Each player may get allocated a Security Domain which is a secured, isolated, firewalled, dedicated space on the SE guaranteeing the security of its essential assets (i.e. Access Keys, Application Code and Data). Security Domains hold keys for encryption, decryption, signature verification, off-card authentication,

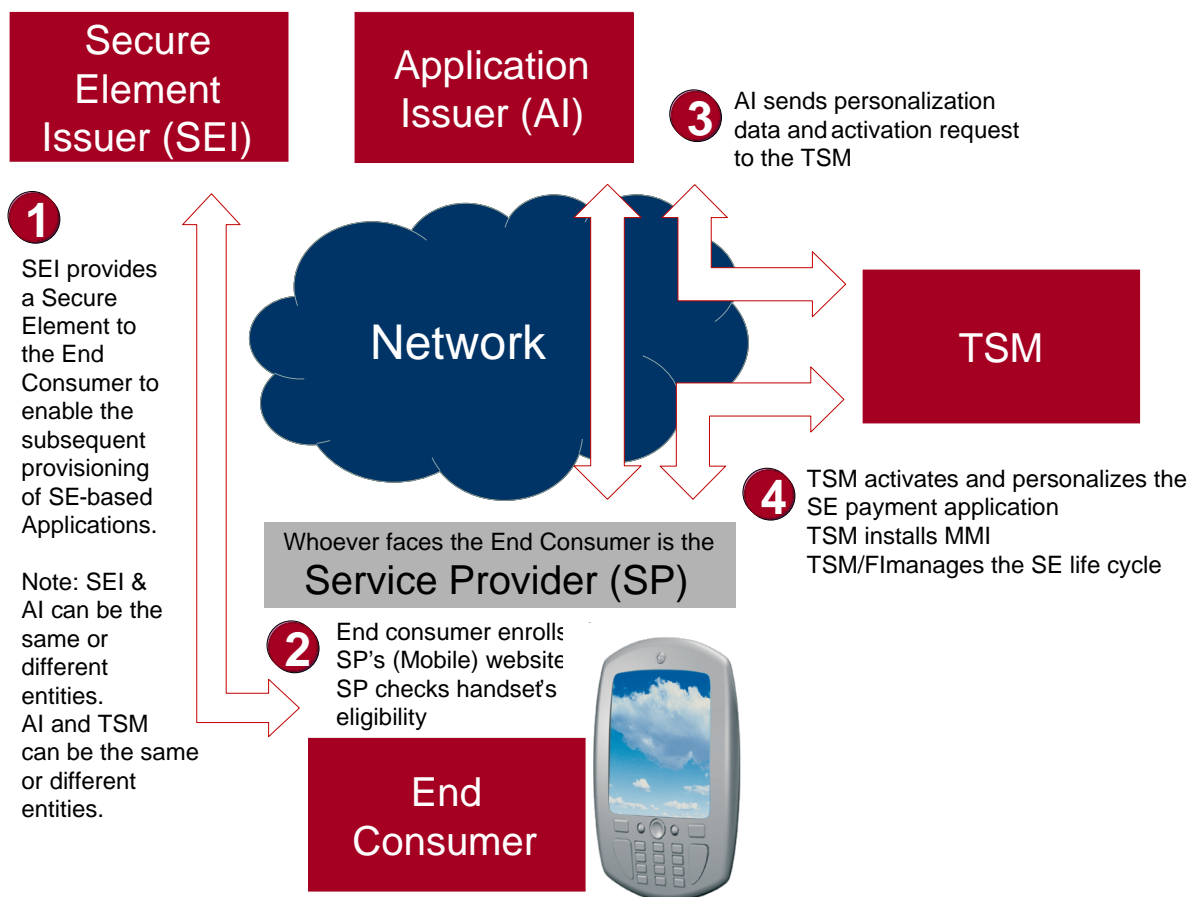
<sup>19</sup> This standard, endorsed by EMVCo and the biggest payment schemes, offers payment-grade secure card content management over any kind of network (fixed or mobile). It specifies dynamic card and Application management as well as Application loading, personalization and life cycle management in a collaborative multi-partner and multi-Applications environment. This issuance standard has been combined for NFC with the TSM (Trusted Service Manager) model.

<sup>20</sup> Note: Application providers are referred to as TSMs or Application Issuers in this paper, relating to the above mentioned explanation of the Value Chain structure.

etc. The Security Domain “belongs to” and is operated by the associated SP, being a TSM himself or working via a TSM.<sup>21</sup> In the latter case, the SP delegates the loading and installation of its Applications to a TSM. This encompasses the creation of its Application Provider Security Domain and the management of its Application loading, personalization and activation.

For example, the SP may get the key for managing its Security Domain from the SE Issuer in a secured way described by GlobalPlatform. The TSM is in charge of securely and confidentially transferring the SP’s keys to the Service Provider’s Security Domain on the SE. Depending on the granted privileges this can be done under SE Issuer control or without the SE Issuer’s involvement.<sup>22</sup>

The SE Issuer gets the Root Keys<sup>23</sup> of the SE from the SE Vendor, enabling him to take control of the SE and to create the Security Domain structures.<sup>24</sup>



**Figure 3: Key Provisioning Process to Secure Elements<sup>25</sup>**

<sup>21</sup> Note: Global Platform also defines different management models, allowing for different levels of flexibility, privacy and control from either the SE Issuer or the Application Issuer. In addition, Application Issuers are granted so called Privileges, giving them more or less autonomy and control in managing the Security Domain. Further, multiple Security Domains can be managed by multiple TSM. Single Security Domains normally relate to single TSMs.

<sup>22</sup> Note: This is one option within Global Platform. In alternative cases, it can be that the keys are not transferred at all.

<sup>23</sup> Note: In the Global Platform terminology these are called Temporary ISD Keys.

<sup>24</sup> Note: For a detailed description of the key provisioning alternatives in shared SEs, see Mobey Forum (2008), p. 48ff. In brief, it finds: Normally, OTA keys are used by the MNO to protect UICC. However, sell-sub keys can be sold to AIs, such as Financial Institutions to enable them to manage their own MFS Applications. Alternatively, key distribution can also be handled by the UICC Vendor. In this case, the MNO does not see any OTA sub keys at all. By using an OTA sub-key sharing mechanism and pre-loading Applications, all of the above indicated business models can be implemented without introducing new technology.

In comparison to the Mobey Forum (2008) paper, the here presented work now offers both options of sharing and not sharing the SE.

### 1.3. Applications for MFS, SE issuance, lifecycle management and TSM pricing models

#### Applications for MFS:

The Applications for MFS to which this paper refers are defined as service modules that enable a multimedia interaction on mobile devices, in particular to execute Mobile Financial Services such as payments for goods and services and mobile banking<sup>26</sup>.

Conceptually, this paper refers to the MFS with Applications as they are shown in Figure 4. The below presented MFS Applications can also be executed without leveraging SEs. Especially in the so called Card Not Present-environment, e.g. in online transactions, other security methods such as One-Time-Passwords (OTP) may also be used.

Enhancing MFS through SEs becomes particularly relevant when transaction volumes increase beyond marginal payments and / or the usage of an SE is legally required. Also, the industry is seeing a general trend towards protecting Financial Services with additional tokens such as the SEs presented in this paper.

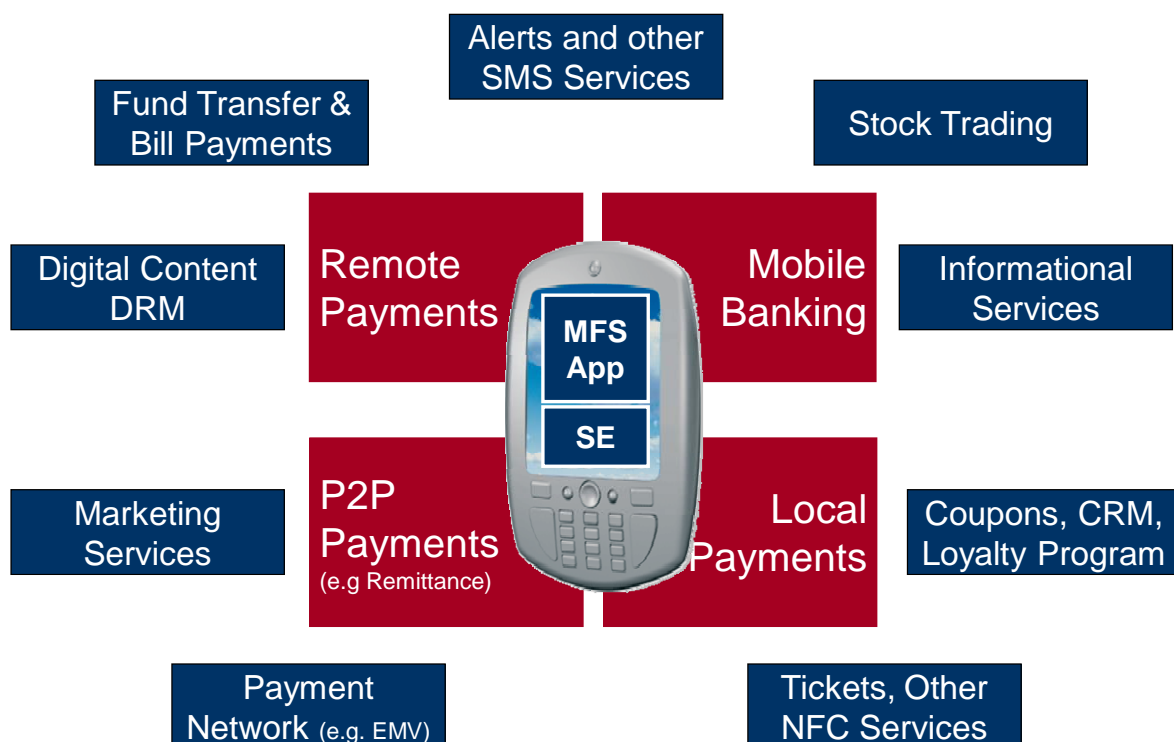


Figure 4: Service Areas of MFS Applications and Secure Elements

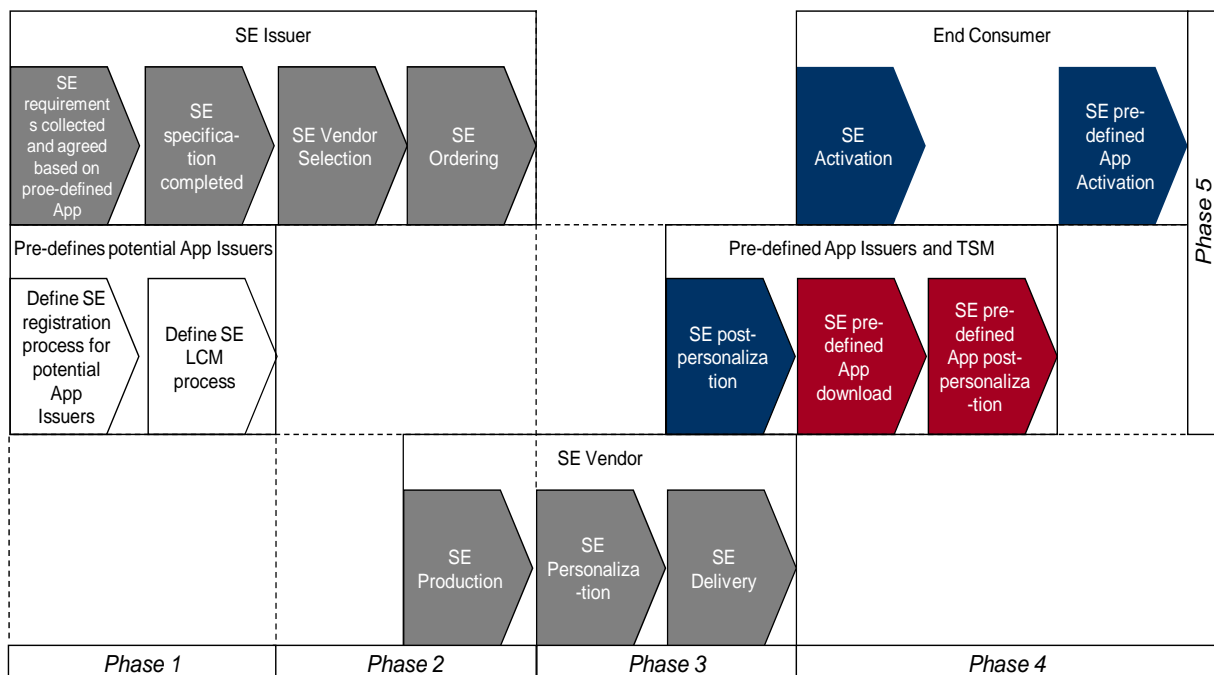
<sup>25</sup> Note: The SEI / AI / TSM can be: a) One entity/company; b) two separate entities / companies; c) Three separate entities / companies.

<sup>26</sup> Note: Including banking Applications such as mobile remittance, i.e. the sending money over distance via the mobile device in one country to another country.

