The current issue and full text archive of this journal is available at
www.emeraldinsight.com/0265-2323.htm

VIEWPOINT

Alternatives for banks to offer secure mobile payments

Liisa Kanniainen
Mobey Forum, Helsinki Nordea, Helsinki, Finland

Abstract

Purpose – Mobile financial services (MFS) applications require a hardware secure storage, secure element (SE) for crucial payment and authentication credentials, comparable to the EMV chip cards recently introduced in the payment card world. However, the diffusion of MFS is currently obstructed due to debate within the industry over which SE technology is to be adopted. The purpose of this paper is to demonstrate how industry participants can position themselves in the value chain and select the ideal SE option, thereby accelerating the acceptance of MFS.

Design/methodology/approach – This paper is based on previous research done in this field by Mobey Forum and other mobile payments bodies.

Findings – The study shows that MFS value chain positioning has a direct effect on which SE alternative is most suitable to the company. Identifying the most suitable SE technology in turn allows companies to seek out the most interesting business partners, and thereby results in a quick and widespread diffusion of MFS.

Originality/value – This study has implications for the adoption of MFS technology and the development of the mobile payments marketplace. It is especially relevant to management working towards creating a working MFS ecosystem.

Keywords Data security, Value chain, Mobile communication systems, Payments, Standards, Mobile Financial services

Paper type Viewpoint

The Mobey Forum published a new white paper *Alternatives for Banks to Offer Secure Mobile Payments* on March 8, 2010. The highlights of this cutting-edge industry white paper are described in this article. The white paper is freely downloadable through www.mobeyforum.org

About Mobey Forum

Mobey Forum is a global non-profit organization, driven by the finance industry. Mobey Forum has over 50 members; member categories are banks, vendors such as leading mobile device manufacturers and semiconductors, payment processors and mobile service providers. The Mobey Forum member banks have over 331 million customers worldwide.

The vision of Mobey Forum is to create a prosperous mobile financial services ecosystem. The mission of the Mobey Forum is to facilitate financial institutions (FI) to offer mobile financial services. Its main focus is in building sustainable business model alternatives.

Mobey Forum's strategy is threefold:

(1) Informational – industry insight, first-hand experience sharing, knowledge repositories, regular industry news and member updates.

International Journal of Bank Marketing
Vol. 28 No. 5, 2010
pp. 433-444

0265-2323
DOI 10.1108/02652321011064926

(2) Networking – Mobey quarterly meetings collect the leaders cross industries to build new relationships.

(3) Shaping the industry: interaction and ongoing liaisons with standardization organizations, analysts and industry influencers.

Security as an element of the mobile financial services value chain

Security is one of the fundamental elements of any payment solution. For certain mobile financial services applications there is a need to have a hardware secure storage, Secure Element (SE), for crucial payment and authentication credentials, comparable to the EMV chip cards recently introduced in the payment card world. However, agreeing which element in the mobile device would serve as this SE, or whether there be several options in parallel, has become a main hurdle for the commercialization of the services. There seems to be severe challenges in reaching consensus, particularly regarding sharing (renting or selling) the SE space amongst the key stakeholders. The complexities and inter-dependencies of the collaborative mobile contactless payment (MCP) ecosystem have proven to be even higher than earlier expected.

Mobey Forum has taken this topic as a subject of the current white paper. It elaborates on the question how different SEs can enable FIs to offer mobile financial services (MFS) and hence empower the take-off of the MFS ecosystem. It is targeted at business managers in FIs. For them, it strives to clarify the business implications of the various technical SE alternatives.

This article presents a brief status analysis of the MFS ecosystem and the stakeholder positions in the MFS value chain. It includes a short introduction of the SE-related stakeholder roles in the MFS Ecosystem (SE vendor (SEV), SE issuer (SEI), application issuer (AI) and trusted service manager (TSM)). Five different SE alternatives are described: stickers (active and passive), secure micro SD card, universal integrated circuit card (UICC), embedded secure element (eSE) and trusted mobile base (TMB). A more detailed analysis of the SE alternatives and related business model scenarios, including technical enablers and inhibitors and opportunities and challenges, is presented in the white paper.

