About the GSMA

The GSMA represents the interests of mobile operators worldwide. Spanning more than 220 countries, the GSMA unites nearly 800 of the world's mobile operators with 250 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and Internet companies, as well as organisations in industry sectors such as financial services, healthcare, media, transport and utilities. The GSMA also produces industry-leading events such as Mobile World Congress and Mobile Asia Expo.

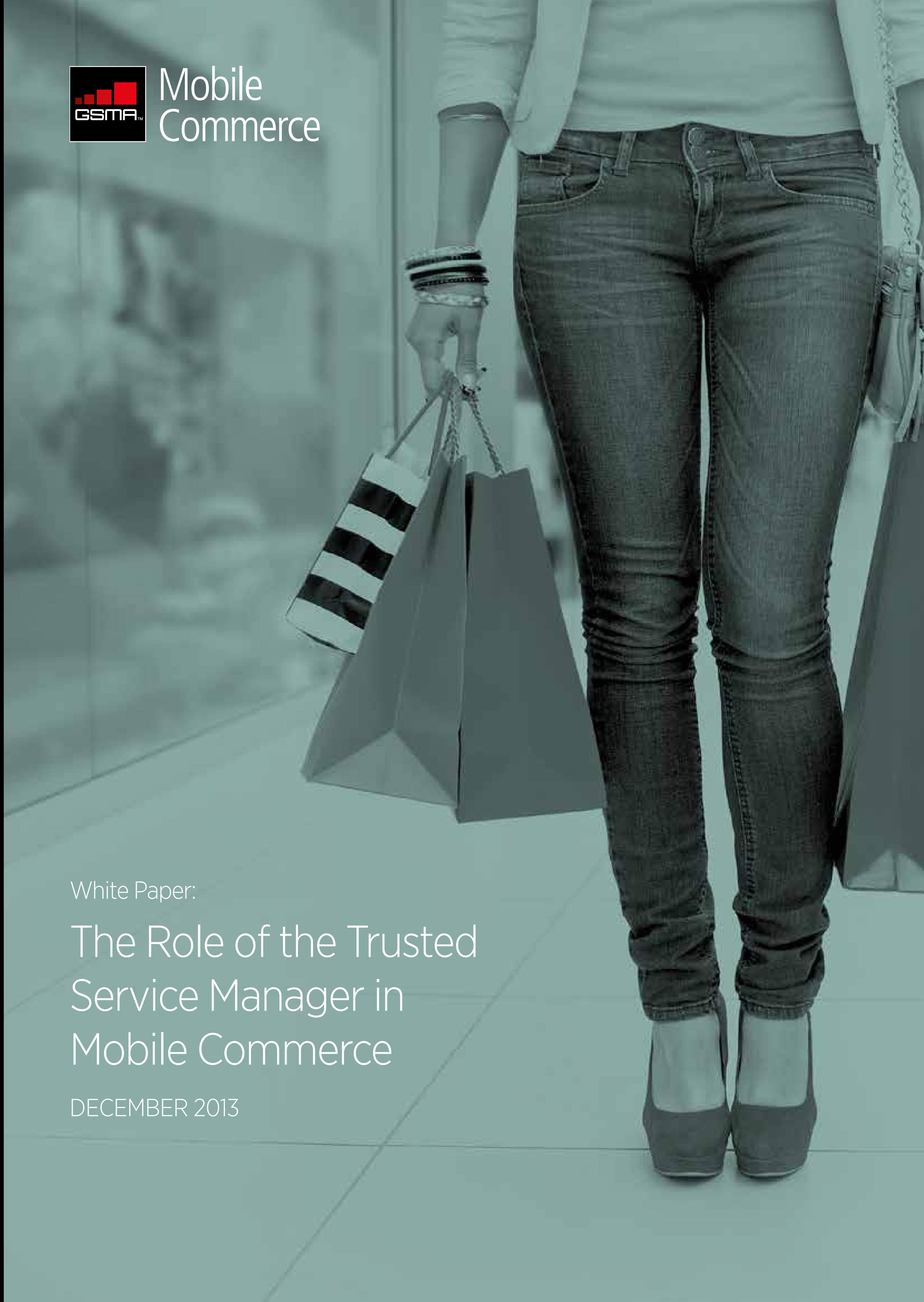
Mobile
Commerce

For more information, please visit the GSMA corporate website at www.gsma.com

Follow the GSMA on Twitter: @GSMA

GSMA London Office
T +44 (0) 20 7356 0600

DECEMBER 2013



Mobile
Commerce

White Paper:

The Role of the Trusted Service Manager in Mobile Commerce

DECEMBER 2013

CONTENTS

1.

Introduction

This paper concerns the role of the trusted service manager (TSM) in managing a new range of *secure card emulation* services for the mobile customer, supporting the use of the mobile phone for contactless transactions of value, such as payment and transit. A TSM mediates between service providers and MNOs.

This paper considers the range of options for the TSM role – both technical and commercial. It also explores the trade-off between expediency on the one hand and full flexibility and scalability on the other.

Although a sophisticated ecosystem of connected participants is required to link multiple service providers to multiple MNOs globally and satisfy the full range of security and service lifecycle requirements, there are simpler and more expedient deployments available to MNOs who wish to launch their first tranche of near field communication (NFC) based services.

The paper aims to help an MNO make an informed decision about their strategy and about sourcing TSM services.

This paper has been produced with significant input from the following suppliers of TSM services:

- Gemalto
- Giesecke & Devrient
- Oberthur

Structure

1. **The Introduction** introduces the paper and the broad subject area.
2. **The Executive Summary** presents the main messages of the paper.
3. **The Mobile Secure Services Ecosystem** gives a more detailed description of the roles of TSMs within the broader ecosystem.
4. **Deployment Models** explains the potential deployment models in more detail.
5. **Technology** gives more detail on the technology.

Reference Documentation: Requirements and Specifications

The joint GSMA and European Payments Council publication, *'EPC – GSMA: Mobile Contactless Payments Service Management Roles: Requirements and Specifications: Doc EPC 220-08, Ver 2.0, October 2010'*[1] is an important reference document for the role of the TSM in managing secure card emulation services.

This TSM Guidelines White Paper is higher level than the joint EPC-GSMA paper, but it develops some aspects further to reflect recent developments in established practices:

- The EPC-GSMA white paper defines service management roles for the secure element issuer (MNO) and the service provider, or their 'subcontractors'. This idea is now extended to cover independent service management actors, such as joint ventures or trusted third parties;
- The EPC-GSMA white paper sets out a range of options. This paper helps to navigate them.

[1] Source: www.gsma.com/mobilecommerce: *EPC – GSMA: Mobile Contactless Payments Service Management Roles: Requirements and Specifications: Doc EPC 220-08, Ver 2.0, October 2010*

New enabling technology, new services

Together, mobile and contactless connectivity are making a wealth of new services available on smartphones. If a consumer touches or taps their handset to a suitable NFC touchpoint, several things can happen. The smartphone's browser can be prompted to open a particular website. Or the smartphone can interact with another device, such as a home entertainment system to play or manage audiovisual content. If the touchpoint is a retail payment terminal or a metro gate, the phone can emulate a payment card or transit ticket respectively. Such card *emulation* requires an application to interact with the reader: This could be an ordinary handset application, known as an applet, or a special type of application stored in a secure element, such as the SIM Card or UICC (universal integrated circuit card), within the mobile phone, providing greater security. The core function of a TSM is to mediate in issuing and managing a secure service on a mobile device – getting the customer's service credentials onto the secure element. Most of the guidelines in this paper are about this core function.

A 'card' in this context is a secure and portable virtual card representing the entitlement of a customer to a particular service – the examples above being a payment service and a transit service. The individual is typically the customer of many service providers, as well as their MNO. The mobile customer can use NFC to interact with service providers in several different ways, whereas TSMs will be mediating between the service providers, the MNOs and their customers to enable the service.

Connecting service providers to their mobile customers

This paper introduces a range of options for how MNOs and service providers can connect via a TSM, and advises on implementation.