Technically, the above mentioned Applications do not only include the interaction modules shown on the display of a mobile device, but also the underlying credentials that identify and authorize the holder of the mobile device to enter financial interactions, e.g. EMV Profiles (i.e. card applets<sup>27</sup>), ID credentials such as private keys, CAP applications or One-Time-Password Lists. These technical modules of the MFS Applications enable the crucial backend processes on which the seamless experience of the End Consumer is based, e.g. the backing of a MFS through a Credit Card or a bank account, and related individual authentication.<sup>28</sup> The Issuer of the MFS Application (i.e. the AI) is controlling the interoperability aspect and features of the Application. An SE may host multiple Applications.

**SE Issuance Process:**

Comparing the presently given issuance process of payment cards and SIM cards, the former are personalized during their highly secure production process (i.e. having a verified name and existing address to which they are matched before their production is ordered), whilst the latter are being produced as blank elements, which are then personalized at the point-of-sale once an End Consumer buys them off the shelf of the MNO.



**Figure 5: Conceptual combination of payment and SE issuance processes**

In order to leverage the SE alternatives here discussed, it will be necessary to specify processes through which the unique identity of the individual End Consumer can be verified and the respective Stakeholders can secure their ownership of the relationship to the individual customer. Also, any process changes shall not impact the continuation of the existing businesses on the mobile devices, e.g. in other

<sup>27</sup> Note: In the wording of EMVCo these would be EMV-based payment applications. Here, EMVCo would define the underlying payment protocols and the entry point for the terminals, but not the contactless payment application itself. The contactless payment applications themselves are defined by the respective Financial Institution, based on EMVCo specifications.

<sup>28</sup> Note: In this document it is not aimed to make any further assumptions on the Payment Application logic. Furthermore, it is assumed that the POS terminal infrastructure supports the AI's payment Applications, i.e. the interoperability is not depending on the SE selected. The SE is able to communicate with POS terminal over a standard interface.

Applications.<sup>29</sup> As a conceptual draft, the SE issuance process could take the form shown in figure 5.<sup>30</sup>

### **Lifecycle management (LCM) of the SE:**

As mentioned above (see section 1.2.3), the FI may choose to use a TSM for LCM services. Here, the FI will remain to be the Security Domain owner. It is up to the FI to decide whether to build the LCM capability in-house or to use a TSM. As an orientation for Make-or-Buy decisions at the FI, the following aspects may assist in estimating Service Prices for a TSM business:

### **TSM investments:**

- The TSM platform / technology supporting all key TSM functionalities.
- The TSM IT infrastructure (e.g. server hardware, Operating Systems, databases, network etc.).
- The TSM data centre.
- The TSM service operation, i.e. having the operations resources to run the TSM services.

Based on these positions, the **TSM may run the following, exemplary, fee models:**

- The TSM charges a one-time fee for service integration, i.e. for the integration with the Application Issuer and assurance of TSM service readiness.
- The TSM charges either a service fee per executed OTA provisioning service<sup>31</sup> or a service fee per executed OTA lifecycle management service<sup>32</sup>.
- The TSM charges one-time implementation fees and service fees thereafter when new service elements are implemented after the initial launch.

The SE Issuers and the AIs can decide to act as TSMs if they wish to control a larger section of the MFS Value Chain, i.e. they are not necessarily depending on interaction with another Trusted Third Party. This is particularly relevant when they employ eSEs, Secure Micro SD Cards, TMB or Stickers. In the case of wanting to employ the UICC as SE for the MFS, however, the AI will have to liaise with the MNO who usually<sup>33</sup> is the SE Issuer of the UICC.

There is no legal obligation to employ a TSM in MFS. EMV and GlobalPlatform have merely set the requirement that the provisioning process needs to be securely managed. So far, industry consensus has grown that that this is managed by a TSM. Nevertheless, the requirement of securely managing the provisioning process could, for example, also be complied with by providing a Software bridge at the respective Service Provider. It does not need to be an independent company.<sup>34</sup>

<sup>29</sup> Note: For a detailed elaboration of the combined SE issuance process, see Mobey Forum (2008), p. 56f.

<sup>30</sup> Note: Mobey Forum (2008), p. 57f.:

“Phase 1 – SE foundation shall be agreed by all key Stakeholders. Pre-defined Application requirements are collected and taken into the framework. SE issuing processes agreed, terms & conditions, liability, security and regulations agreed and lifecycle management details specified. Phase 2 – SE Supplier selection, ordering and manufacturing. SE Issuer selected (not necessarily the same as the SE owner). UICC can be co-owned or owned by one of the Stakeholders. Phase 3 – SE Manufacturing, Delivery and Personalisation according to the payment card requirements. SIM/USIM Application post-personalisation and activation for network access. Phase 4 – SE activation by the end-user. Access to the pre-defined Applications (Payment Card Application, SIM/USIM Application). Phase 5 – SE operational stage, normal lifecycle management. Additional Applications from other Service Providers can be downloaded.

<sup>31</sup> Note: Prices may differ depending on the Application and the services included in the OTA provisioning, e.g. whether data preparation is included or not.

<sup>32</sup> Note: Prices may differ depending on the LCM action such as OTA lock, unlock, delete or post-issuance EMV scripting etc.

<sup>33</sup> Note: Technically, it is also feasible that a FI can issue a “blank” UICC where the USIM application will be personalized afterwards. Hence, the MNO may be the most likely SEI, but this is not necessarily the case.

<sup>34</sup> Note: For detailed insight, refer to publications by industry bodies such as GSMA, EMVCo and Global Platform.

## 2. Analysis of SEs

The AI can decide between different SEs and build his service package independently or together with various SEs and various TSMs.<sup>35</sup> His selection of the SE will depend on his respective business logics and the service level which he wants to achieve.

In order to clarify what the different SEs can do, the following sections describe them one after the other and comment on how they respectively enable competition, drive the market acceptance, are customizable and enable different business models. Also, it is shown which drivers and barriers apply to the different SEs.

### 2.1. Sticker

#### 2.1.1. Concept description

So called “Stickers” are self-adhesive contactless cards or tags designed to be attached on the back of mobile devices. Although being very similar to a standard contactless Smart Card, they have a specifically designed antenna combined with a ferrite backing layer to cut distortion to and from the phone’s components and its radio signal. Currently, there are two forms of Stickers: Passive Stickers and Active Stickers, depending on whether or not they are connected to the Handset’s Application execution environment, i.e. the Operating System. Passive Stickers are widely available while Active Stickers are currently seeing market introduction.

- **Passive Stickers:** These Stickers are compliant with all mobile phones. Being “Passive”, they have no connection to the Operating System of the mobile device. Therefore, they neither allow dynamic Application management, be it by a TSM for Application updates or by the consumer for additional services via a phone’s user interface, nor do they offer the full NFC use case range or multi-Application flexibility. Passive Stickers have been mass produced in millions of units since Q1 2009 for payment and loyalty Applications. Today, they are also certified by the major payment schemes. For traditional memory-only-class non-EMV Passive Stickers, the price point is rather low. EMV-capable full-blown Smart Card class Passive Stickers are also possible. In this case the price will be higher due to the increased capability.
- **Active Stickers:** “Active” Stickers are connected to the Handset Application execution environment, for example, via a Bluetooth connection. Hence, they are eligible for approximately 70% of all mobile phones.<sup>36</sup> Active Stickers enable all the usual NFC use cases such as card emulation, reader mode and Peer-to-Peer / Person-to-Person interaction.

<sup>35</sup> Note: It can be noted that at the moment simultaneous use of multiple SEs are not supported by the standards. However, there is work ongoing to reach this common target for example in Global Platform and on other standardization forums. See Global Platform (2009a) and Global Platform (2009b)

<sup>36</sup> Note: The average of 70% might vary according to the installed base in the respective geographical region, being closer to 90% in the industrialized world while being closer to 50% in the emerging markets. In general, Active Stickers can be expected to fit well in the high- to mid-tier markets.

OTA provisioning and life cycle management by a TSM is possible for Active Stickers because of their connection to the phone. The end customer may also manage his / her MFS Applications via the phone's user interface.

Active Sticker solutions will be ready for limited trials in Q1 2010. Mass production is expected from Q2 2010. Active Stickers are more expensive than passive ones. Depending on the capabilities of the selected chip in the Active Sticker, price points will vary between rather low cost solutions and more sophisticated product concepts.

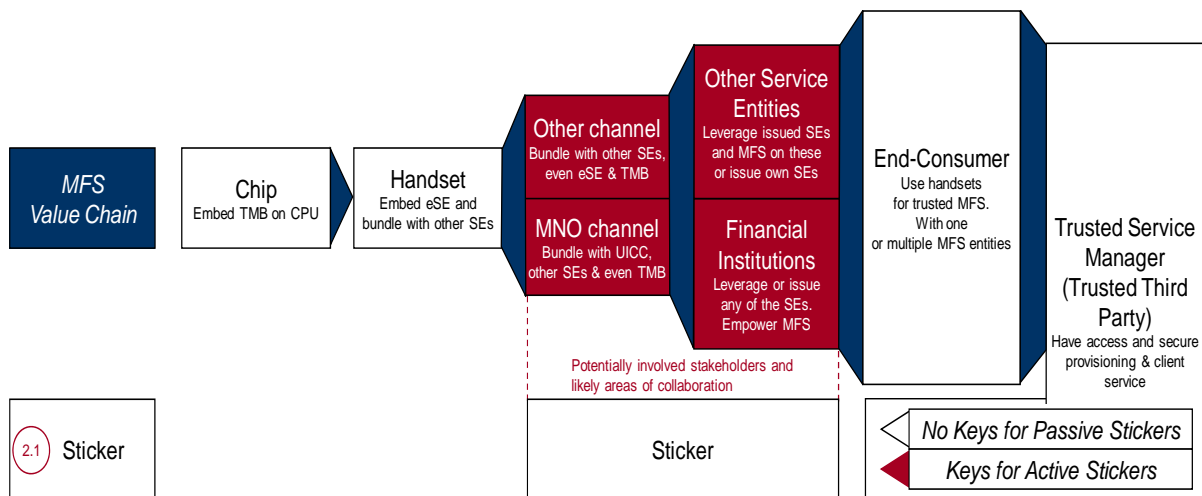
### 2.1.2. Business model scenarios

Stickers are offering interesting opportunities for SP-centric models, especially for players who are already engaged in Smart Card programs, for example, payment, loyalty and transport entities. With a reasonable price point, a limited impact on existing processes and without any technical or consumer adoption risks, SPs could easily complement and enhance their existing Smart Card programs by bundling them with Stickers.

The main objective of contactless payment is convenience and addressing small ticket purchases and cash displacement. In this context, Passive Stickers are an interesting companion for either legacy contact payment cards or contactless cards. They offer:

- Compliance with the full Handset installed base.
- Convenience of using mobile Handsets as a “cool & easy” way for small payments.
- A way of educating consumers towards more complex MFS: The End Consumers will get used to the “waving” gesture and the usage of their mobile device for payment purposes.

In brief, Stickers offer a potential first step for a SP to go mobile, with a limited investment and impact on current processes. However, due to limited capabilities in multi-application offering Stickers may be limited to intermediary offering, depending on consumer adoption and usage preferences.



**Figure 6: Stickers in the context of the MFS Value Chain and the Stakeholders**

Overall, Passive and Active Stickers provide Financial Institutions, Other Service Entities as well as Mobile Network Operators and Other Mobile Distribution Channels with an interesting SE alternative to quickly offer and promote MFS to the End Consumers.<sup>37</sup>

### 2.1.3. Technical enablers and inhibitors

#### **For Passive Stickers:**

In the payment segment, Passive Stickers are so far limited to contactless magstripe Applications and do not support contactless EMV Applications.<sup>38</sup> They could, however, be promoted in EMV countries as a “daughter card” (i.e. a card addressing the same user account as a primary card) of a legacy payment card or contactless EMV card. As such, they would be bundled with EMV cards.

#### **For Active Stickers:**

At present, Active Stickers face some usage disruption: During the installation phase, the Sticker needs to be paired with the Bluetooth module of the Handset. During day to day usage, the Sticker needs to be recharged, as it uses a dedicated battery. The End Consumer needs to be comfortable with these two processes of pairing and charging. The next generation of Stickers, however, is expected to make the user experience more convenient and similar to that of NFC native phones.<sup>39</sup>

The price points of Active Stickers seem to require a sound Return on Investment and a clear Application case for mass deployment. As soon as usability improves and prices become even more attractive, usage of Active Stickers can be expected to move beyond the present professional Applications such as healthcare, governmental services or business processes.

### 2.1.4. Opportunities and challenges

#### **The Service Providers’ fulfillment processes remain unchanged:**

The fulfillment and provisioning model of Sticker Applications is rather undisruptive, with a low impact on the SP’s existing processes: Passive Stickers are offered by traditional Smart Card Vendors to SPs and leverage the existing personalization and logistics processes.