The article concludes with a summary about the various SE alternatives for MFS and presents a brief outlook on the next steps for the MFS industry.

In brief, the key finding is that each FI now needs to decide which position it wants to claim in the MFS value chain – to become a SEI, AI 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.

Status of the MFS ecosystem

The first MCP pilot started 2003, and since then there have been many pilots testing the NFC payments (GSM Association, 2008; Mobey Forum, 2009a). By now it has been proven that the technology works and consumers love it (Mobey Forum, 2009b). 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 detailed roles of the stakeholders and the division and level of costs and revenues continue to be the main discussion points.

There seems to be severe challenges in reaching consensus, particularly regarding sharing (renting or selling) the SE space amongst the key stakeholders. The complexities and inter-dependencies of the collaborative MCP ecosystem have proven to be even higher than earlier expected.

Therefore, understanding the characteristics of the various SEs will play an important role for the different stakeholders along the MFS value chain. Whoever dominates the respective SE will have a strong position to build trusted services around the SE, in all possible definitions of MFS.

Role of SEs for MFS

A 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 (see Figure 1). Conceptually, SEs can be categorized into three areas (Mobey Forum, 2005):

(1) removable SEs (e.g. stickers, secure micro SD cards and UICCs);

(2) non-removable SEs (e.g. embedded SEs); and

(3) SEs from a combination of software programs on dedicated hardware (e.g. TMB).

At present, the use of a SE is only mandatory for the EMV-based contactless payment area, based on the EMVCo 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 to enhance security and usability.

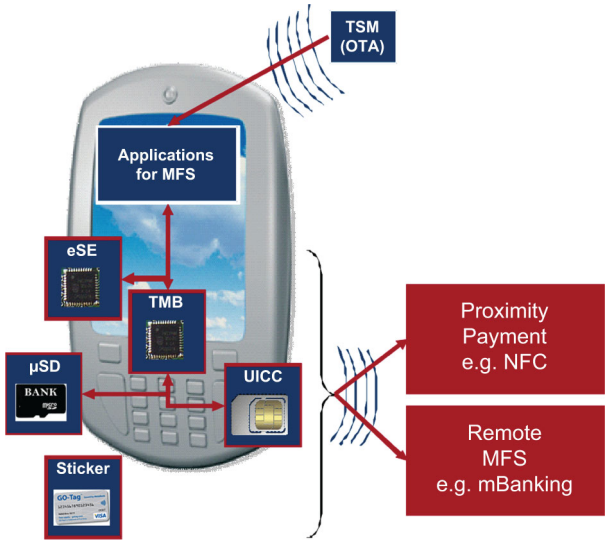

Figure 1.
Potential secure elements for mobile financial services

SE-related roles in the MFS ecosystem

There are four main roles along the value chain of MFS which are essential in making the overall system work (see Figure 2):

(1) *The SEV*. The physical producer of the SE. This can be chipset corporations (esp. for TMBs), Handset providers (esp. for eSEs) and other SE producers such as semiconductors, e.g. in the domain of stickers, secure micro SD cards, or UICCs. Although the SEV may also be the manufacturer, this is not always the case.

(2) The *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 AIs. Alternatively, SEIs can also be independent companies that wish to empower MFS and claim a position in the newly developing MFS Ecosystem and offer services directly to End Consumers.

(3) *The 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. Although sometimes referred to as the application provider, we have used AI to clearly differentiate between app issuance and provisioning. The AI often outsources the provisioning and management of application to a third party.

(4) *The 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.