The types of interaction between a service provider and its customer are as follows (see Fig. 1):

1. Issuing and managing the service (by the service provider): Getting the customer's service credentials on to the secure element, and amending or 'stopping' them as needed – equivalent to creating and sending a plastic card.
2. The customer's self-service management of their account, or other service, using the handset: In part this is comparable to online self-service, and in part it is 'all new' for mobile secure services – for example, activating and deactivating services.
3. Routine service usage: Carrying out everyday transactions such as payment or validating a travel ticket, by tapping on an NFC reader or by using secure online services.

In addition the mobile application (wallet) provided by the MNO or service provider (SP) gives a user-friendly method to interact with the applets stored on the SIM.

HOW A SERVICE PROVIDER, A TSM AND A MOBILE CUSTOMER INTERACT

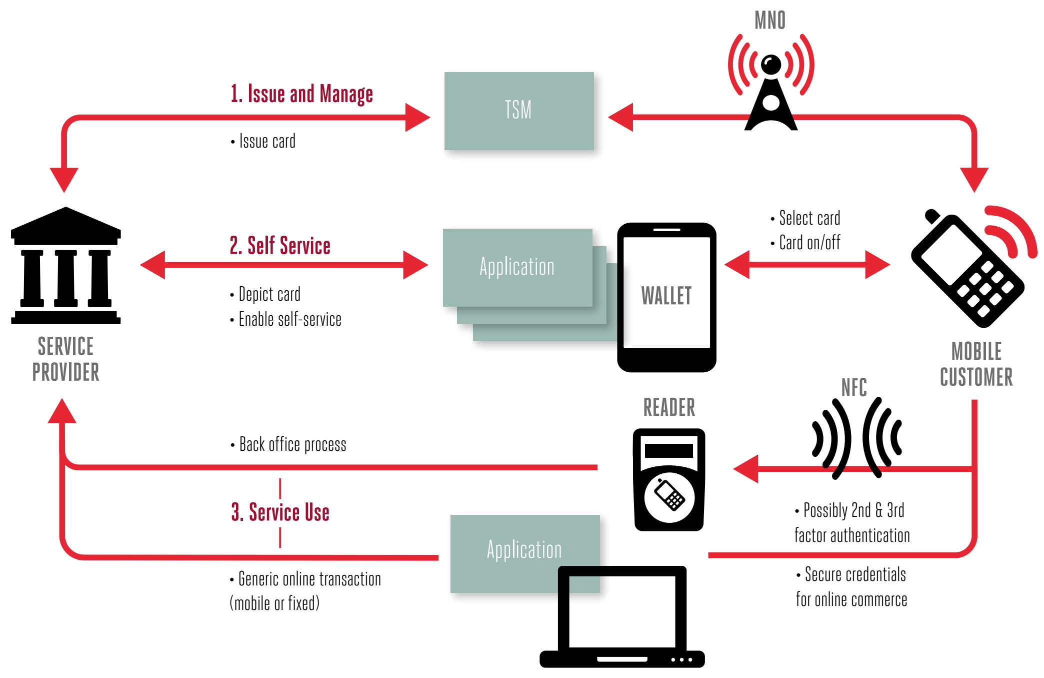


Figure 1

2.

Executive Summary

Business strategy

For an MNO wishing to bring secure services management to their customers, the first step is to consider their own place in the value chain and to form a business strategy for this new commercial space.

Market maturity, the position of competitors and the distance of its planning horizon (short-term or long-term) will also influence an MNOs TSM choices. As markets mature, TSMs may specialise in serving a particular class of service provider, such as payment, transport, retail (loyalty and coupons), identification (e-signature, public services), healthcare, access control and more. In a mature market, such decisions may be made independently of MNOs, but in a developing market an MNO might influence early TSM structures.

Roles of TSMs

In the provisioning and managing of secure services, the role of the TSM is of central importance. The TSM acts as the connection point between service providers, such as banks, transit operators and merchants, and the MNOs issuing the secure element (SE).

The utilisation of over-the-air channels by the TSM provides:

- Life Cycle Management of security domains on the secure element in order to provide secured blocks of space for services.
- Life Cycle Management of applets on the security domain of a secure element.
- The ability to update the secure element with access control hash for service provider applets to work on newer devices.
- The recovery mechanisms to the MNO and service provider utilising the service in case of outages.
- The ability to report to each service provider on the amount of space used and the number of services running.

In summary, the TSM infrastructure can be regarded as a 'general purpose over-the-air (OTA) personalisation system' for secure element applets and also a 'generic life-cycle manager' of the provisioned applets.

> As markets mature, TSMs may specialise in serving a particular class of service provider

THE ROLE OF THE TSM CAN BE SPLIT IN TWO

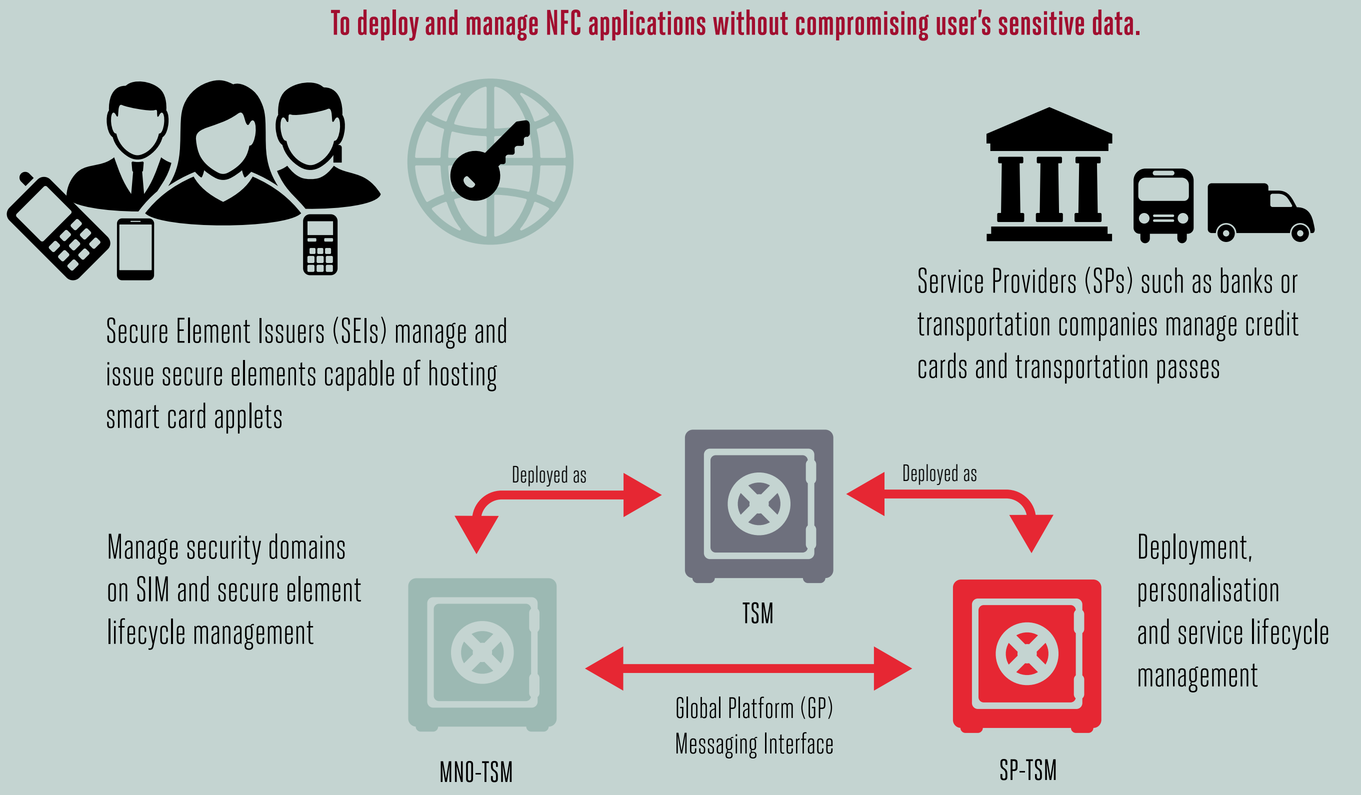

To deploy and manage NFC applications without compromising user's sensitive data.
Secure Element Issuers (SEIs) manage and issue secure elements capable of hosting smart card applets
Service Providers (SPs) such as banks or transportation companies manage credit cards and transportation passes
Deployed as
Deployed as
TSM
Manage security domains on SIM and secure element lifecycle management
Deployment, personalisation and service lifecycle management
Global Platform (GP) Messaging Interface
MNO-TSM
SP-TSM