#### **Making the most out of the contactless promise: Innovation & education:**

There is an evident trend around Stickers from SPs. Stickers are used as standalone contactless cards or are bundled with contact-based or contactless primary cards. The solution’s convenience serves SPs in customer attraction and retention. Also, there might be an achievable “coolness” factor in the design of the stickers (e.g.

<sup>37</sup> Note: The summarizing sentences for each SE section reflect the opinion of the contributing parties of this paper, as a discussion result at the time of writing.

<sup>38</sup> Note: Magstripe relates mainly to U.S.-based service offerings and sets a more limited extent of security requirements than EMV. EMV, for example, requires online resetting of the counters on the SE after a dedicated number of transactions which is not feasible with Passive Stickers. Hence, Passive Stickers are not applicable for e.g. contactless EMV Applications. Under certain circumstances of individual project / solutions, however, magstripe Applications can also be sold in the European Union.

<sup>39</sup> Note: For example, pairing an Active Sticker with the device is expected to be as easy as simply accepting a pairing request by pushing the ‘yes’-button.

haptic and visual effects, etc<sup>40</sup>) which could also add additional branding opportunities for the SP. Up to now, all marketing studies regarding the Sticker trials have shown an adoption and satisfaction rate in the range of 90%.<sup>41</sup>

### **Further opportunities:**

For existing Smart Card-based services with an online-backend (e.g. contactless magnetic stripe payments, ID-Applications or loyalty programs), Passive Stickers could be used as interaction module at the Point-of-Sale while a mobile Application then relates to the backend (i.e. over-the-air) and enables the user to manage the Sticker-related account and get additional information such as payment logs, account balances or redeem loyalty points or coupons triggered when paying with the Passive Sticker. The dynamic and interactive combination of Passive Sticker technology and web-based services could provide great marketing opportunities for SPs and compensate the lack of connectivity between the Passive Sticker and the mobile device.

### **Challenges:**

The main challenges with Passive Stickers are the missing LCM capabilities and multi-application support. It is hard to imagine that there would be applications from several AIs on the same Passive Sticker issued by one AI. Furthermore, this may lead to a market situation where consumers might have several Stickers on their mobile phone. Stickers may also wear off after certain time period and are not really changeable from one device to the next one. However, consumer behavior is often surprising, and they may be perfectly happy to start the mobile payment experience with Stickers.

## **2.2. Secure Micro SD Card (Secure $\mu$ SD)**

### **2.2.1. Concept description**

Mobile users are generally familiar with SD Cards in mobile phones. 40% of all mobile device holders are active SD Card users. In 2009, 90% of all shipped Handsets that included memory cards used SD Cards slots, increasingly being slots for Micro SD cards.<sup>42</sup> Since 2000, 2,5 billion cards of the globally interoperable SD memory card standard have been shipped<sup>43</sup>, making it the “the world-leading de facto interface of removable media.”<sup>44</sup>

With a low impact on the Bill of Materials of the Handset Vendor, diffusion of SD card slots has increased from 30-40% in 2006 to approx. 50% at present.<sup>45</sup> Through the use of adaptors, even mobile devices with regular SD Card slots can today use MiniSD and MicroSD cards, the latter becoming the dominant form factor. In 2009, over 60% of all mobile devices shipped included a Micro SD Card slot. It can be expected that in 2011 60% of the installed mobile device base will hold a Micro SD

<sup>40</sup> Note: The fashionable design of the stickers is expected to be particularly important in Asia.

<sup>41</sup> Note: This figure is a common industry opinion at the time of writing. For up-to-date figures, refer to industry bodies, e.g. [www.gsmworld.com](http://www.gsmworld.com), or market intelligence providers.

<sup>42</sup> Note: See iSuppli (2009): Also, in 2007 this figure was still at 57%. Until 2012, this figure is expected to continue at 92%.

<sup>43</sup> Note: See SD Association (2010)

<sup>44</sup> Note: SD Association (2010), p.1; Basic form factors of SD memory cards include SD, miniSD and microSD. All form factors share the same interoperability and plug-and-play convenience.

<sup>45</sup> Note: Electronic storage (2006): “For the Handset maker it’s just \$0.5 to have the slot and they don’t have to fit the card.[...] Four years ago no phones had slots; now it’s 30-40%”, p.53

Card slot.<sup>46</sup> With these trends towards microSD™ slots, Micro SD Cards with an embedded chip that serves as Secure Element are a potential way to extend the security level and service offerings on mobile devices.

For the use in MFS, Micro SD Card with Secure Elements are particularly applicable (i.e. the so called Secure Micro SD Card or “Sec. μSD”). This card connects to the mobile device through the Micro SD Card slot.<sup>47</sup> Secure SD Cards allow the distribution of MFS to a wide End Consumer base. SEIs and AIs can address the End Consumers directly with these cards, e.g. to promote the uptake of NFC payments.

Secure Micro SD Cards can even be issued for extended usage across the End Consumer’s electronic devices such as laptops, portable media players or navigation devices<sup>48</sup>. Leading edge Secure SD cards with their integrated SE can be expected to be compliant to GlobalPlatform standards and are able to host a number of different Applications. Also, they will offer a Secure Domain for the AI and other separate Secure Domains.

Hence, a Secure Micro SD card can, for example, host the following Applications:

- EMV profiles and other payment Applications.
- ID Applications such as financial IDs and access to Virtual Private Networks
- Loyalty and bonus programs in the area of ticketing and customer relationship management.
- Security Applications and Privacy Protection for social media services such as private and professional communities and networks.

The Secure Micro SD Card can be a mere storage provider and SE holder. Also, and this is particularly interesting for NFC-based MFS, the Secure Micro SD Card can include an NFC antenna. Hence, there are three possible models of Secure Micro SD Cards:

1. **“Full NFC”**: The Card includes the secure storage, Security Domain, NFC chip and the antenna.<sup>49</sup>
2. **“Antenna on the mobile”**: The Card includes the secure storage, Security Domain and NFC chip, but the antenna is on the mobile device.<sup>50</sup>
3. **“Only SE”**: The Card includes the secure storage and Security Domain. The NFC modem and the antenna are on the mobile device.

All three conceptual alternatives allow decoupling the SE and its embedded Applications from the “NFC” phone. There are several business model-related interests for doing so:

<sup>46</sup> Note: Estimation based on 800.000 mobile devices with Micro SD Card slot shipped in 2009 while the total mobile device shipments were 1.270.000.000, i.e. 63% of shipment in 2009 include Micro SD Card slots. Given an exchange time of 2 years for mobile devices in subsidized markets, the present market share of Micro SD Card slots in mobile devices of 40%-50% can be expected to increase to approx. 60% in 2011 in these markets.

<sup>47</sup> Note: For the usage with NFC phones, the mobile devices need to support the Micro SD with an additional specific connector and interface in the Micro SD slot. This interface has not been standardized yet. However, such phones have been prototyped in Asia since 2008.

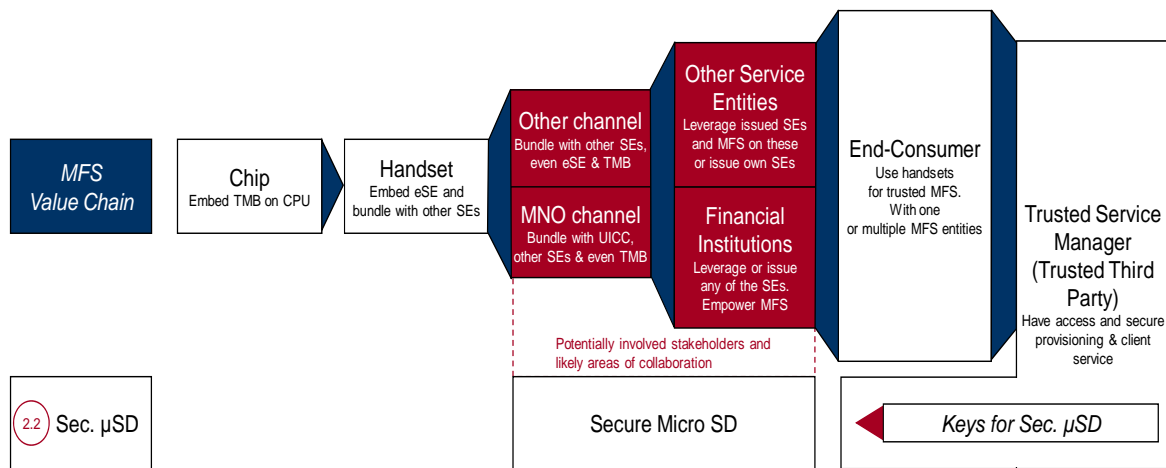
<sup>48</sup> Note: This is possible with a passive standard SD adapter.

<sup>49</sup> Note: In this concept, the NFC only works when the phone is switched on.

<sup>50</sup> Note: In this concept, the NFC also works when the phone is switched off.

- The MNO can offer a flexible means to distribute NFC Applications independently from his UICC channel which is more complex regarding provisioning and fulfillment processes. In addition, the SD Card could be monetized via a sound after market with significant gross margins.
- The Financial Institutions and / or Other Service Entities can distribute NFC Applications independently of the MNOs, use standard retail channels (e.g. large consumer retail chains) and re-use its provisioning and fulfillment processes for payment cards and loyalty card to directly market SD cards to its customer base.

In the context of the MFS Value Chain, this puts the Secure Micro SD Card into the following position:



**Figure 7: Secure Micro SD in the context of the MFS Value Chain and the Stakeholders**

In brief, the Secure Micro SD Card is therefore an interesting SE alternative for Financial Institutions, Other Service Entities, Mobile Network Operators and Other Mobile Distribution Channels to offer and promote MFS to the End Consumers.<sup>51</sup>

### 2.2.2. Business model scenarios<sup>52</sup>

#### Issuance, provisioning and distribution of the SD:

There are three models for the issuance, provisioning and distribution of the SD:<sup>53</sup>

- The FI provides the SD.
- A retailer provides a Blank SD to the End Consumers.
- The SD card is bundled to the sale of the mobile device.<sup>54</sup>

<sup>51</sup> Note: The summarizing sentences for each SE section reflect the opinion of the contributing parties of this paper, as a discussion result at the time of writing.

<sup>52</sup> Note: These scenarios reflect the current major trends in the NFC ecosystem and do not intend to be final. They do not address the different possibilities of bundling Memory with SE.

<sup>53</sup> Note: In any of these potential business scenarios, the Financial Institution or the Other Service Provider needs to have a link to the SD Issuer to provide the necessary key as the "Root of Trust".

<sup>54</sup> Note: These bundles can be done by the MNO, the phone Vendor or the retailer. For example, a bank could contact a local phone distributor, jointly discuss the market size and marketing and the bundle needs (incl. the SD and even its packaging). This distributor repackages the phones towards the bank's needs, sell them through its channels and combine with a bank issued SD (e.g., credit card-ready corporate phones for travelling professionals).

### Card issuance model for a FI's<sup>55</sup> SD:

The Micro SD is personalized and distributed to the End Consumers as in the current Card issuance process of FIs. However, FIs have to find a way to assess the eligibility of their customers for such a Secure Micro SD (ie assess they have the right kind of phones). After the eligibility and enrolment process, the SE lifecycle is optionally managed by the TSM of the FI with the same GlobalPlatform mechanisms used for managing for instance eSEs or UICCs.

- **Enrolment:** The FI pitches the service to its End Consumers and checks their phone eligibility to the service. The Secure Micro SD Card is then provisioned in the same manner as a regular Smart Card. A TSM could be used for the LCM of the Secure Micro SD Cards.
- **Business model:** The FI designs its own business model around the Card as it is part of its price policy. End Consumers are used to pay a premium for Secure SD Cards and the after market of SD Card is usually getting significant margins.<sup>56</sup>
- **Distribution:** The FIs distribute the Secure Micro SD through their regular channels (i.e. via Branches, on-line Banking or Direct Mailing). Also, the FIs could enter new distribution channels, e.g. via direct retail as presently done with prepaid Stickers in the United States. Opening an additional distribution channel could be of particular interest to the FI as it could directly present its Brand to End Consumers, even beyond the installed base of its clients. Subsequently, the End Consumer could discover the various additional service offerings of the FI through marketing around the Card.
- **Open questions:** Due to the requirement for an SD Card slot in the mobile device, not all End Customers' phones might be eligible for a Secure Micro SD card. Further, the Cards need to pass a specific personalization process and the FI's (or its Card Issuance partner's) machinery might need to be adapted to issuing Secure Micro SD Cards. Once the FI has established a footprint as provider of its own Secure Micro SD Cards, it can decide whether or not to invite other parties to provide Applications into that Card to open an additional sphere, complementary to other SEs, for additional services in the phone.

From an End Consumer perspective, the challenge might occur that the end user will have to manage multiple Secure Micro SD cards if his FI does not want to open the Card to other Application Issuers, but the End Consumer still wants to interact with more than one FI or wants to use other SD Card-based Applications that are not on his FI SD. However, assuming there is multi-SE architecture, for the second FI there would be several options: to partner with the SD issuer, or to partner with the MNO, or to utilize the Stickers or TMB.