Starting from the point of view of the end consumer, the following motivations apply along the value chain of MFS:

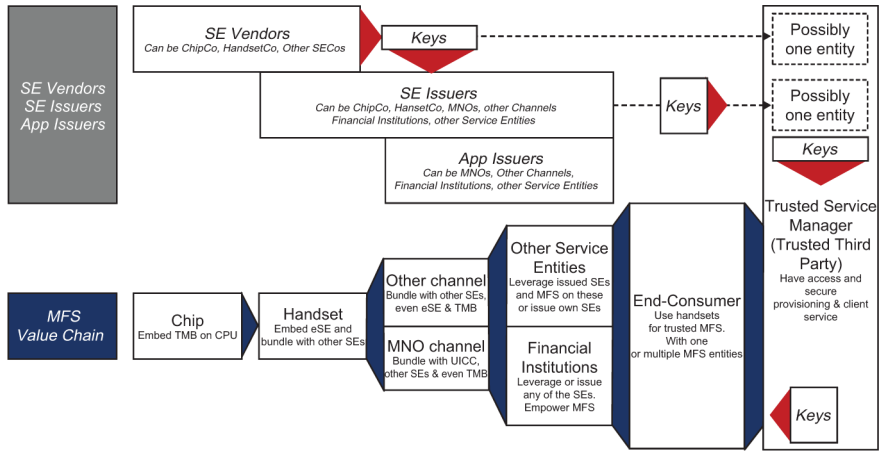

Figure 2.
The mobile financial services value chain

(1) FIs and other service entities (e.g. transport authorities, merchants, customer loyalty programs, frequent traveler programs, governmental service entities, etc) 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 AIs in this paper. From the perspective of these two stakeholders, the first potential enablers are NFC-enabled secure micro SD cards and stickers, as both can be rapidly deployed and flexibly attached to the mobile devices.

(2) Mobile network operators (MNOs) and other channels of mobile device distribution (consult www.gsmworld.com for up-to-date figures on mobile distribution in various markets) 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 SEIs. Alternatively, MNOs can decide not to get directly involved with MFS 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.

(3) 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 SEIs as well.

(4) Chip vendors can integrate additional open SE architectures and platforms into the central processing unit (CPU), leveraging the 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 SEIs 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 an SEI and have full control over the SE – hence even opening it to other AIs for additional MFS. 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.

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) business-to-business (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 AIs, 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 FI 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 alternatives

The AI can decide between different SEs and build his service package independently or together with various SEIs and various TSMs (GlobalPlatform, 2009a, b). Simultaneous use of multiple SEs is not currently supported by the standards, but work is ongoing to reach this common target for example in GlobalPlatform and on other standardization forums. The selection of the SE will depend on AI's respective business logics and the service level they want to achieve.

In any decision concerning the FIs' 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.

In order to clarify what the different SEs can do, the following sections describe them one after the other. Detailed evaluation of the SE alternatives is available in the Mobey Forum white paper.

Sticker

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:

(1) *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 (UI), 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.

(2) *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 percent of all mobile phones, although the figure is closer to 90 percent in the industrialized world and around 50 percent in emerging markets. Active stickers enable all the usual NFC use cases such as card emulation, reader mode and peer-to-peer/person-to-person interaction.

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 UI.

Active sticker solutions are available 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.

Secure Micro SD card (secure μSD)

Mobile users are generally familiar with SD cards in mobile phones. In total 40 percent of all mobile device holders are active SD card users. In 2009, 90 percent of all shipped Handsets that included memory cards used SD Cards slots, increasingly being slots for Micro SD cards (iSuppli, 2008). Since 2000, 2.5 billion cards of the globally interoperable SD memory card standard have been shipped, making it the "the world-leading de facto interface of removable media" (SD Association, 2010).

With a low impact on the bill of materials of the handset vendor, diffusion of SD card slots has increased from 30-40 percent in 2006 to approximately 50 percent at present. 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 percent of all mobile devices shipped included a micro SD card slot. It can be expected that in 2011 60 percent of the installed mobile device base will hold a micro SD card slot. With these trends towards microSD™ slots, micro SD cards with an embedded chip that serves as SE are a potential way to extend the security level and service offerings on mobile devices.

For the use in MFS, micro SD card with SE is 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. Although this interface has not yet been standardized, prototypes have been in use in Asia since 2008. 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.