Figure 2

In a typical deployment, the TSM role is split in two – the service provider TSM and the secure element issuer TSM. The latter can be referred to as a mobile network operator TSM (MNO TSM), where the MNO issues the secure element (SIM/ UICC Card). This separation of TSMs reflects the typical business model:

1. The MNO provides banks, retailers, corporates, mass transit authorities and other service providers with secure access to the secure element and related life cycle management; simply put, it allocates security domains on its secure element to service providers.
2. Service providers use the security domain they are allocated to provision and manage their own end-user services securely, with or without the MNO, based on the capabilities and commercial agreements between them, MNO and/or any other third party being able to get access to the secure and sensitive contents of the service providers' applets.
3. The MNO TSM will provide the SP TSM with notifications related to the mobile subscriber's service and their life cycle.

Commercial relationships

MNOs, service providers and TSM suppliers will need to establish commercial relationships (with each other and end-users) and/or trade off the costs against other expected benefits.

The TSM is an independent business entity and many types of company are entering this competitive market.

TSMs and the wallet

A 'wallet' is defined by the GSMA "*as an application on a mobile handset that functions as a digital container for payment cards, tickets, loyalty cards, receipts, vouchers and other items that might be found in a conventional wallet. The mobile wallet enables the user to manage a broad portfolio of mobile services from many different providers, and, in the case of NFC services, it provides the means of managing applets on the UICC.*"[2]

The importance of the wallet concept has grown significantly from the early days of secure NFC when the technology was driven by pilots typically involving just a single application and with no immediate need for the dynamic addition of new services. Now, with the rise of commercial launches, requirements for the wallet have changed dramatically. As TSMs continuously enable the dynamic provisioning of an increasing number of new secure services to the secure element, it is increasingly important that the chosen wallet also supports this dynamism. The depiction of a secure application (card image, with associated data) needs to be added dynamically to the wallet, in parallel with the secure delivery of the applet to the secure element.

As TSMs provide dynamic flexibility and online connectivity, enabling end-users to access their services at any time, service enrolment should be implemented accordingly. This could mean, for example, that enrolment of a mobile service is initiated from the handset – more specifically from its wallet through a service discovery service. Thus the wallet would typically need to support interaction with a service provider's back-end systems to have the new service provisioned in a matter of minutes. A wallet server is now generally used to manage the contents – typically the depiction of services – of a wallet on the handset.

The wallet plays an important role in controlling the services on the secure element. The MNO, as the issuer of the secure element, has an interest in controlling the applications and wallets that can access it. For this reason, as well as broader commercial reasons, many MNOs and service providers wish to provide their own wallet.

In this highly innovative and competitive market, wallets are available from a variety of suppliers some offering a 'white label' wallet and wallet server for consideration by MNOs as one of their deployment options.

It is technically possible to authorise a wallet to connect to any set of applets, and it is possible to have more than one wallet accessing the same secure element. An MNO, as the secure element issuer (SEI), may grant access to service providers to have their own handset applications acting partially in the role of a wallet – for example a multi-function application from a bank, retailer or transport provider. This may lead to a situation where the end-user has several wallets on their handset. In this case, the wallet issuers need to agree on general rules on co-existing wallets, especially with respect to declaring the 'top of wallet' payment card (or other card category) in order to offer offering the best user experience to the end-user and avoid any drop-out in the use of the service. The MNO, in agreement with the service providers owning the other wallet(s), needs to develop anti-contention disciplines for multiple wallets (there is no standard for this). At the time of writing, this matter requires further research.

In summary, the wallet:

- Is an integral part of any secure mobile services ecosystem.
- Provides a user interface to secure mobile services.
- Can have a central role in various key processes, especially in enrolment, that may be the decisive factor for the end-user when considering whether or not to adopt a specific service.

> As TSMs provide dynamic flexibility and online connectivity, enabling end-users to access their services at any time, service enrolment should be implemented accordingly.

[2] Source: www.gsma.com/mobilecommerce: The Mobile Wallet, Version 1.0, September 2012 and NFC Core Wallet Requirements and Core Package File Technical Proposal, Version 1.0, 10th October 2012.

Variations in the TSM set-up

This section summarises the main architectural choices open to MNOs.

Essentially MNOs can choose a common approach or reach an agreement to offer a pragmatic solution like a TSM Hub:

- The common approach yields longer term benefits, as the ecosystem matures, through the use of a standards-based architecture. But more effort is required and it involves greater interdependence on other ecosystem participants.
- A pragmatic approach offering a TSM Hub to service providers can be fast to deploy, and more controlled, but involves compromise and collaboration between MNOs, which may need to be resolved as services mature.

TSMS CAN BE HOSTED, LICENSED AND/OR SHARED BASED ON AN MNO'S DECISIONS AND ASSESSMENTS

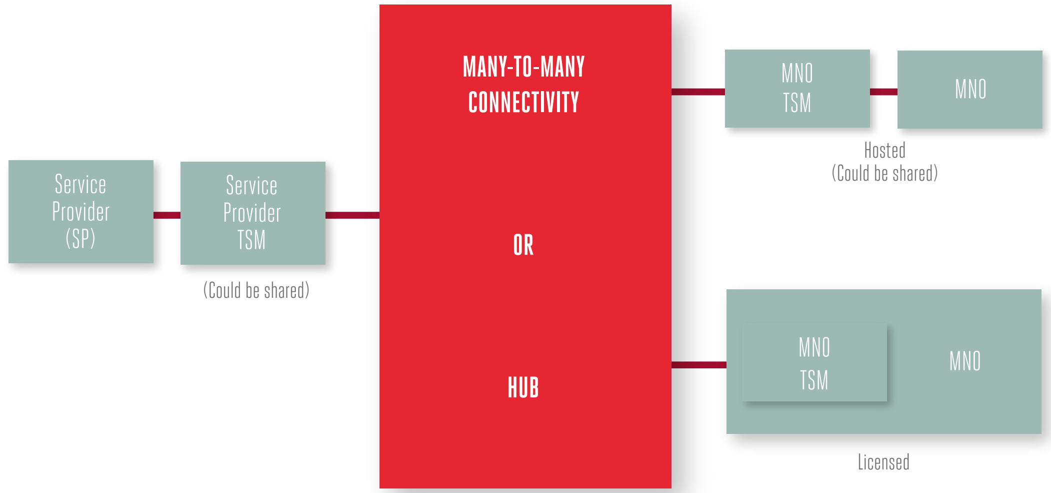


Figure 3

The standards-based deployment model is as follows:

- Fully modular and technically independent service provider TSMs and MNO TSMs. In this case:
  - MNO or service provider TSMs are either hosted or licensed. A hosted solution may make it easier to achieve EMV certification taking into account the mode used to deploy the service, as certification would be part of the hosted TSM's service.
- Shared TSMs may be set up for commercial reasons (within legal/regulatory constraints), but care is needed that they do not become an architectural constraint. In this case:
  - Service providers may choose to share TSMs within a market (e.g. one for transport, one for small retailers).
  - MNOs may also choose to share TSMs.
  - Confidentiality of information can be maintained in a shared environment.
- The messaging protocol for TSM-TSM interactions should be able to support both GlobalPlatform[3] (GP) and, if required, locally adopted standards (such as the Association Française du Sans Contact Mobile (AFSCM[4]) v2). Global Platform and AFSCM have been working together to include the requirements and specifications done by AFSCM within Global Platform in order to reach a common standard.
- Security domain provisioning might be through dynamic allocation (rather than pre-issued) using a secure mechanism. Even if pre-issuance (factory allocation) is selected for rapid early deployment, support for dynamic allocation should be established for future use.
- Commercial relationships can be decided independently of technical relationships and can be established directly between service providers and MNOs.