### MNO model for a blank SD

In the current UICC-centric model, MNOs are controlling MFS such as NFC Applications via the UICC and their OTA management process. SD-based solutions could complement this position. MNOs may see a more flexible and economical means of distributing NFC Applications in Secure Micro SD Cards. Also, the End Consumer may be willing to pay for a Secure Micro SD Card - providing the MNO

<sup>55</sup> Note: The "Card issuance model for a FI's SD" can be applicable for numerous FIs – At the time of writing, however, it is expected to be mainly in the interest of Banks.

<sup>56</sup> Note: Once Secure Micro SD cards include secure applications for MFS, this might negatively affect the readiness to renew SD cards and hence be a drawback for the volumes of SD cards being put-through by SD retailers.

with a significant margin. Further, the MNO could offer additional services without jeopardizing his installed base of UICCs.

In addition, a MNO-branded SD card would drive competition in the SD-based payment sphere, because MNOs could offer Secure Micro SD Cards as independent service modules, even to End Consumers that are linked to a different MNO. Furthermore, MNOs could sell NFC services to customers who do not have NFC compatible devices yet – even across the corporate boundaries. Then, service quality for NFC payments would become the differentiating factor between different MNOs.

- **Enrolment:** The post issuance enrolment process in this scenario equals the Card issuance model.
- **Business model:** The consumer pays for the Secure Micro SD Card and possibly for the services provided onto this SD card. More specifically, some SD-based secure services could be free of charge and others might be service-fee based.
- **Distribution:** The MNO could distribute the Secure Micro SD Card via his established distribution channels.
- **Open questions:** For the MNO, this model offers more flexible ways of integrating Mobile Financial Services into his service offerings. The SD Card does not bear the legacy of the existing telecommunication infrastructure.<sup>57</sup> Essentially, MNOs will have to take long-term decisions whether they want to become Financial Service Providers or not. If so, the Secure Micro SD Card can be a valid first step into this direction.

### Retail model for a blank SD

In this scenario, blank Secure Micro SD Cards or FI-branded Secure Micro SD Cards would be distributed off-the-shelves by regular Business-to-Consumer retailers or through Business-to-Business channels. The distribution of such Cards could be issued by:

- The Handset Vendor.
- The MNO.
- The Retailer / Distributor (possibly with its own payment card).
- A Payment Association (e.g., a credit card company product).
- A Financial Institution.
- The SD card Vendor (e.g. alone or in alliance with a credential provider).
- A TSM.

This model would be multi-Application by definition. However, the “Root of Trust” that has been provided by the FI in the Card Issuance Model would here have to be provided by a neutral third party such as, for example, a TSM<sup>58</sup>, a credit card company or the Secure SD Card Vendor.

For the End Consumer, this could result in a seamless experience as long as the industry or a specifically designed venture manages to implement the business logics and arrangements behind this service offering before going to the market with a Blank SE solution.

<sup>57</sup> Note: The UICC has to accommodate proprietary memory needs of the MNO. This is not needed in the SD.

<sup>58</sup> Note: This TSM could potentially be owned by a bank or even a MNO. If there is only one bank as the retail provider, the model resembles the one mentioned in section on “card issuance model for a Bank’s SD”.

The packaging of such a Secure Micro SD Card solution would need to clearly mention which Third Party supports this service and can be trusted by the End Consumer. The SE would be blank (i.e. un-personalized) and would be linked to a TSM from scratch when being initialized OTA. Such a Blank Secure Micro SD could also be sold via existing distribution schemes as a bundle with the phones (e.g. via Handset Vendor, retailer or MNO).

- **Enrolment:** The post issuance enrolment process in this scenario equals to one of the card issuance model. To the end-consumer, it does not make a difference. See chapter 1.3 further detail.
- **Business model:** The End Consumer pays for the SD and possibly for the services provided onto it. More specifically, some services can be free of charge and others might be service-fee based.
- **Distribution:** Regular retail channels (e.g. Metro, Carrefour, Carphone Warehouse etc). Here, the respective SD card Issuer can present its own brand to the End Consumer as well as the brands of the services that may be accessible through the SE. The End Consumer can discover the various service offerings through any of the SPs, the SD card provider or additional retailers.
- **Open questions:** For the End Consumer, this might offer a wider set of service offerings rather than any proprietary model such as the FI- or MNO-issuance of Secure Micro SD Cards. However, there could be confidence issues from the End Consumer perspective towards the Issuer of such a Blank SD card. From the industry's perspective, providing a consistent root of trust and aggregating the different services on the blank SD will be a crucial challenge.

### 2.2.3. Technical enablers and inhibitors

Technically, there are the above introduced three conceptual alternatives of Secure Micro SD Cards (see 2.2.1): "Full NFC", "Antenna on the mobile" and "Only SE". Looking at these three alternatives, "Full NFC" may be a good bridge technology which enables rapid diffusion of NFC services because there is no need for an installed base of NFC capability in the mobile phones. Placement of the SD card in the phone may affect the NFC functionality. This is a design issue which the phone manufacturers should take in account when designing the phones.<sup>59</sup>

The other technologies have specific requirements towards the mobile device. For such requirements towards the mobile device itself, there are no implementations and standards yet which can be expected to cause an additional time lag until market uptake. In terms of driving the discussion of MFS technologies, "Full NFC" would be the quickest path towards implementation, even if industry wide standards might currently be missing.<sup>60</sup>

In order to develop the market it would be optimal to have a standardized way to access the Secure Micro SD cards used as SEs in mobile phones. So far there

<sup>59</sup> Note: if viewed very critically, the fact that the NFC antenna is positioned on the SD card might initially present a usability challenge, depending on the location of the SD card within the phone (e.g. below the battery or behind metal). For example, the SD card might need to be held against the respective terminal in a certain angle.

<sup>60</sup> Note: When heading towards implementation, it is recommended to check with the respective Handset Vendors whether the chosen SD solution is compatible with the favored devices. For example, first Secure Micro SD Solutions seamlessly interface with Blackberry and Android phones.

hasn't been a market force driving for standardization of Secure Micro SD card interfaces on the same level than with some other SE alternatives.

## 2.2.4. Opportunities and challenges

### Memory capacity of the SD

SD memory is flash memory which is a highly flexible technology. The memory density is following Moore's Law and as such doubling approximately every 12 months. The average memory point was 2 GB in 2008, 4 GB in 2009 and likely to be around 8GB in 2010. Increasingly, the End Consumer will need and appreciate this space for data storage, e.g. for music, documents or other content. It is known that 60% of SD card users are not leveraging their SD-based storage, 40% are.<sup>61</sup> This opens two paths for SD-based solutions:

- Memory does not matter.
- Memory can be used as additional value proposition. For the SD supplying party – be it a FI, MNO or others - this opens additional channels for consumer interaction through which storage upgrades can be nurtured. Additionally, this can offer a business opportunity to store and provide the SD-based credentials to the End Consumer on a repetitive basis.

### Two SD market segments and storage capacity trade off

The End Consumer market for NFC-enabled, SD-based SEs is expected to be two-fold:

- End Consumers who do not care about the storage capacity and value the NFC payment Application alone.
- End Consumers who are technology-affine and will want SD-based NFC functionality, but will also want highest possible storage capacity.

Tailoring the marketing activities to these two markets segments will be the responsibility of the SD-providing parties. Ideally, it will be the latest generations of Secure Micro SD cards that will be including NFC / payment functionalities as described above. If the SD-providing party decides to get involved with the topic of SD-based storage, it will need to analyze more thoroughly how much storage is needed for which market segment and at which additional this can be sold.

### Removability and multiple cards

Given that the Secure Micro SD cards see a successful market uptake, End Consumers might end up holding numerous  $\mu$ SDs from different issuers. Because the  $\mu$ SD is removable, this could empower the flexible usage of different MFS, provided by different issuers (e.g. just as with multiple payment and credit cards today). Nevertheless, convenience in using multiple  $\mu$ SDs will be an issue as long as Mobile Devices have only one SD slot. Here, further standardization and 'plug-and-play' functionalities could provide additional benefit. Alternatively, the market will drive for the Service Providers to share the Secure SD card space or other SE's available in the phone.

<sup>61</sup> Note: This figure is a common industry opinion at the time of writing. For up-to-date figures, refer to industry bodies, e.g. [www.gsmworld.com](http://www.gsmworld.com), or market intelligence providers.

## 2.3. Universal Integrated Circuit Card (UICC)

### 2.3.1. Concept description

In 2<sup>nd</sup> generation mobile Networks (2G), the SIM is the physical Smart Card used to control access of mobile devices to the MNO network. In 3<sup>rd</sup> generation networks (3G), this physical component is called UICC. UICCs can contain SIM, USIM and/or CSIM Applications. UICCs use Java-based Operating Systems. However, the clear majority of installed base on the market is still using SIMs instead of UICCs. Especially, SWP-compliant UICCs are still in the phase of market introduction.<sup>62</sup>

Increasingly, UICCs can include additional Applications such as information-on-demand menus, SIM-based browsers, m-banking Applications, EMV profile Applications or ID credentials for MFS.<sup>63</sup> Hence, they serve as SEs for MFS just as the other SEs described in the above and below chapters.

### 2.3.2. Business model scenarios

Normally, the MNO dominates the issuance and the access to the UICC because it is a key part of his mobile network management. Also, the UICC contains software for secure network access and the MNO's core business processes. Hence, the MNO normally plays a crucial role when UICCs are issued and shall also serve as SEs for MFS. Therefore, UICC-based SE business models are most likely alliance models between the MNO as SE Issuer and an Application Issuer (for example a Financial Institution or Other Service Entity) to "share" the UICC. Financial Institutions are only likely to become SE Issuers for UICCs if they act as a Mobile Virtual Network Operator (MVNO) and thus also control the UICC. For collaboration agreements between MNOs and Financial Institutions, three Business Model Scenarios can be distilled:<sup>64</sup>

- **The so called "Rental Model":** The UICC is owned by the MNO. Partitions of the UICC are rented out, e.g. to Financial Institutions as App Issuers. The MNO may have risk sharing agreements with a Financial Institution via long term contracts or even shared investments into this infrastructure. The main business control over the UICC, however, is in the hands of the MNO. This model is favored by many MNOs.
- **The so called "Hotel Model":** The UICC is fully owned and managed by the MNO. Contract durations can be shorter than in the "Rental Model". The MNO covers capital expenditures as well as operating expenses. Financial Institutions rent partitions of the UICC short term as "guest".
- **The so called "Ownership Model":** The UICC is co-owned by the MNO and a Financial Institution. The concept allows independence to manage each UICC partition separately. Capital expenditures and operating expenses are shared

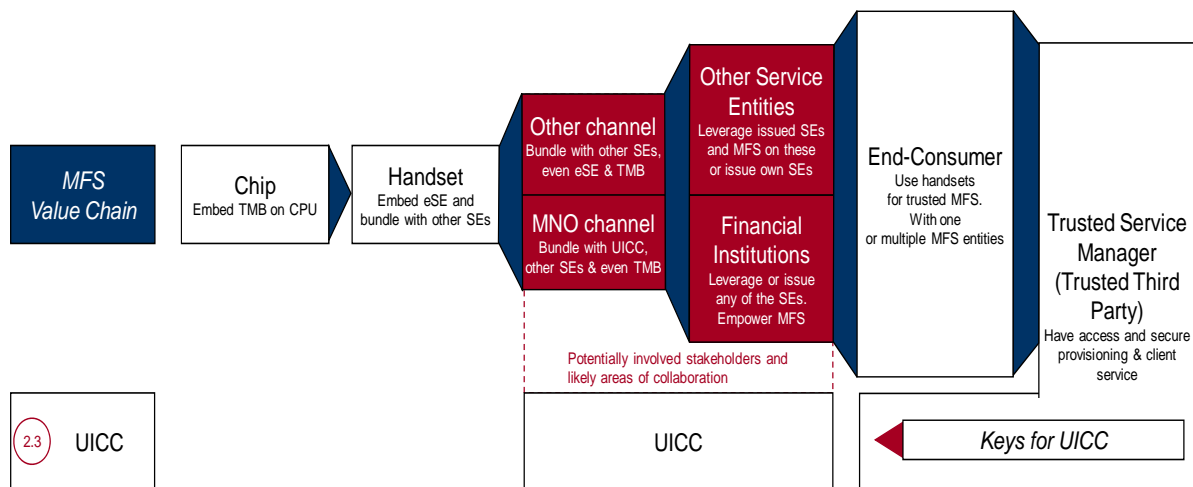
---

<sup>62</sup> See [www.gsmworld.com](http://www.gsmworld.com)

<sup>63</sup> Note: For an explanation of the migration from SIM to UICC, the capabilities of the UICC and the enrolment of a Bank on an UICC as shared SE, see Mobey Forum (2008), p.42ff, graph taken from Mobey Forum (2008), p. 44

<sup>64</sup> Note: For a detailed description of these conceptual models for the UICC as Shared SE, see Mobey Forum (2008), p.40ff and p. 50ff as well as Mobey Forum (2006), p.10ff. For a detailed description of the business models behind these concepts, see Mobey Forum (2008), p.60ff.

between the MNO and the Financial Institution. Each App Issuer is individually responsible for the maintenance his own MFS Application, based on agreed joint business principles. The distribution of the UICC may even take place through the FI.