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. In this concept, the NFC only works when the phone is switched on.

(2) *Antenna on the mobile.* The card includes the secure storage, security domain and NFC chip, but the antenna is on the mobile device. In this concept, the NFC also works when the phone is switched off.

(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:

- The MNO can offer a flexible means to distribute NFC applications independently from his UICC channel that 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 FIs 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 brief, the secure micro SD card is therefore an interesting SE alternative for FIs, Other service entities, MNOs and other mobile distribution channels to offer and promote MFS to the end consumers.

UICC

In second generation mobile networks (2G), the SIM is the physical Smart Card used to control access of mobile devices to the MNO network. In third generation networks (3G), this physical component is called UICC. UICCs contain at least the SIM or USIM application. 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.

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 (Mobey Forum, 2008). Hence, they can serve as SEs for MFS just as the other SEs described in the above and below chapters.

eSE

Today, 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.

TMB

A 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 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 by *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 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.

With the option of being pre-certified for EMV, 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.

Summary on secure mobile payments alternatives and the outlook for MFS

As a summary, there are five potential SEs for MFS:

(1) Passive and 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 especially for FIs, Other service entities, MNOs 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 that could be leveraged together with other MFS value chain stakeholders to open an additional service path for FIs 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.

For FIs 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. Therefore MNOs shoud now first decide what kind of position they want to claim in the MFS value chain. Other distribution channels of mobile handsets can leverage their position to collaborate with FIs – they can for instance bundle SEs to enhance the MFS offering on the market.

Handset vendors can leverage their position through eSEs or TMBs, either through collaborating with FIs or becoming a service provider themselves. The TMB can also be opened up to FIs 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 picture of the MFS Ecosystem shown in Figure 3.

The essential questions – which are also the key recommendations to the readers of the white paper – are the following:

(1) The stakeholders along the value chain have to define their positions. Do they want to be:
   - SEIs?
   - AIs?
   - 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 TSM or does a stakeholder want to hold this position in-house?

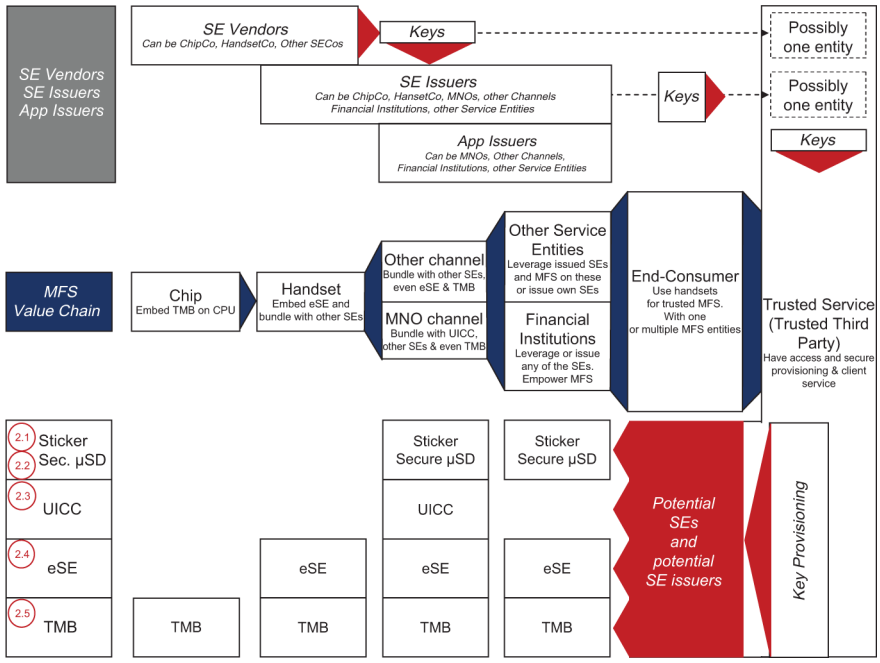

Figure 3.
Overview of value chain, stakeholders and SEs for MFS

(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. This is creating a major opportunity for the industry to finally bring mobile contactless payments towards the commercial stage.