[3] GlobalPlatform (GP) System Messaging Core covers the following relations: • Between the Service Provider and the Trusted Service Manager • Between the Trusted Service Manager and the Mobile Network Operator • Between the Trusted Service Manager and the Secure Element Provider

[4] Association Française du Sans Contact Mobile (AFSCM) was established in April 2008 by Bouygues Telecom, Orange and SFR as a non-profit organisation to foster the development of mobile contactless services. AFSCM objective is to support the inception of new contactless services for mobile phone users.

A SERVICE PROVIDER TSM INTERACTS WITH MULTIPLE MNO-TSMS

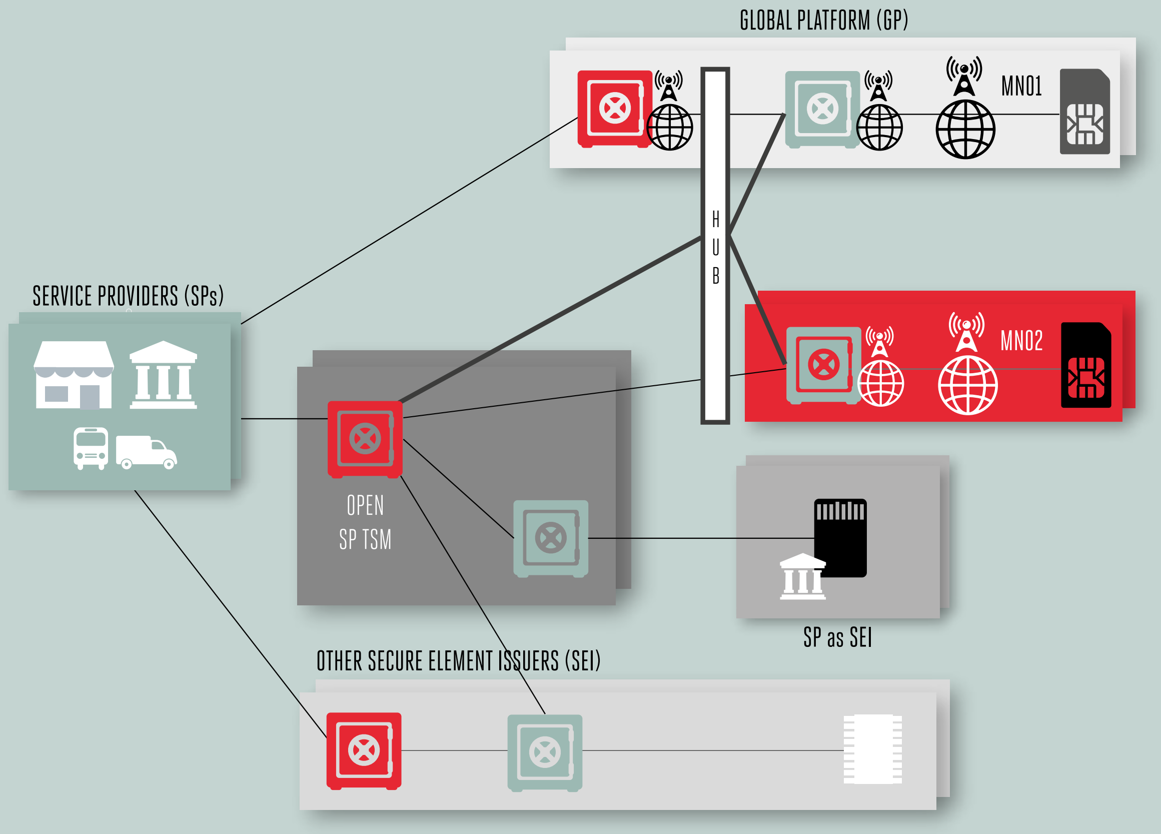


Figure 4

For pragmatic reasons, such as speed of launch, greater control of the technical environment and/or greater control of commercial relationships, some market participants might adopt pragmatic deployment models.

Potential variations on the standard deployment model include:

- Deployment by the service provider of a TSM service directly or both elements (service provider TSM and MNO TSM) combined in one single entity.
- The use only of a locally adopted messaging standard (such as AFSCM).
- The use of a locally adopted messaging standard (such as AFSCM).
- A pre-issued or 'factory built' security domain.

Another possibility is that a public or governmental body or an independent commercial enterprise (an aggregator) sets up a common service provider TSM to kick-start market activity. Alternatively, this common TSM could be set up by the initiating MNOs in which case care will be needed to ensure compliance with local legal, regulatory and competition constraints.

The actual choice of model will be governed in part by the circumstances in the market – especially other deployments, other decisions already made, and the intentions of other MNOs. However, any non-standard/non-strategic deployment should consider the migration path to the strategic model, and the related costs and challenges (e.g. using the GSMA document on MNO-SP Interfaces[5], to plan the migration from AFSCM to GlobalPlatform). Note that the migration away from early shared TSMs will typically be gradual, as shared TSMs are a valid possibility within the strategic modular architecture.

[5] Source: www.gsma.com/mobilecommerce: NFC Mobile Network Operator – Service Provider Interface: Business Process Implementation Guidelines using GlobalPlatform Protocols, Version 1.0, 30 July 2012

Choice of management modes

A service provider has a choice of detailed mechanisms by which it installs its applet, and manages it, on the security domain within the secure element. These management modes are known as simple, delegated or dual – see section 4 for a description of these modes.

The choice of management mode is made independently for each secure domain on the secure element (for example, Payment Network 1, Payment Network 2, Transport Ticket, Loyalty Card) taking into account the following factors:

- Each security domain potentially has a different service provider TSM.
- The choice of management mode would reflect how the parties see their technical relationship – there is no 'quick rule' or 'right choice'.
- The management mode would in practice be decided as part of the negotiation of how the entire end-to-end process works, from the service provider, to the service provider TSM, to the MNO's TSM.
- If EMV certification is required for an applet, and if simple mode is adopted, then the MNO TSM might need to be EMV certified. The same principle would apply in the case of any other industry-wide certification regime. For this reason, delegated mode is popular for payment applications and may well, in future, become popular for other schemes requiring certification.

Delegated mode is popular for payment applications, and may well, in future, become popular for other schemes requiring certification

The future

The structure of two TSM types (service provider, mobile operator) is a prerequisite for fully flexible connectivity across international borders. However, global scalability could be achieved by the development of a number of centralised TSM hubs rather than a proliferation of bilateral relationships.

A service provider has a choice of detailed mechanisms by which it installs its applet, and manages it, on the security domain within the secure element.

3.

The Mobile Secure Services Ecosystem

The roles of the TSM

Earlier in this paper, the TSM infrastructure was introduced as a 'general purpose OTA personalisation system' for secure element applets and also a 'generic life-cycle manager' of the provisioned applets. As discussed in section 2, the TSM role is logically split into two parts – the service provider TSM and the SEI or MNO TSM.

THE ROLE OF THE TSM CAN BE SPLIT IN TWO

To deploy and manage NFC applications without compromising user's sensitive data.