**Figure 8: UICC in the context of the MFS Value Chain and the Stakeholders**

In addition to these three examples, more centralized Business Models have been discussed recently: The idea of the TSM has been expanded into the Trusted Transaction Manager (TTM) concept.<sup>65</sup> In this concept, the TTM holds B2B relationships with all MNOs and acts as Application Issuer by sharing, renting or owning space on each MNO UICC. The TTM offers similar Applications to each MNO. To the Financial Institutions, the TTM can act as single interface, assisting them in offering “secure transactions as a service” on all UICCs of the different MNOs. The TTM concept addresses the issues of coverage, esp. the fact that customers of one Financial Institution might use different MNOs / UICCs and actively deals with the challenge of market complexity because of the fragmentation in MFS technologies and service propositions.

Alternatively, an MNO could also decide to act as a TTM for different FIs / Banks and serve all his End Consumers with “secure interactions as a service” for different Financial Institutions. All of the above mentioned business models depend largely on the implementation of the key provisioning process via the MNO or other entities.<sup>66</sup>

In brief, the UICC is an interesting SE alternative, especially for MNOs and, if the MNOs decide to leverage this strong existing position in the MFS Value Chain, can potentially become an interesting service path for Financial Institutions and Other Service Entities as well in order to offer and promote MFS to the End Consumers.

<sup>65</sup> Note: The TTM is a business model based on managing relationships between the different stakeholders in the Ecosystem. The TSM in comparison is one Stakeholder in the Value Chain.

<sup>66</sup> Note: For a detailed description of the key provisioning alternatives, see Mobey Forum (2008), p. 48ff. In brief: Normally, OTA keys are used by MNO to protect SIM. However, sell-sub keys can be sold to AIs, such as Financial Institutions to enable them to manage their own MFS Applications. Alternatively, key distribution can also be handled by the UICC Vendor. In this case, the MNO does not see any OTA sub keys at all. By using an OTA sub-key sharing mechanism and pre-loading Applications, all of the above indicated business models can be implemented without introducing new technology.

### 2.3.3. Technical enablers and inhibitors

The UICC may have separate Security Domains for each Application, administered by the Application Issuer and based on the use of secret administrative keys. The Card's Operating System usually implements a firewall that established secure partitions on the UICC and prevents the different Applications from accessing, sharing or corrupting data between them. Today, UICCs are technically capable to create Secure Domains and Secure Sub Domains. TSMs have the technology to manage UICC memory space and create Secure Domains. Applications can be pre-loaded to UICCs or can be provided OTA. Applications can be taken to Secure Domains over Bearer Independent Protocol (BIPs, e.g. SMS). Thus, all technical components are available to enable secure Applications in UICCs for remote<sup>67</sup> MFSs.<sup>68</sup>

As SEs for MFSs, UICCs have the advantage of being able to use the so called SIM Toolkit mechanism. This mechanism can communicate with screen of the mobile device and receive information from the keypad of phone. Hence, End Consumers can communicate with the Application in the Secure Element without the requirement of adding new software to the phone itself.<sup>69</sup> However, a challenge remains: Visually, the SIM Toolkit's appearance is limited and branding options are based on text only. In the future, however, Smart Card Web Servers will offer a richer environment for End Consumer communication via the UICC.

### 2.3.4. Opportunities and challenges

In terms of implementation of MFS on MNO-controlled UICCs, there is a clear challenge in how a single MNO can cover a single Financial Institute's customer base, especially if their markets don't totally overlap. Here, the standardization of SE interfaces would enable all MNOs to offer similar services based on the widely distributed UICC SEs, even to various FIs and across national boundaries.

On a more conceptual level, however, the role of the UICC as potential SE for MFS will largely depend on the strategic orientation of MNOs in the future and the question whether they will want to leverage their dominance of the UICC by opening it to other AIs and their services, particularly in the field of MFS. Especially the agreement on the business model and compensation levels is crucial here. Currently, the market situation shows that UICCs may technically work, but the business model agreement between MNOs and FIs seems to be difficult to achieve.<sup>70</sup>

---

<sup>67</sup> Note: In the NFC context (i.e. proximity payments), however, the lack of Single Wire Protocol (SWP), which empowers the communication between UICC Apps and the NFC radio remains a challenge.

<sup>68</sup> Note: For more detail on the enrolment of Bank Applications on UICCs, especially via SMS, see Mobey Forum (2008), p. 45f.

<sup>69</sup> Note: According to the GSM specifications all phones manufactured after 1991 should support SIM Toolkit. However, few (2-3% of tested phones) deviations have been encountered in tests mainly amongst some newest smart phones. For more information, please refer to leading mobile operators' support sites.

<sup>70</sup> Note: Without favouring that agreements in this regard need to be made, the authors expect that existence of such agreements would additionally assist the market take-off of MFS as a whole.

## 2.4. Embedded Secure Element (eSE)

### 2.4.1. Concept description

Today, embedded Secure Elements (eSEs) are shipped in NFC-enabled phones as well as non-NFC devices. They have a good level of technical maturity and have been tested since 2004. The concept of eSEs is very close to the UICC SE model as it requires a TSM and leverages the same core provisioning technology. The integration of SEs in NFC phones has also been greatly simplified by technology vendors with a limited or no impact at all on the phone design in terms of hard- and software.

eSEs add a small premium to the Bill of Material (BOM) of the Handsets, depending on the technical capabilities of the eSE and whether they are purely payment focused or offer a greater multi-Application support. For some offerings, non-EMV based mobile proximity payment on focused eSEs could be made pervasive with a very low price point. For this, however, there is agreement needed between interested AI, the Handset Manufacturer, the MNO or Other Phone Distribution Channels.

### 2.4.2. Business model scenarios<sup>71</sup>

The usual Stakeholders are expected to be involved in eSE business model scenarios: A SP (e.g. a Bank or other Financial Institution in the case of the below elaborate examples), a TSM<sup>72</sup> and a Handset Vendor. Of course, innovative plays could be tempted by adding Retailers or MNOs in those schemes.

Also, these scenarios would assume that the Handsets have successfully passed the proper certification processes from the Payment Scheme to be allowed to support MFS such as mobile proximity payment Applications.<sup>73</sup> This is done by the Handset Providers for the single Handset models or chipsets. The SP can work with the resulting certified Handsets.

#### FI-centric model (“Decoupled Debit” model)

A Financial Institution strikes a deal with a Handset Vendor for a given geography and / or a given market segment. For example, a Credit Card corporation or the corporate arm of a Bank joins forces with a Handset Vendor to deliver SE-based MFS on smart phones for executive clients.

- **Enrolment:** Here, the required personalization details can be pre-personalized into the phone by the Handset Vendor. The actual enrolment process of the individual End Consumer is then executed and managed by the Financial Institution’s or Handset Vendor’s TSM.
- **Business model:** The SP compensates the Handset Vendor for the cost of the eSE, if this is requested by the Handset Vendor. Additionally, a FI that joins forces with a Handset Vendor could subsequently open the SE to other Financial Institutions (Application Issuers) on a rental basis. Hence, the FI that issues the SE

<sup>71</sup> Note: These scenarios reflect the main current trends in the NFC ecosystem and do not intend to be final.

<sup>72</sup> Note: This TSM could be independent, owned by the Service Provider or the Handset Vendor, or a joint venture of multiple players.

<sup>73</sup> Note: As done today for WiFi and Bluetooth technologies, for example.

could even become a host for financial services provided by its competitors to the open SE and receive a compensation for enabling MFS to the wider group of FIs.

- **Distribution:** The Handset Vendor uses his regular channels or the Financial Institution enters agreements with MNOs or other phone distribution channels to promote these devices in the market.
- **Issues:** Unless the NFC payment feature is attractive enough to push consumer to changing between Financial Institutions, this model would work best for specific payment services which are decoupled from the Debit Account of the user (e.g., prepaid Cards, Credit Cards, retailer payment Cards, decoupled Debit Cards, etc.).<sup>74</sup>

### TSM-centric model

All phones distributed by a Handset Vendor in a given geography are linked to a given TSM via a pre-personalization process (possibly controlled by a Financial Institution or an association of Financial Institutions). The TSM ensures the link with all the Financial Institutions that support and offer the mobile device-based payment service.

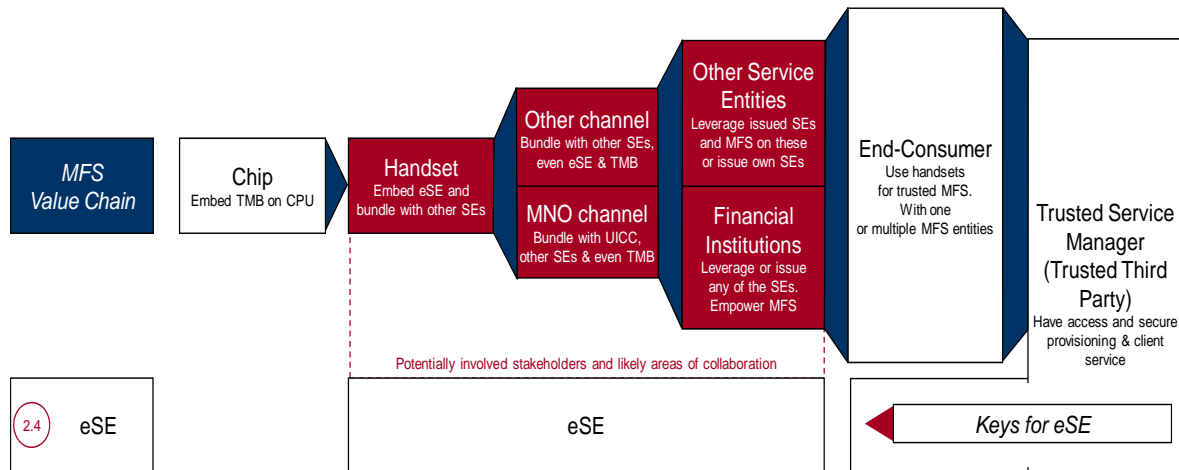
- **Enrolment:** All the enrolment details are pre-personalized in the phone by the Handset Vendor. The enrolment process is routed by the TSM which links to the Financial Institutions.
- **Business model:** The TSM compensates the Handset Vendor for the cost of the SE and collects the money back from the MFS Application Issuers.
- **Distribution:** The Handset Vendor uses its regular channels or the TSM closes deals with MNOs or Other Distribution Channels.
- **Issues:** The TSM architecture will have to be transparent, open and accessible for all market players to prevent the TSM being a control point. One way of reaching this is that the TSM is an association of the local Financial Institutions or SPs.

### Handset-centric model (“White Handset”)

The Handsets are sold with a “white” (i.e. non-personalized) eSE.

- **Enrolment:** The End Consumer activates the payment service by accessing a (mobile) web site whose URL is provided by the respective SP. The SP triggers the provisioning process via its TSM. The activated Security Domain in the SE is then “owned” by the SP.
- **Business model:** The Handset Vendor could get an activation fee from the SP who wishes to own the Security Domain in the SE.
- **Distribution:** The Handset Vendor uses the existing channels of distribution.
- **Issues:** The TSM architecture will have to be transparent, open and accessible for all market players. The ownership, liability and certification model needs to be clarified in cooperation with Handset Vendors and the SPs, e.g. the Financial Institutions.

<sup>74</sup> Note: Based on the available market information, the churn rate between banking services is approximately around 6% per year in Europe. For up-to-date figures, please refer to market intelligence bodies.



**Figure 9: eSE in the context of the MFS Value Chain and the Stakeholders**

In brief, the eSE particularly depends on the Handset Vendors embedding the SE and then, together with the subsequent Stakeholders in the Value Chain, finding collaborative business models which cover the initial costs of embedding the SE into the mobile devices and structure agreements on sharing the potential revenues from empowering these eSE with MFS Applications.

### 2.4.3. Technical enablers and inhibitors

#### Service Providers' Push

A significant number of SPs will have to require / mandate the eSE in the mobile devices to enforce its implementation in the first place. This could be done by associations like the Mobey Forum, EMVCo and Retailer Associations<sup>75</sup>.

#### Open SE models

The "blank-SE" model still offers a couple of challenges before being fully viable: the liability and eSE ownerships issues need to be clearly solved between Handset Vendors, TSMs and SPs. Furthermore, accessing the eSE and the provisioning of the User Interface would need to be based on clearly defined standards and more seamless for the SPs. The various industry forums could be appropriate entities to propose solutions and have the industry players develop a consensus.