However, further work is required to ensure a modular, open and standards based MFS ecosystem. It would be optimal if all AIs could have the opportunity to openly and independently offer their services to the mobile consumers without unnecessary complexities and inter-industry dependencies, leveraging different underlying SEs with standard processes and interfaces.

References

GlobalPlatform (2009a), "GlobalPlatform's value proposition for the public transportation industry", available at: www.globalplatform.org/documents/whitepapers/GP_Value_Proposition_for_Public_Transportation_whitepaper.pdf (accessed December 6, 2009).

GlobalPlatform (2009b), "The GlobalPlatform Value Proposition for Identity Management", available at: www.globalplatform.org/uploads/GP_White-Paper_IdentityMGMT_justified.pdf (accessed December 6, 2009).

GSM Association (2008), "GSMA calls for Pay-Buy-Mobile handsets", available at: http://gsmworld.com/newsroom/press-releases/2008/2090.htm#nav-6 (accessed January 12, 2010).

iSuppli (2008), "Mobile handset shipments with micro SD/Micro SDHC", *Data Flash Market Tracker*, Q3/2008, supplied via SD Association.

Mobey Forum (2005), "Security element technical analysis", (executive summary), available at: http://mobeyforum.org/files/Mobey%20Forum%20Security%20Element%20Analysis%20Summary%202005.pdf (accessed December 6, 2009).

Mobey Forum (2008), "Best practices for mobile financial services, enrollment business model analysis", available at: http://mobeyforum.org/files/bestpractice/Best%20Practices%20for%20MFS%20Enrolment%20Business%20model%20analysis%20final.pdf (accessed December 6, 2009).

Mobey Forum (2009a), "Global Overview of commercial implementations and pilots of NFC payments during 2009". article for globalsmart.com – Smart Card Technology International, available at: http://mobeyforum.org/ (accessed February 5, 2009).

Mobey Forum (2009b), "Why aren't banks rushing for NFC payments?", available at: http://mobeyforum.org/ (accessed February 5, 2009).

SD Association (2010), "SD Association celebrates 10 years of innovation at CES", available at: www.sdcard.org/press/SD_Celebrates_10_Years_of_Innovation_at_CES_2010.pdf (accessed January 10, 2009).

Further reading

Electronic Storage (2006), "Removable memory cards: not just a flash in the pan", available at: www.oto-online.com/pdf/oto_download/2006/06/OTO_June_P5254_MemoryCards.pdf (accessed December 6, 2009).

Informa (2009), *Informa Telecoms and Media: Mobile Distribution and Retail*, 6th ed., Informa, St Hellier.

Mobey Forum (2002), "Preferred payment architecture: local payment", available at: http://mobeyforum.org/files/Local%20Payments%20Discussion%20Document%201.0.pdf (accessed December 6, 2009).

Mobey Forum (2003), "Mobey Forum white paper on mobile financial services", available at: http://mobeyforum.org/files/Mobey%20Forum%20White%20Paper%20on%20Mobile%20Financial%20Services%20v1_14.pdf (accessed December 6, 2009).

Mobey Forum (2006), "Mobile financial services - business ecosystem scenarios and consequences", available at: http://mobeyforum.org/files/Mobey%20Forum%20MFS%20Business%20Ecosystem%20Summary.pdf (accessed December 6, 2009).

PrimeLife (2008), "D 6.2.1 infrastructure for trusted content", available at: www.primelife.eu/images/stories/deliverables/d6.2.1-infrastructure_for_trusted_content-public.pdf (accessed December 6, 2009).

PrimeLife (2009), "Identity management infrastructure protocols for privacy-enabled SOA", available at: www.primelife.eu/images/stories/deliverables/h6.3.1-requirements_for_privacy_enhancing_soas-public.pdf (accessed December 6, 2009).

Corresponding author

Liisa Kanniainen can be contacted at: liisa.kanniainen@nordea.com