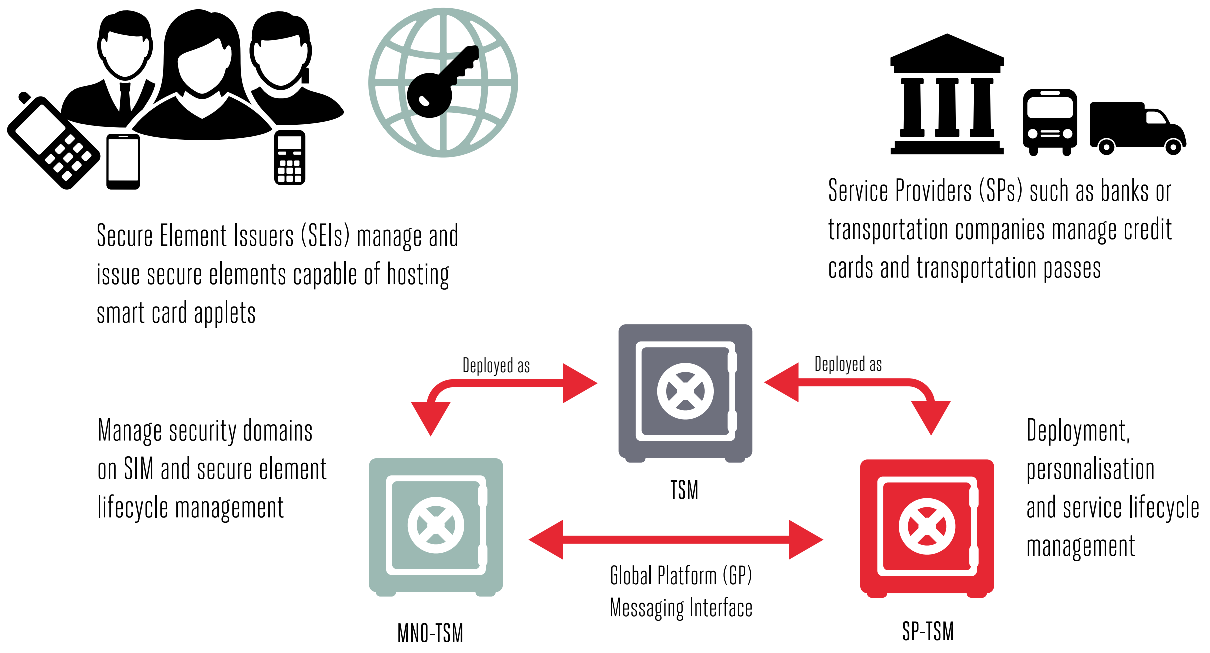

Secure Element Issuers (SEIs) manage and issue secure elements capable of hosting smart card applets
Service Providers (SPs) such as banks or transportation companies manage credit cards and transportation passes
Deployed as
Deployed as
TSM
Manage security domains on SIM and secure element lifecycle management
Deployment, personalisation and service lifecycle management
Global Platform (GP) Messaging Interface
MNO-TSM
SP-TSM

Figure 2

The two TSM types have distinct roles defined in the GlobalPlatform Messaging Specification (see section 5 for the referenced documents). These are further detailed below:

- Service provider TSM: This may be deployed by a service provider or as a shared service towards many service providers by a trusted third party acting as an 'aggregating' service provider TSM. The service provider TSM deals with the service lifecycle operations, from the service provider's perspective – deploying the service, personalisation, locking/unlocking, etc. It integrates with the service provider's IT systems to facilitate simple extension of their existing provisioning processes to take in NFC support. The service provider TSM can implement its own OTA system for communication with the mobile device and secure element, but it is more likely to communicate with an MNO TSM to do this.

The use of a standard GlobalPlatform messaging interface between these TSMs facilitates the connection of different service provider TSMs to different MNO TSMs (e.g. several payment services being offered to four different MNO subscribers). The exchange of GlobalPlatform messages also needs to be as harmonised as possible to facilitate this interconnection. This is the purpose of the GSMA document on MNO-SP Interfaces[6].

- MNO TSM: This TSM deals with the management of the secure element, securely allocating space (a security domain), deploying applets or enforcing aspects of the service lifecycle, on behalf of the service provider TSM. It will typically implement the OTA infrastructure, or mechanism for communication with the secure element.

THE DIFFERENT ELEMENTS OF A TYPICAL NFC ECOSYSTEM

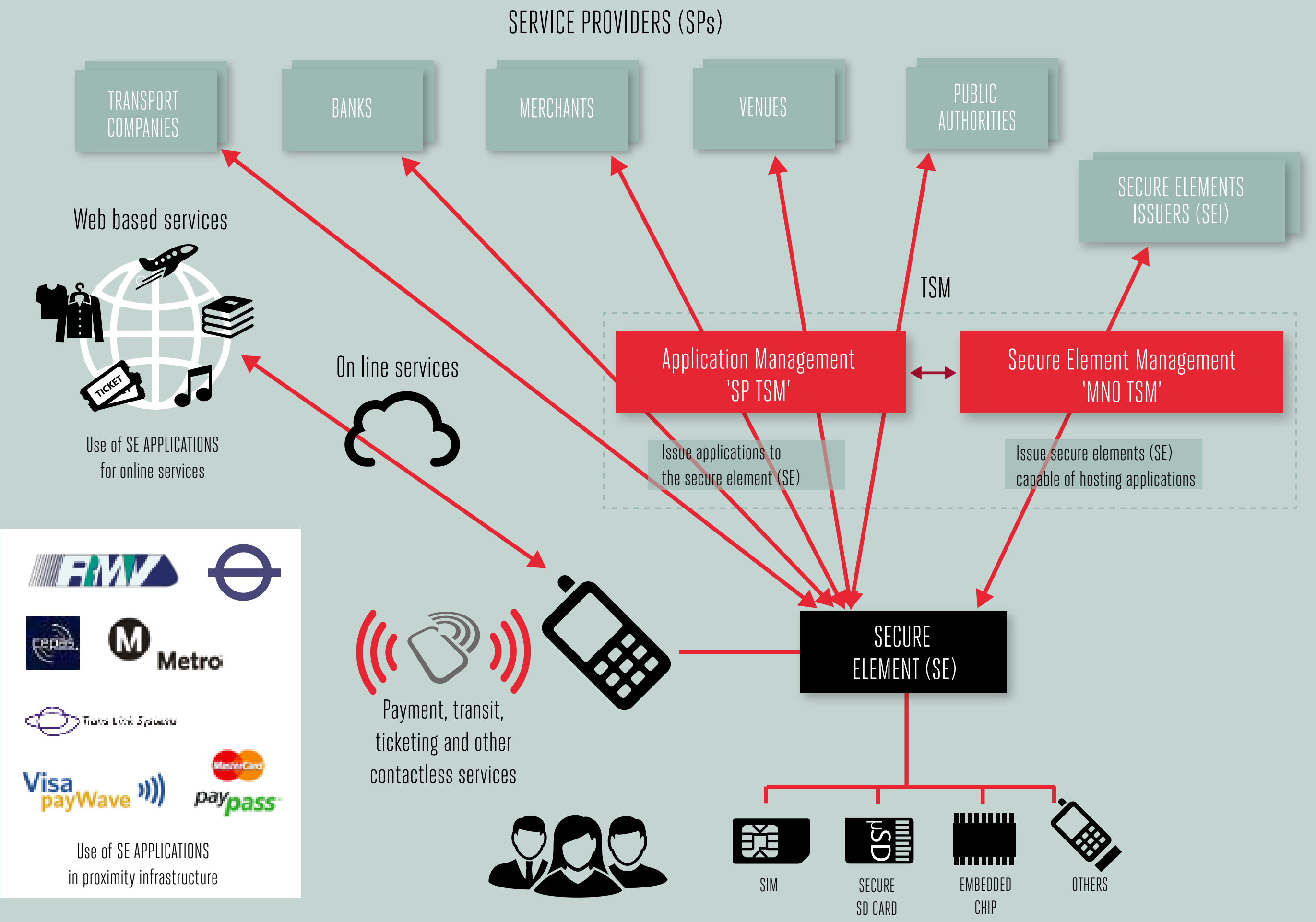

SERVICE PROVIDERS (SPs)
TRANSPORT COMPANIES
BANKS
MERCHANTS
VENUES
PUBLIC AUTHORITIES
SECURE ELEMENTS ISSUERS (SEI)
Web based services
TICKET
Use of SE APPLICATIONS for online services
On line services
TSM
Application Management 'SP TSM'
Secure Element Management 'MNO TSM'
Issue applications to the secure element (SE)
Issue secure elements (SE) capable of hosting applications
SECURE ELEMENT (SE)
RMV
cepas.
Metro
Visa payWave
MasterCard
paypass
Use of SE APPLICATIONS in proximity infrastructure
Payment, transit, ticketing and other contactless services
SIM
SECURE SD CARD
EMBEDDED CHIP
OTHERS

Figure 5

[6] Source: www.gsma.com/mobilecommerce: NFC Mobile Network Operator – Service Provider Interface: Business Process Implementation Guidelines using GlobalPlatform Protocols, Version 1.0, 30 July 2012

In a typical NFC deployment, banks, transit companies and other service providers utilise a managed TSM service provided by a trusted third party.