### 2.4.4. Opportunities and challenges

At present, there are several on-going disruptions in the mobile industry which are expected to ease the adoption of eSEs:

- **Distribution:** Around 50% of Handsets are distributed independently of the MNOs worldwide. Of course, this fact hides different local realities: Mobile device sales revenues in Europe are split between operator and other channels (e.g. independent distribution). Operators amount for a total of approx. 47% of the total volume in 2009, says Richard Jesty of Informa Telecoms & Media, a leading industry

<sup>75</sup> Note: Like the National Retail Federation (NRF) in the U.S. in which the ARTS Subgroup drives the related standardization.

source for data on mobiles. In Middle East / Africa and Asia, 90%+ of the mobile devices are sold via independent channels and only a minority via the operator channels.<sup>76</sup> Some countries also strictly forbid bundled sales (i.e. Subscription + Handset). On top of that, some major retailers are engaged in payment services with their own payment Cards and have also launched mobile services through MVNO ventures.

- **Smart Phone Vendors:** There is undeniably an iPhone effect which is pushing Smart Phones and Handset Providers to propose their own services portfolio (i.e. own Application Stores and Multimedia Stores).
- **ODM Vendors:** So called “Original Design Manufacturers” are growing players that offer custom Handsets to consumer brands, Retailers or MNOs. Those ODMs are likely to be major players in offering eSE-enabled Handsets to SPs.
- **Focus on core business:** An increasing number of mobile device users are getting used to receiving their services from smaller players like Tier 3 MNOs or MVNOs.<sup>77</sup> Those players tend to focus on managing their customer relationship and maintaining their operational margins and will likely not release NFC services on their own. They are ready for partnerships and innovation with major Service Providers and will require turnkey services, avoiding liabilities issues.
- **Liabilities & dispute management:** The separation of SEs transfers liabilities to the SP or to the TSM, with a clear decoupling between the UICC and the SE. This will relieve smaller players (Tier 3 MNOs or MVNO) from a significant liability burden.
- **The SIM issue:** There is still a remaining challenge to get the UICC certified to a payment level while eSEs are an already certified Smart Card component from the payment segment. Isolating the payment function in a dedicated component will simplify the certification of the mobile device for payment purposes and wider MFS.
- **Easiness of eSE integration into mobile phones:** eSE enablers have successfully passed trials in the past 4 years: Handset Vendors have a significant experience in integrating eSEs, TSMs are ready and Payment Associations have defined certification processes for SE-enabled devices. eSEs are stacked on top of NFC chips, offering a pin to pin compatible integration on NFC phones and a seamless hardware integration into Handsets. Interfaces to TSMs and Phone Applications are based on standards and shared with the SIM-UICC. The same standards are eligible for both SIM and eSE: JSR 177 and 257 for eSE/SIM resources access, TSM interfaces with GlobalPlatform OTA standard management, convergence Java Card execution environment in both eSE and SIM.
- **Future Proof Investments:** The fact that both the SIM-UICC and eSEs are sharing the same set of standards makes the investments from SPs and TSM replicable for both technologies.

---

<sup>76</sup> Note: This figure is a common industry opinion at the time of writing, backed by studies such as Informa (2009). For up-to-date figures, especially for specific regions and market niches, refer to industry bodies, e.g. [www.gsmworld.com](http://www.gsmworld.com), or market intelligence providers.

<sup>77</sup> Note: A tier 1 MNO is a transit-free network that does not pay settlements to any other network to provide mobile connectivity. Tier 2 MNOs peer with some networks and buy network traffic slots from tier 1 MNOs. Tier 3 MNOs solely purchase network traffic slots from a selected tier 1 MNO.

## **2.5. Trusted Mobile Base (TMB)**

### **2.5.1. Concept description**

A Trusted Mobile Base (TMB) enables the full variety of SPs to create and protect additional business revenues from new consumer device services, based on an entirely open environment. TMBs are promising upcoming solutions which may help take the fragmentation out of the market of MFS through an integrative solution. TMBs may or may not become SEs later.

The “TMB SE” is designed into the Central Processing Unit (CPU) of the mobile devices. Being part of the CPU equals natural distribution to a wide consumer base. Being built into the CPU, the TMBs could, for example, come at no additional hardware costs and rather be based on service agreements with the respective TSM or SP. TMB-related services can be provided ad hoc OTA.

TMBs are not mutually exclusive to other SEs. Rather, they can serve as a complementary and integrating nucleus (i.e. “glue technology”) for services which depend on partial identities distributed across other SEs such as the Active Stickers, Secure Micro SD Cards, UICCs and eSE. TMBs combine these into integrated solutions, assuring seamless interaction and security of processes executed in the periphery of the respective SE.

Together with TMBs, other SEs can reach unprecedented levels of certified security whilst assuring convenient usage of integrated solutions to the End Consumer. For example, TMBs can enable Secure User Interfaces (UIs) and OTA credential provisioning to securely isolated Security Domains and the different Applications stored in every one of these.

A special capability of the TMB is that numerous SPs and TSMs can access a single TMB, each with their own Applications in their Security Domains. To do so, the respective party activates single sections within the TMB which then become their securely separated, proprietary domains and are filled with the Applications that shall be secured by the TMB. In such a set-up, TMBs can also be considered as additional SE alternative, especially if they achieve the appropriate level of security certification such as, for example, EMVCo’s requirements.

In essence, the TMB is being developed towards becoming a glue technology within the overall mobile device, in particular enhancing the security levels through:

- A Secure User Interface as additional service quality
- Leveraging partial identities stored on other SEs such as the SD or the UICC (e.g. the identity of an individual user on his SIM card is leveraged for authentication in a banking interaction for which the account number is stored in the TMB).

In brief, TMBs are open platforms with standardized interfaces towards the other SEs and the Application world. They provide the “glue” to connect Open OSs, security sensitive devices and other SEs such as Active Stickers, UICCs, Secure Micro SD Cards, eSEs and NFC frontend controllers with the backend infrastructure.

With the option of being pre-certified<sup>78</sup>, TMBs provide a sustainable security level across a broad range of mobile devices. The security level can even be enhanced according to the requirements of the respective Application and SP, e.g. to enable MFS such as Macro Payments, Stock Trading, DRM and related trustworthy Information Services. TMBs can be linked to the NFC interface in order to enable NFC payments and other NFC services as soon as the respective TMB-Application is activated.

## 2.5.2. Business model scenarios

The majority of (NFC-enabled) mobile phones will be provided with an Application Processor that includes a TMB as a built-in SE in the future. TMBs cause no fixed up-front costs for the TSMs or the SPs. Rather, TMB-based secure solutions may come via service-based agreements.

- **Distribution:** TMBs are built into the processors of mobile devices and are therefore “naturally distributed”. SE Issuers or TSMs delegated by them can activate these TMBs directly and ad hoc OTA.
- **Competition:** The TMB is accessible for TSMs and SPs. Thus, it opens up for different applications and further diffusion MFS.
- **Choice and customization:** The respective TSM or SP can fully customize his Application in his proprietary module of the TMB, define the necessary security level (even beyond the pre-certification if needed) and provide it to the mobile device OTA.
- **Motivation to the market:** The TMB is a new, standardized, secure, pre-certified / or fully certified and modularized SE for the quick provisioning of mobile payment services, based on a service-based agreement.
- **No fixed costs:** The assumption is that activation and payment of TMB takes place only if and as needed (“pay as you activate”).
- **Full flexibility:** OTA provisioning via TSM or directly through the SP.
- **Fully customizable:** TMBs come as a pre-certified, white-label solution with open Application Programming Interfaces (APIs).

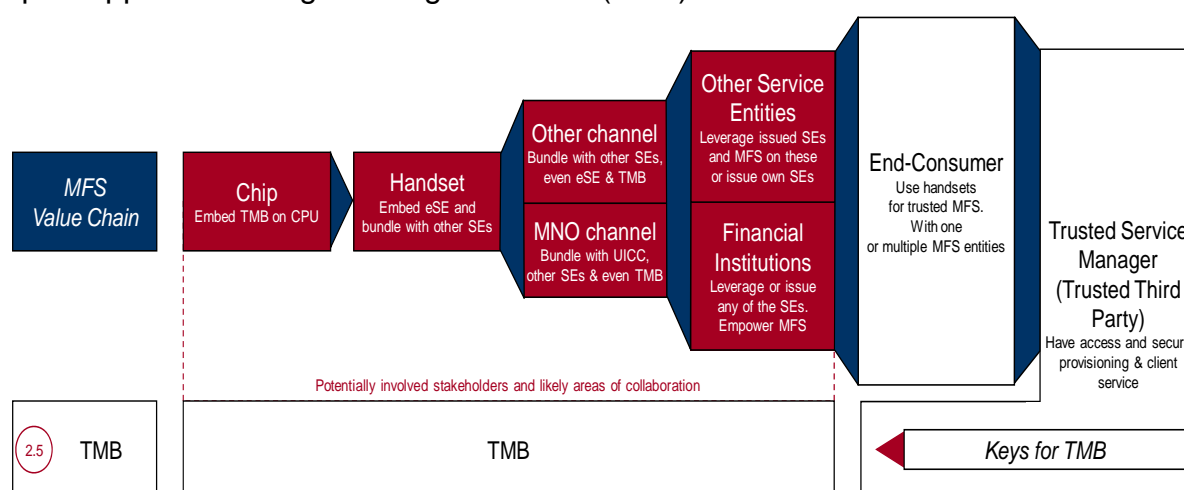


Figure 10: TMB in the context of the MFS Value Chain and the Stakeholders

<sup>78</sup> Note: Pre-certification can for example be based on Common Criteria.

In brief, the TMB is an effort to promote MFS which roots in the very heart of the mobile device, the CPU, and empowers the whole subsequent Value Chain to leverage the potential of MFS, based on a standardized, open SE that is naturally distributed to all new mobile devices shipped.

### 2.5.3. Technical enablers and inhibitors

In technical terms TMBs are based on four conceptual pillars:

- Assurance of the integrity and robustness of the whole mobile device by separating security critical processes from normal Applications.
- Assurance of trustworthy user interaction between the mobile device, different SEs and a service backend.
- Empowerment of numerous, separated and certified security spaces for different service and Application providers on one mobile device.
- Empowerment of the integrated provisioning of various secure services to different mobile devices for independent Application and Service Providers.

The management of TMBs is in the process of being standardized in order to rather rapidly establish a wide understanding of the interfaces with other SEs and the potential access points to the TMB.<sup>79</sup> Also, quick common understanding of the crucial entry point to the TMB shall hinder a fragmentation of the installation activities.

### 2.5.4. Opportunities and challenges

TMBs add an integration layer, pre-certified security and open interfaces to the overall service concept of mobile devices. While other SEs provide rather closed execution environments and no secure and brandable user interface, TMBs can add an open architecture and new levels of security to the SPs.

By leveraging TMBs in their service approach, SPs do not only get the opportunity to rapidly deploy their MFS offerings OTA, but are also able to combine the IDs from and across existing SEs for new service designs and business models. Further, TMBs and other SEs can be integrated with the value of a trusted UI, pre-certification and OTA-provisioning to empower new MFS.

This all comes with no fixed costs but may include service-based agreements, e.g., on a “pay as you activate” basis. This is an assumption of the business model, other models may also exist based on the business interests of the involved parties like chip and handset vendors.

---

<sup>79</sup> Note: Activities include initiatives in, for example, the Global Platform Consortium.

### 3. Summary on Secure Mobile Payments alternatives and the outlook for MFS

The above chapters have presented five potential Secure Elements for MFS:

1. Passive & Active Stickers – being particularly interesting for the Stakeholders at the rear of the MFS Value Chain, where a quick, no frills path to MFS is wanted.
2. Secure Micro SD Cards – being an SE alternative esp. for Financial Institutions, Other Service Entities, Mobile Network Operators and Other Mobile Distribution Channels to extend their services in the mobile domain and go beyond established distribution channels and business logics.
3. UICCs – being a domain of the MNOs which could be leveraged together with other MFS Value Chain Stakeholders to open an additional service path for Financial Institutions and Other Service Entities and promote MFS to the End Consumers.
4. eSE - particularly depending on the initiative of Handset Vendors which could then empower collaborative business models with the subsequent Value Chain Stakeholders.
5. TMB – as a promising upcoming technology at the root of the mobile devices, the CPU, which can help unleash the full service potential of the entire Value Chain and across different SEs, based on the initiative of the Chip and Handset Vendors.

In the following picture the various SEs are illustrated in relation to the MFS Ecosystem Value Chain.