In a typical NFC deployment, banks, transit companies and other service providers utilise a managed TSM service provided by a trusted third party. End-users will typically need a mobile handset with a secure element. Whereas a bank, for example, may have traditionally used its internal customer provisioning system to initiate the provisioning of a payment card, these requests would now be securely channelled via the service provider TSM to carry out the provisioning towards the NFC device and secure element. The TSMs will then manage the following processes:

- The service provider TSM requests the MNO TSM to check the eligibility of the subscriber's handset/device, secure element and subscription to get access to this service.
- Once the checks are complete, the service provider TSM may request the MNO TSM to allocate a security domain, or secure area on the secure element on which the service-related applet and data can be deployed.
- Part of this security domain provisioning process would involve the service provider TSM negotiating secure end-to-end keys which would be used to ensure that all communication between the service provider TSM and the security domain created for this service is encrypted, and cannot be seen by the MNO TSM or any other party.
- The MNO TSM may, depending on the chosen deployment model (as defined in GlobalPlatform), carry out the operations towards the secure element on behalf of the service provider TSM, or may utilise a token/receipt mechanism to delegate the execution of many of the operations to the service provider TSM, while approving/monitoring these operations via the token/receipt.

During the lifecycle of the service, the MNO TSM will keep track of the status of the mobile device, and the secure element, and can provide notifications towards the service provider TSM in relation to different events, such as device lost, change of device, SIM change, and number (MSISDN) change and so on. Similarly, it can, based on a request from the service provider, or directly from the end-user, lock/unlock the NFC service, update software or configuration and delete or revoke the service.

Subject to the internal logic of each NFC service, the TSMs may also be used as a channel to update application specific parameters, such as resetting the offline counters of an EMV applet, unlocking the offline PIN or topping up value to a mass transit application. These services may be provided by application issuers and then managed OTA by TSMs, or they can be value add services provided by the service provider TSM.

HOW VALUE MIGHT FLOW WITHIN AN NFC ECOSYSTEM

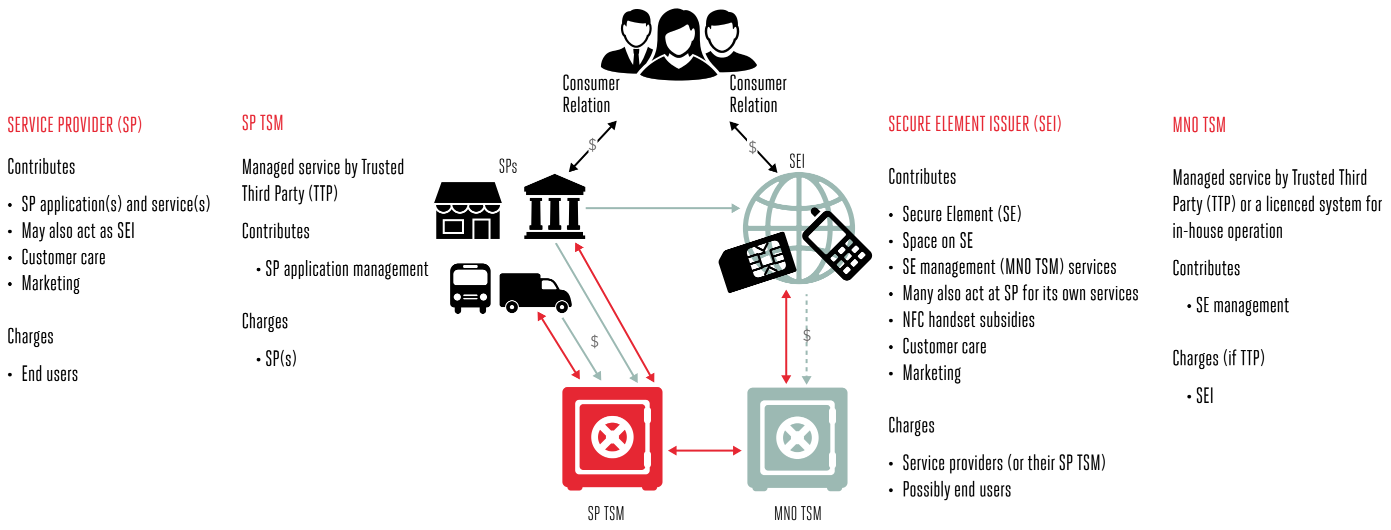


Figure 6

Potential business models for service providers and MNOs

The typical high-level business model and contributions by various parties are summarised in the figure above. (TTP refers to a trusted third party, who is trusted to provide these types of security-sensitive services requiring a strict service level agreement). Note that the MNO TSM can be operated in-house, in which case the MNO would either develop the MNO TSM software itself or purchase it from a vendor ('licensed solution'). However, in this business model description, a TTP acts as both the service provider TSM and MNO TSM, as this is a widely adopted model.

Service providers, such as banks, have direct relationships with consumers. Banks, transit authorities and other service providers could potentially charge consumers additional fees for contactless services or the business model can be based on cost savings, especially in the longer term, or the need to maintain or gain a competitive edge. In this case, service providers will offer and promote services to consumers and run customer care as part of their support function.

MNOs provide secure elements (such as the SIM), management of the secure element applets and (often) delivery of NFC handsets to the market. This role requires marketing and promotion, as well as customer care for consumers. MNOs have several potential revenue streams. One model is to charge service providers a fee for space on the secure element. Another model is to charge consumers a fee for services enabled by secure element issuers.

TTPs operating a TSM service expect to get paid for establishing the service readiness and for actual TSM services, such as the download and personalisation of contactless applications.

> MNOs provide secure elements, the management of the secure element applets and delivery of NFC handsets to the market.

4.

Deployment Models

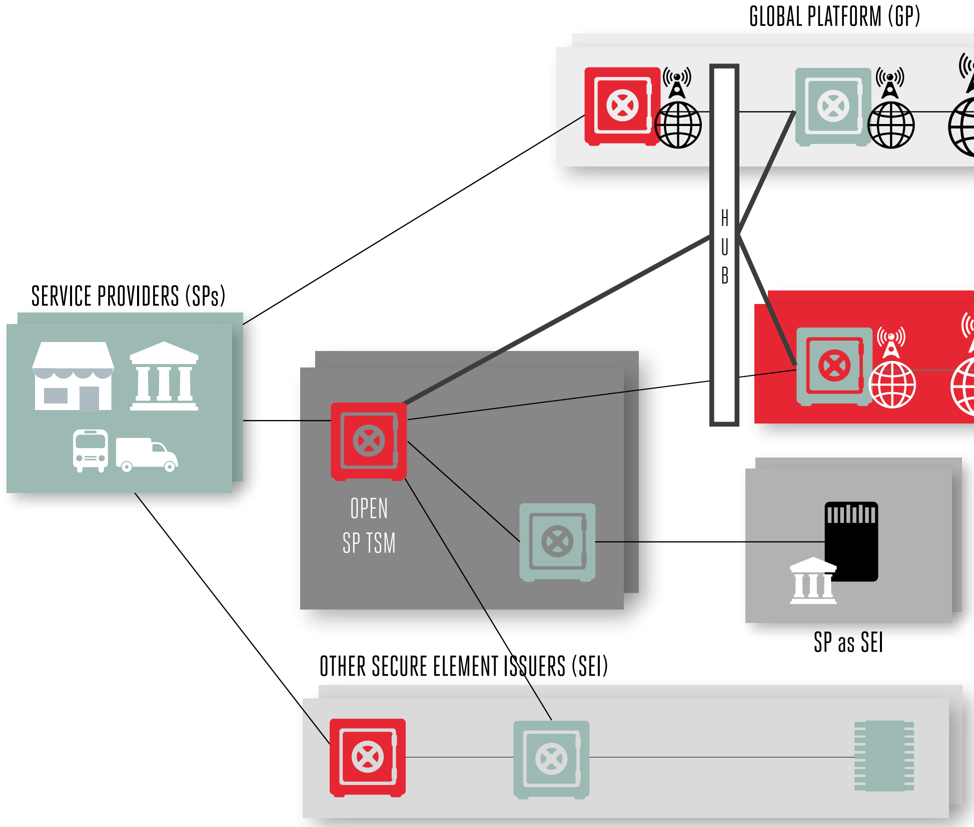
TSM Deployment

Certain trends and distinct approaches are emerging in the TSM marketplace.