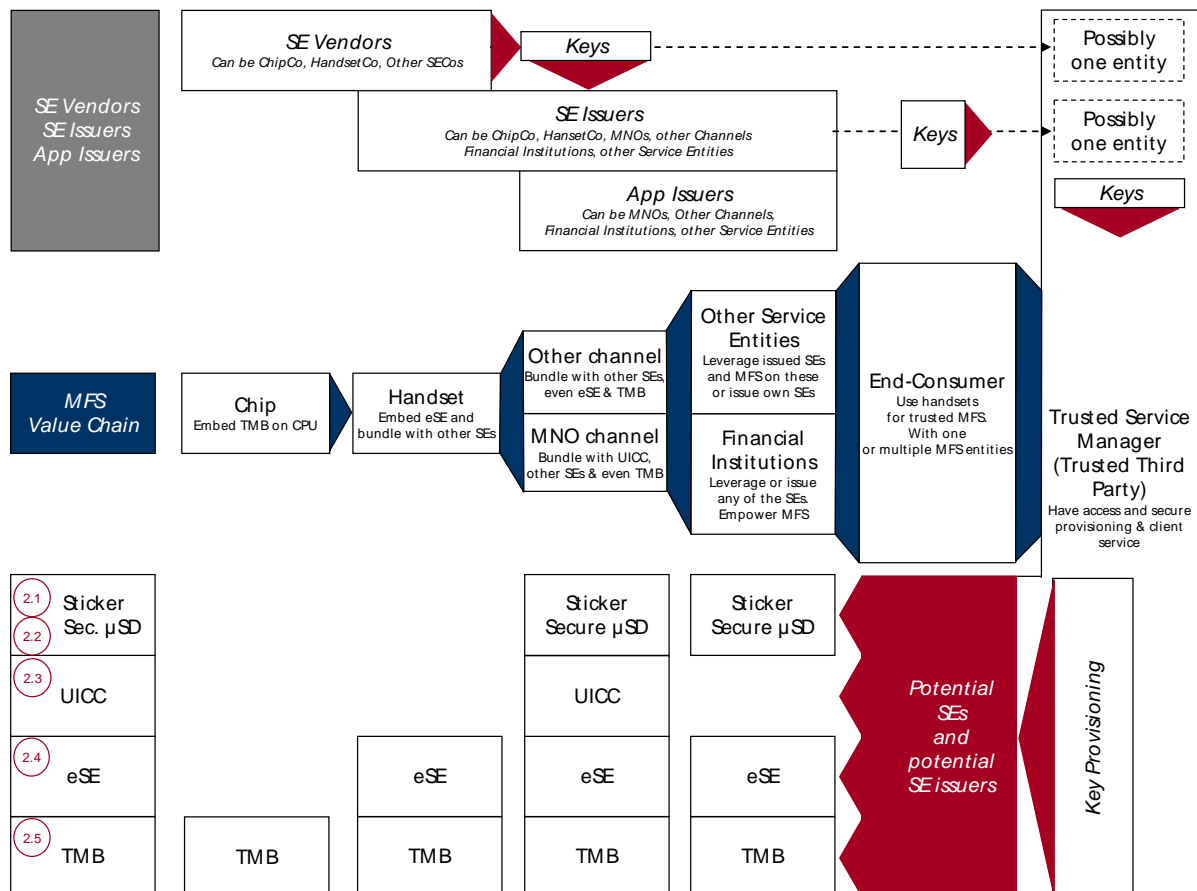
For Financial Institutions and Other Service Entities the options that they can drive independently to the market (i.e. become the SEI) are Stickers and Secure SD cards. Some form of collaboration is possible with these options as well, and in some cases even recommended in order to reach sufficient market coverage. In collaboration with other Stakeholders the FIs can issue their applications through other SEs like eSEs and TMBs and even become the SEI through appropriate agreements.

For MNOs UICCs provide an additional SE token which they can utilize as becoming SEI. This can take place in collaboration with SPs or independently, depending on the business interests of the MNO. Other distribution channels of mobile handsets can leverage their position to collaborate with SPs through SE bundling to enhance the MFS offering on the market.

Handset vendors can leverage their position through eSEs or TMBs, either through collaborating with SPs or becoming a SP themselves. The TMB can also be opened up to SPs in order to facilitate the market acceptance.

Chip vendors can leverage their position mainly through offering security enhancing service agreements based on TMBs.

Together, these solutions draw the following picture of the MFS Ecosystem:



**Figure 11: Overview of Value Chain, Stakeholders and SEs for MFS**

This overview shows the essential questions for the further advancement of the MFS ecosystem. These questions are also the key recommendations to the readers of this paper – as a next step in MFS development they should be answered by the respective organization. Implementation of a chosen SE technology will result as a consequence, e.g. based on the characteristics explained in the Appendix:

1. The Stakeholders along the Value Chain have to define their positions: Do they want to be
  - a. SE Vendors
  - b. SE Issuers
  - c. Application Issuers
  - d. A combination of these?
2. Based on this positioning in the MFS Value Chain, which technology would best fit their needs?
3. Based on the SE technology, which process of key provisioning shall be implemented, i.e. who is the Trusted Service Manager or does a Stakeholder want to hold this position in-house?

4. Based on the context of the respective Stakeholder along the Value Chain, who might be interesting partners to design joint business models and trigger a quick diffusion of the SE technology and the hence empowered services?

From the industry's perspective, existing bridge technologies already allow the introduction of MFS in specific areas, as some of the above described examples have shown.

For large scale take-off of MFS, however, joint efforts remain necessary in the areas of:

- Designing a modular, interface-based architecture for the overall Ecosystem.
- Promoting interaction and collaboration across companies and technologies.
- Standardizing SEs as well as the relevant interfaces and provisioning processes related to them.
- Opening the Ecosystem through the introduction of platform technologies which empower the Application Issuer to openly and independently leverage the different underlying SEs.

Hence, it is now in the hands of the various players in the MFS industry to take this paper as a guideline for deciding and implementing the next steps in the development of Mobile Financial Services – for the sake of the industry's prosperity and the promotion of convenient, trustworthy and secure Mobile Financial Services for the End Consumers.

## Appendix - Requirements table

### aa. Prerequisites

In order to enable a true take off of the MFS industry, this paper has assumed the following prerequisites to be given:

#### i. Multi-Application management capability

SEs must eventually be capable of handling several Applications from several Issuers. This is equally valid for MFS referring to proximity payments via NFC and remote MFS. It is understood that this might not be the case in the beginning and the market may as well start with solo-Applications, in particular if the respective SE Issuers and / or App Issuers want to solely leverage their technological positions for a certain time. Here, the group sees that there are three main alternative routes:

1. A SE supports only few, i.e. 1 or 2 MFS Apps from sole or allied entities.
2. A SE supports full multi-App capability for multiple MFS providers, i.e. fully covering one vertical industry.
3. A SE supports Apps from multiple vertical industries, for example Transport, Health Care, Insurance, Loyalty Programs etc. including and in addition to MFS.

The complexity and certification requirements may increase significantly from point 1 to 3. SE costs may increase if proprietary, non-standardized (i.e. not clearly modularized and without clear APIs) Apps shall be supported.

The more complexity and costs are involved, the more challenging a design of a business case will become. Nevertheless, interesting business models could particularly lay in systemic designs that reduce complexity in the ecosystem, i.e. an integrative solution across industry verticals.

From a provisioning perspective, the TSM service can be expected to initially be built and billed for one service. Adding new Apps may be billed on a modular basis, not only variable cost additions, as long as the SE and its management are clearly modularized and based on open standards / Open APIs.

The above points translate into a capability to serve the mass market with the introduced SEs, if not from the very beginning, then at least over time and based on a modular and multipliable core system and business model.

#### ii. Secure management across the full lifecycle of MFS Apps

Full secure management for MFS Apps, in particular when issued by Financial Institutions, has to be ensured across the entire lifecycle of the Apps, i.e. all the way from the enrolment through to the final and full cancellation of the Application. For instance, key management, authentication and certificates created which, together,

then enable and guarantee the access to and interaction with financial assets must meet the same security levels as provided by the existing physical solutions (e.g. Debit and Credit Cards).

### iii. Interoperability across locations

International interoperability guarantees that the End Consumer can use the mobile device-based MFS seamlessly, even if travelling across borders. The scope of the required interoperability depends on the respective service and can range from city-wide to full global interoperability. Interoperability can be ensured or limited by the Application Issuers. Initial Applications could be limited to a certain locations or region to limit complexity in setting up the system. Also, and data services for particular MFS may be disabled to avoid unnecessary costs when travelling.

### iv. Compliance with applicable law

Legal requirements must be taken in account. Each Service Provider and App Issuer must fully comply with the respectively relevant law (i.e. the specific regulations and requirements of the respective nation and Financial System) in order to safeguard the End Consumers' rights. Differences in international / inter-continental legislations will need to be taken into account when designing and issuing Applications that shall be internationally interoperable.<sup>80</sup>

The legal context for MFS might not be fully defined in the respectively relevant regions yet. In the European context, for instance, SEPA requirements for mobile payments will need to be clarified further and translated into requirements to which the MFS industry can then comply with.

#### **bb. Initial Bank Requirements: Table**

Description	UICC	eSE	Sec. µSD	TMB	Sticker
1. Can credentials be provisioned OTA?	Yes.	Yes.	Yes.	Yes.	Passive Stickers: No. Active Stickers: Yes.
2. What kind of LCM is possible? <sup>81</sup>	All, based on GlobalPlatform	All, based on GlobalPlatform	All, based on GlobalPlatform	Dynamic LCM.	Passive Stickers: None. Active Stickers: All, based on GlobalPlatform.
3. Are business agreements with 3 <sup>rd</sup> parties (e.g. an MNO or a TSM) needed for App	An agreement with the MNO is needed, defining the terms for UICC-access.	An agreement is needed with a TSM if issuance and LCM is not done in-house.	An agreement is needed with a TSM if issuance and LCM is not done in-house.	An agreement is needed with a TSM if issuance and LCM is not done in-house.	For both Stickers: None on the Handset and Network side.

<sup>80</sup> Note: For example, PINs for MFS are allowed in the United States but forbidden in France.

<sup>81</sup> Note: LCM can be static or dynamic. Static refers to LCM that depends on the End Consumer coming to a specific site for provisioning, e.g. a Bank branch. Dynamic LCM refers to OTA provisioning.

issuance and LCM?	Also, a TSM agreement is needed if issuance & LCM is not done in-house.				Addition for Active Stickers: Agreement is needed with a TSM if issuance and LCM is not done in-house.
4. Is there a technical dependency on any party?	Dependency exists towards the MNO as UICC Issuer.	Dependency exists towards the Handset Vendor for embedding the eSE.	Secure Micro SD can be sourced directly from the SE Vendor.	Dependency exists towards the Chip Vendor for embedding the TMB.	For both Stickers: Can be sourced directly from the SE Vendor.
5. What kinds of changes are required compared to existing card issuing processes?	The need for an in-house or TSM-related solution means that the processes will change to integrate the OTA option of personalization (see section 1.2.3.).	The need for an in-house or TSM-related solution means that the processes will change to integrate the OTA option of personalization (see section 1.2.3.).	If traditional pre-personalization (i.e. static, in-house) is applied, close to existing card issuing processes.  If OTA post-personalization is targeted, in-house or TSM-related process changes are needed (see section 1.2.3.).	The need for an in-house or TSM-related solution means that the processes will change to integrate the OTA option of personalization (see section 1.2.3.).	For both Stickers: No changes.
6. Which interaction takes place in the personalization process and how convenient is it for the End Customer? <sup>82</sup>	Pre-personalization may require interaction with the MNO. Post-personalization is most likely.	Post-personalization is expected to be the only relevant alternative.	Similar to existing Card issuance processes. For pre- and post-personalization a physical token is handed out, attached into the mobile and either already holds pre-personalized credentials or established an OTA installation process.	Both pre-and post personalization possible. The step of sticking a physical SE into the phone becomes obsolete.	For both Stickers: Similar to existing card. For the Passive Sticker only pre-personalization is possible. Conceptually easy for the end user since a physical token is handed out to be stuck onto the mobile device.
7. From the FI perspective, is there a commercial agreement needed with other Value Chain Stakeholders (e.g. alliance structures, revenue sharing, etc)? <sup>83</sup>	Yes, with the MNO as the UICC Issuer.	No, can be independent.	No, can be independent.	No, can be independent.	For both Stickers: No, can be independent.

<sup>82</sup> Note: It is assumed that a convenient enrollment process is designed, leveraging existing mobile and internet technologies (including triggering the installation via (secure) SMS as done, for example, in the case of Mobile Boarding Cards) and respecting the applicable legislation so that the End Consumer does not need to care. End Consumer support may be required in all alternatives.

<sup>83</sup> Note: This refers to any commercial arrangements beyond a co-operation with a TSM. If issuance and LCM are done in-house, not even an external TSM arrangement is needed.