MNOs typically opt for one of two TSM roles:

1. Delivering the secure element (SIM/UICC) with related MNO TSM services.
2. As above, but also acting as a service provider TSM for various service providers.

TRENDS IN THE TSM DEPLOYMENT MODEL



TRENDS:

- Both SP TSM and MNO TSM as a managed service for one or several stake holders
- Especially bank and transit segments look for open, SE and SEI neutral SP TSM that is best positioned to provide access to total market
- Joint venture initiatives, subject to antitrust regulation

Figure 7

As a service provider typically looks for the widest possible user base for its services, it aims to access as widely as possible the secure elements in the market place. Therefore, at least in the longer run, service providers wish to be able to utilise secure elements run by all or most MNOs. Some service providers may also opt to issue non-UICC secure elements, such as microSDs or accessories, by themselves or working with other SEI MNOs emerging in the market.

For the same reasons, stakeholders in the NFC ecosystem are often looking for co-operation (commercial and technical) to facilitate the simpler, faster and more cost-effective deployment of a variety of NFC services, avoiding fragmentation. As an example, MNOs may consider co-operating to provide a single point of interface, providing simplified access to all participating MNOs' secure elements and services.

As a service provider typically looks for the widest possible user base for its services, it aims to access as widely as possible the secure elements in the market place.

Potential TSM business models

Potential TSM business model options include:

The MNO acts as the service provider TSM and the MNO TSM and it provides the secure element.
This approach offers one-stop-shopping for service providers, but service providers will need one TSM for each MNO.

THE MNO TAKES ON THE ENTIRE TSM ROLE

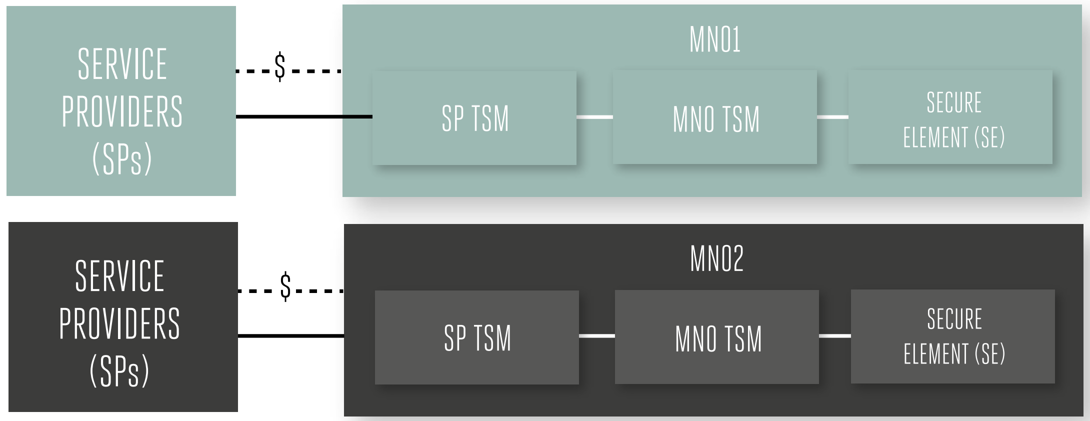


Figure 8

The service provider TSM acts as a technical aggregator and the MNOs sell their services independently. In this case, the service provider needs to make a contract with one service provider TSM only, but enter into several MNO contracts.

THE SERVICE PROVIDER TSM ACTS AS A TECHNICAL AGGREGATOR

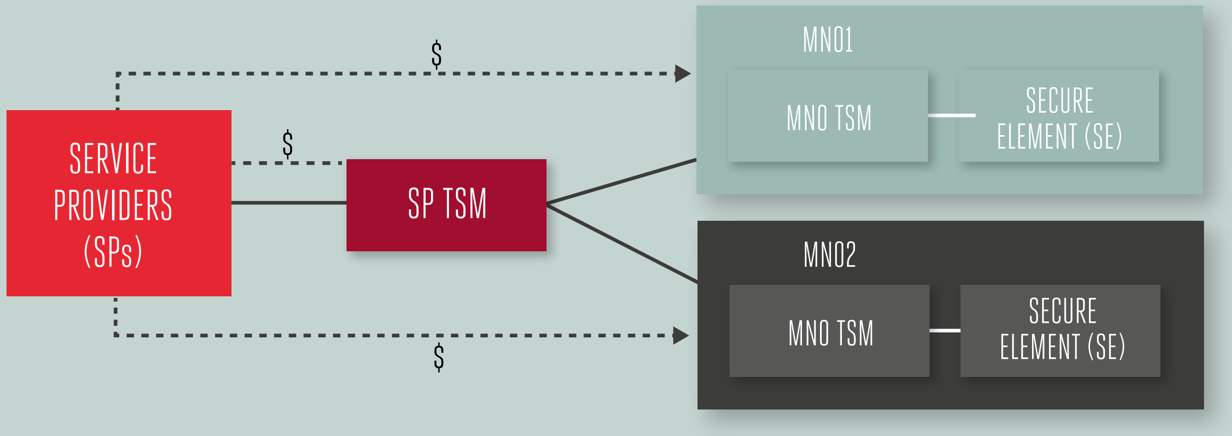


Figure 9

The service provider TSM acts as a technical and business aggregator selling its services and reselling MNO services as a package. This approach provides one-stop-shopping for service providers, but requires contractual arrangements between service providers TSMs and MNOs.

THE SERVICE PROVIDER TSM ACTS AS A TECHNICAL AND BUSINESS AGGREGATOR

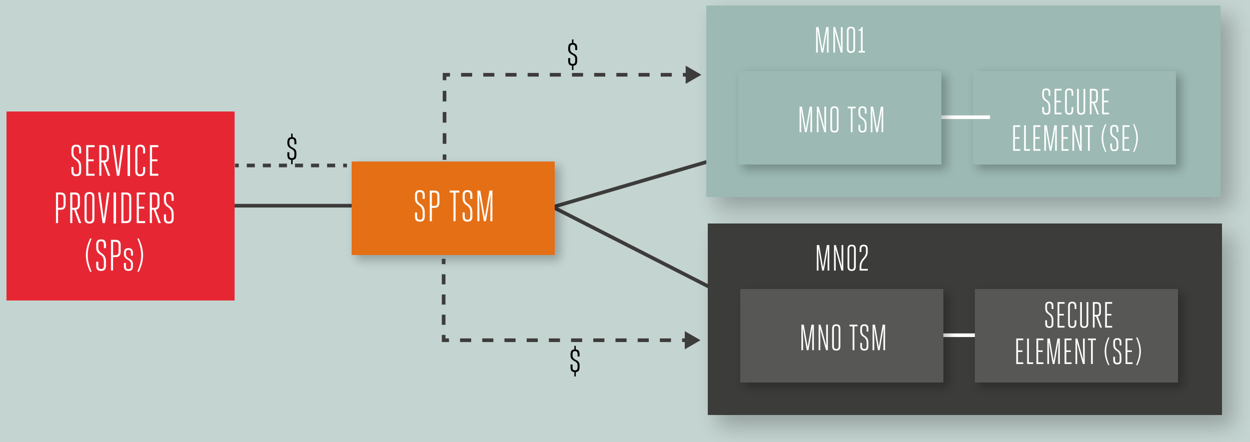


Figure 10

Management modes

As outlined in section 2, there are several mechanisms by which the service provider can install its applet, and manage it, on the security domain within the secure element. These are known as management modes, defined by GlobalPlatform (see section 5 for the referenced documents). The management modes are known as simple, delegated or dual.