8. Which LCM costs need to be expected? <sup>84</sup>	Depending on agreements with the MNO and TSM and the ecosystem setup.  LCM services need to be paid for the TSM.	Depends on business model set-up (e.g. proprietary, alliances, TSM or in-house).	Depends on business model set-up (proprietary, alliances, TSM or in-house).  No LCM needed, if the Sec. $\mu$ SD is issued in a static mode.	Depends on business model set-up (proprietary, alliances, TSM or in-house).	For Passive Stickers: None, static.
					For Active Stickers: Depends on business model structure (proprietary, alliances, TSM or in-house).
9. When is the SE alternative supported by the mobile devices on a mass market scale for NFC payments? <sup>85</sup>	First phones in early 2010, mass deployment in 2011 / 2012.	Commercially available since 2005. Availability expected for CDMA markets in 2010. GSM markets availability on demand.	SD slots available in a great variety of phones <sup>86</sup> , but additional driver or interface necessary (see section 2.2.3.). Smart Phones drivers for Secure SD w/o antenna exist. Secure SD with antenna / NFC are being introduced for example in Taiwan / Malaysia.	First phones expected in 2010.	Passive Stickers: Now, can be used on all phones or other portable devices.
					Active Stickers: Depends on the diffusion of Bluetooth technology in the phones.
10. When is this SE alternative available for mass market use?	First products (SWP UICCs) exist since late 2009. More products expected in 2010.	Products already exist for years.	Sec. $\mu$ SD with integrated antenna / NFC expected in 2010. Sec. $\mu$ SD w/o antenna available since 2007.	First products expected in 2010.	Passive Stickers: Available. Tens of millions already sold.
					Active Stickers: Expected for 2010.
11. Does it work with existing point of sale infrastructure for NFC? <sup>87</sup>	Yes, see several NFC trials all over the world.	Yes, see several NFC trials all over the world.	Yes, as proven in first trials. However, more commercial trials needed to confirm.	Yes. Can also be used for remote payments, i.e. give trusted output and feedback without merchant infrastructure via Secure Display and Secure Keypad. NFC if supported by the phone.	For both Stickers: Yes. Acts like a Contactless Card attached to the phone.

<sup>84</sup> Note: The costs of the LCM also depend on the level of security and service provided, e.g. are they rather comparable to EMV Credit Cards or merely magnetic stripe solutions.

<sup>85</sup> Note: This depends on the Single Wire Protocol support and the built in NFC antenna being ready.

<sup>86</sup> Note: See calculation in footnote 39.

<sup>87</sup> Note: Availability of merchant infrastructure depends on region. Merchants must have contactless infrastructure independent of the solution – this is not the case as of today outside some London districts and some places in the US and Asia. In the EMV countries, there might be a need for software upgrade of POS terminals.

**cc. Operational Bank Requirements: Table**

Description	UICC	eSE	Sec. µSD	TMB	Sticker
12. Does the SE utilize the multimedia capabilities of the mobile phones for branding purposes?	Yes.	Yes.	Yes.	Yes.	Passive Sticker: The only possibility is a logo on the Sticker.
					Active Sticker: Yes b/c they are linked to the Application processor.
13. Can the SE Issuer brand the physical device holding the SE?	Yes, logo on the UICC and the packaging, however, not visible once stuck into the mobile device.	Yes, logo on the phone and the packaging.	Yes, logo on the Sec. µSD and the packaging, however, not visible when stuck into the phone.	Yes, logo on the phone and the packaging.	For both Stickers: Yes, logo on the Sticker and the packaging. Will be visible while used.
14. Can the same SE be utilized for multiple Applications / services from the same Application Issuer?	Yes.	Yes.	Yes.	Yes.	Passive Stickers: Assumed to be no, since no mechanism for application selection at the point of sale.
					Active Stickers: Yes.
15. Is the customer able to store all his Applications on this SE (from other SPs as well)?	Yes, depending on the business relation between the App Issuers, the SE Issuer and the MNO.	Yes. The eSE is designed to include numerous service environments from different Service Providers. They can load a variety of Apps into their secure service environment on the phone.	Yes, depending on the business relation between, potentially numerous, SPs. One SP – or a central party - has to be SE Issuer. Subsequent SPs broker an agreement with the SD Issuer.	Yes, multiple SPs can issue their own trusted Execution Environment (i.e. their own SE) on one TMB.	Passive Stickers: No. One App from the respective SP.
					Active Sticker: Yes, in principle.
16. Who should design the Customer Care solution and how is it communicated to the End Consumer?	The MNO and respective SP need to communicate the Customer Care arrangement clearly.	The involved Stakeholders need to consider the Customer Care solution together and clearly communicate it to the End Consumer.	The involved Stakeholders need to consider the Customer Care solution together and clearly communicate it to the End Consumer. If single point of contact towards the end user, this SP will provide the Customer Care.	The involved Stakeholders need to consider the Customer Care solution together and clearly communicate it to the End Consumer.	For both Stickers: There is one point of contact to the End Consumer. This Service Provider needs to provide Customer Care.

**dd. Security Bank Requirements: Table**

Description	UICC	eSE	Sec $\mu$ SD	TMB	Sticker
17. Has the solution been approved to the EMVCo security standards?	Not yet. Case by case acceptance existing for closed loop payment systems.	Yes. Most eSEs are EMV certified.	Not yet but is in progress. Case by case acceptance exists for closed loop payment systems.	EMV certification hasn't been applied yet.	Passive Sticker: Yes, but likely to be limited to magnetic stripe-like security standards.
					Active Sticker: If counter reset may be performed, EMVCo security standards could be met.
18. Who defines the security requirements for Bank payment Application other than EMVCo?	Requirements set by the SE Issuer and the payment schemes.	Requirements set by the SE Issuer and the payment schemes. Used in the US since 2005.	Requirements set by the SE Issuer and payment schemes. No standardization efforts started yet.	Requirements set by SE Issuer and payment schemes. E.g. used in the US since 2009.	For both Stickers: Requirements set by SE Issuer.
19. Who defines the security requirements for Mobile authentication Application?	Requirements set by the App Issuer, i.e. also becoming Identity provider. E.g. various wireless PKI Applications exist.	Requirements set by the App Issuer, i.e. also becoming Identity provider. E.g. various wireless PKI Applications exist.	Requirements set by the App Issuer, i.e. also becoming Identity provider. E.g. various wireless PKI Applications exist.	Requirements set by the App Issuer, potentially limited to certain implementations. Simple forms of ID credentials may also suffice.	For both Stickers: Requirements set by SE Issuer, because only his Apps are pre-personalized.
20. Are there (country-specific) regulatory requirements that should be taken in account?	Limitations in using encryption and issues regarding privacy, anti-trust, and security of mobile payment might occur in selected countries. <sup>88</sup>	Limitations and other issues as for UICC.	Limitations and other issues as for UICC, and eSE.	Not allowed yet by payment schemes or many central banks. Limitations and other issues as for UICC, eSE and SD.	Limitations and other issues as for UICC, eSE, SD and TMB.
21. Are there sufficient open standards available for the interfaces (e.g. the NFC module, the phone functions), and are there transaction protocols in place?	Yes, the relevant standards are : Java Card GlobalPlatform EMVCo NFC Forum ISO 14443 ETSI (SWP, HCI).	Yes, the relevant standards are: Java Card GlobalPlatform EMVCo NFC Forum ISO 14443.	Sec. $\mu$ SD – Handset interaction not yet standardized in all devices. Proprietary implementations varying by Handset; 1 <sup>st</sup> standardized solutions available. Relevant standards: Java Card, GlobalPlatform, EMVCo NFC Forum, ISO 14443, MC-Ex. SDA proposed as physical interface standard.	Standards are to be defined. Basic functions are standardized, SE-related ones are being developed by the Trusted Computing Group, and possibly in the Mobile Industry Processor Interface Alliance.	For both Stickers: Yes, the relevant standards are: ISO14443, JavaCard, and GlobalPlatform.

<sup>88</sup> Note: For example, PINs on mobile may be an issue in some countries. Also for Card Not Present Applications, national regulations (in technical rather than legal terms) may hinder the MNO to become SEI for MFS.

## List of References

- Electronic Storage (2006):** Removable memory cards: not just a flash in the pan,  
URL: [http://www.oto-online.com/pdf/oto\\_download/2006/06/OTO\\_June\\_P5254\\_MemoryCards.pdf](http://www.oto-online.com/pdf/oto_download/2006/06/OTO_June_P5254_MemoryCards.pdf),  
Accessed: Dec 6<sup>th</sup> 2009.
- GlobalPlatform (2009a):** GlobalPlatform's Value Proposition for the Public Transportation Industry,  
URL: [http://www.globalplatform.org/documents/whitepapers/GP\\_Value\\_Proposition\\_for\\_Public\\_Transportation\\_whitepaper.pdf](http://www.globalplatform.org/documents/whitepapers/GP_Value_Proposition_for_Public_Transportation_whitepaper.pdf),  
Accessed: Dec 6<sup>th</sup> 2009.
- GlobalPlatform (2009b):** The GlobalPlatform Value Proposition for Identity Management,  
URL: [http://www.globalplatform.org/uploads/GP\\_White-Paper\\_IdentityMGMT\\_justified.pdf](http://www.globalplatform.org/uploads/GP_White-Paper_IdentityMGMT_justified.pdf),  
Accessed: Dec 6<sup>th</sup> 2009.
- GSM Association (2008):** GSMA calls for Pay-Buy-Mobile handsets,  
URL: <http://gsmworld.com/newsroom/press-releases/2008/2090.htm#nav-6>,  
Accessed: Jan 12<sup>th</sup> 2010.
- Informa (2009):** Informa Telecoms & Media: Mobile Distribution and Retail, 6<sup>th</sup> edition.
- iSuppli (2008):** Mobile Handset Shipments with micro SD / Micro SDHC, in: Data Flash Market tracker Q3/2008:, supplied via SD Association.
- Mobey Forum (2002):** Preferred Payment Architecture: Local Payment,  
URL: <http://mobeyforum.org/files/Local%20Payments%20Discussion%20Document%201.0.pdf>,  
Accessed: Dec 6<sup>th</sup> 2009.
- Mobey Forum (2003):** Mobey Forum White Paper on Mobile Financial Services,  
URL:  
[http://mobeyforum.org/files/Mobey%20Forum%20White%20Paper%20on%20Mobile%20Financial%20Services%20v1\\_14.pdf](http://mobeyforum.org/files/Mobey%20Forum%20White%20Paper%20on%20Mobile%20Financial%20Services%20v1_14.pdf),  
Accessed: Dec 6<sup>th</sup> 2009.
- Mobey Forum (2005):** Security Element Technical Analysis (Executive Summary),  
URL: <http://mobeyforum.org/files/Mobey%20Forum%20Security%20Element%20Analysis%20Summary%202005.pdf>,  
Accessed: Dec 6<sup>th</sup> 2009.
- Mobey Forum (2006):** Mobile Financial Services - Business Ecosystem Scenarios & Consequences,  
URL: <http://mobeyforum.org/files/Mobey%20Forum%20MFS%20Business%20Ecosystem%20Summary.pdf>,  
Accessed: Dec 6<sup>th</sup> 2009.
- Mobey Forum (2008):** Best Practices for Mobile Financial Services, Enrollment Business Model Analysis,  
URL:  
<http://mobeyforum.org/files/bestpractice/Best%20Practices%20for%20MFS%20Enrolment%20Business%20model%20analysis%20final.pdf>,  
Accessed: Dec 6<sup>th</sup> 2009.
- Mobey Forum (2009a):** Global Overview of commercial implementations and pilots of NFC payments during 2009. Article for globalsmart.com – Smart Card Technology International.  
URL: <http://mobeyforum.org/>,  
Accessed: Feb 5<sup>th</sup> 2010.
- Mobey Forum (2009b):** Why aren't banks rushing for NFC payments? Article for globalsmart.com – Smart Card Technology International.  
URL: <http://mobeyforum.org/>,  
Accessed: Feb 5<sup>th</sup> 2010.
- PrimeLife (2008):** D 6.2.1 Infrastructure for Trusted Content,  
URL: [http://www.primelife.eu/images/stories/deliverables/d6.2.1-infrastructure\\_for\\_trusted\\_content-public.pdf](http://www.primelife.eu/images/stories/deliverables/d6.2.1-infrastructure_for_trusted_content-public.pdf),  
Accessed: Dec 6<sup>th</sup> 2009.
- PrimeLife (2009):** Identity Management Infrastructure Protocols for Privacy-enabled SOA,  
URL: [http://www.primelife.eu/images/stories/deliverables/h6.3.1-requirements\\_for\\_privacy\\_enhancing\\_soas-public.pdf](http://www.primelife.eu/images/stories/deliverables/h6.3.1-requirements_for_privacy_enhancing_soas-public.pdf),  
Accessed: Dec 6<sup>th</sup> 2009.
- SD Association (2010):** SD Association celebrates 10 years of innovation at CES.  
URL: [http://www.sdcard.org/press/SD\\_Celebrates\\_10\\_Years\\_of\\_Innovation\\_at\\_CES\\_2010.pdf](http://www.sdcard.org/press/SD_Celebrates_10_Years_of_Innovation_at_CES_2010.pdf),  
Accessed: Jan 10<sup>th</sup> 2010