Simple mode is where the MNO TSM performs the card content management upon request from the service provider:

- The service provider delegates full management of its application to a MNO TSM.
- The MNO TSM is responsible for card content management – carrying out both security domain management and secure element applet management.
- The service provider TSM requests these operations are carried out by the MNO TSM.
- The service provider is responsible for the data personalisation of its applet through the MNO TSM.
- In the case of EMV payment applet, the MNO TSM might need to be EMV certified as part of the end-to-end process (this is not required for delegated mode, which 'passes through'). The same principle would apply in the case of any other industry-wide certification regime.

Delegated mode is where card content management is performed by the service provider TSM:

- Each operation requires a pre-authorisation, in the form of a token, from the mobile operator.
- The service provider TSM can install the secure element applet directly, or through the MNO TSM, using the token to gain access (with a check/respond protocol to control the process).
- The MNO TSM still maintains responsibility for security domain management (allocating the space).
- In this case, the infrastructure certification is the responsibility of the service provider TSM.

Dual mode is where card content management could be performed by both the MNO and the service provider TSM on their own reserved domains of the secure element:

- In this mode, the secure element must have at least two security domains, one dedicated to the MNO and one to the service provider TSM. The MNO is able to offer specific space for the SP's secure domain based on the rules to manage the memory allocated for a secure domain specified by GlobalPlatform.

Irrespective of the modes, the subscriber lifecycle management is the responsibility of the MNO and the application management is performed by the service provider TSM.

With respect to existing deployments, it may be that some TSMs may not be able to comply with the full range of GlobalPlatform technical standards. In that case, the TSM may not have the flexibility to accommodate an alternative mode.

> Irrespective of the modes, the subscriber lifecycle management is the responsibility of the MNO and the application management is performed by the service provider TSM.

5.

Technology

The MNO TSM and service provider TSM lie at the heart of the NFC ecosystem. To meet demand for interoperability, these TSMs need to be compliant with a number of technical specifications and standards.

Interfaces specifications and standards

The illustration below highlights the MNO TSM and service providers TSM interfaces with their environment.

THE INTERFACES BETWEEN TSMS, SERVICE PROVIDERS, MNOS AND MOBILE HANDSETS

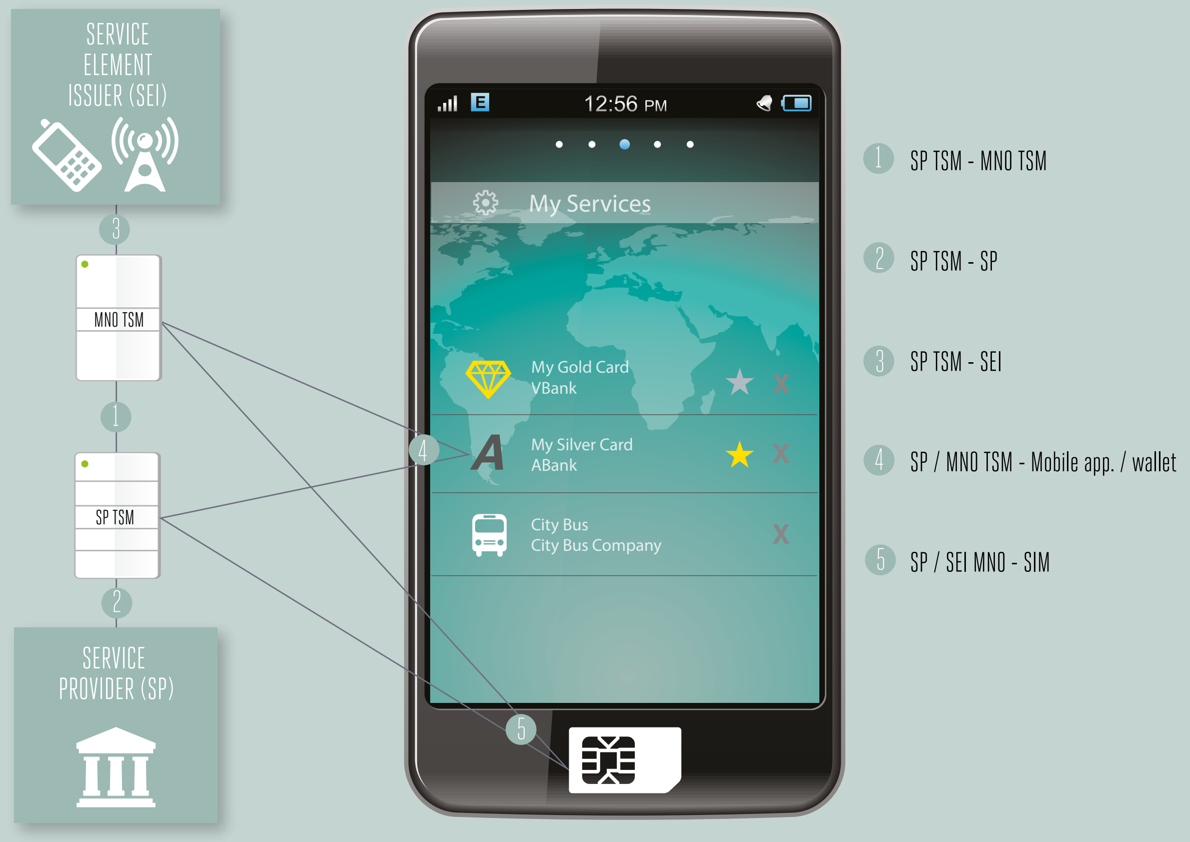


Figure 11

Service provider TSM – MNO TSM interface

In the context of a split ecosystem where MNOs and service providers have different TSMs, this interface allows the MNO TSM and service provider TSM to manage jointly the various NFC use cases covered by the TSMs.

Various specifications of this interface have been issued following the initial one from AFSCM. The publication by GlobalPlatform and GSMA of such specifications also ensures greater worldwide interoperability.

The table below presents the major specification releases for service provider TSM – MNO TSM interface.

NAME	CONTENT	RELEASE	DATE
AFSCM Interface specification between MNOs and NFC service providers	API and business processes	1.2	October 2009
AFSCM Interface specification between MNOs and NFC service providers	API and business processes	2.0.1	September 2011
GlobalPlatform Messaging specification for management of mobile NFC Services	API only	1.1	February 2013
GSMA NFC Mobile Network Operator – Service Provider Interface: Business Process Implementation Guidelines using GlobalPlatform Protocols	Business processes only	1.0	July 2012

Service provider TSM – Service provider interface

The interface between the service provider and its TSM is part of the GlobalPlatform messaging specification.

NAME	CONTENT	RELEASE	DATE
GlobalPlatform Messaging specification for management of mobile NFC Services	API only	1.1	February 2013

MNO TSM – MNO interface

Although some APIs of the GlobalPlatform Messaging specification can be used to some extent for the integration of the MNO and its TSM, there is no proper standard for this. As it is essentially an ‘internal’ interface between a MNO and its TSM, this has no impact on the solution’s global interoperability but it remains of high importance and impact during project implementation.

Service provider / MNO TSM – mobile application/wallet interface

There is currently no standard for this interface.

Service provider / MNO TSM – SIM

The management of the SIM is specified by various specifications from GlobalPlatform.

Some of the most important specifications are the following ones (in their current latest version).

NAME	RELEASE	DATE
GlobalPlatform Card Specification	2.2.1	January 2011
GlobalPlatform Card Specification v2.2 – Amendment A Confidential Card Content Management	1.0.1	January 2011
GlobalPlatform Card Specification v2.2 – Amendment B Remote Application Management over HTTP	1.1.1	March 2012
GlobalPlatform Card Specification v2.2 – Amendment C Contactless Services	1.0.1	February 2012
GlobalPlatform UICC Configuration	1.0.1	January 2011

Certification

Some of the NFC services managed by the MNO TSM and service provider TSM are particularly sensitive and require the TSM to be audited and certified.

The certification requirements, which are defined by relevant players, such as the financial payment schemes, are applicable to the service provider TSM and potentially to the MNO TSM as well.