GLOBALPLATFORM
THE STANDARD FOR SMART CARD INFRASTRUCTURE

GlobalPlatform Mobile Task Force

Requirements for NFC Mobile: Management of Multiple Secure Elements

Version 1.0

Public release

February 2010

Document Reference: GP_REQ_004

Table of contents

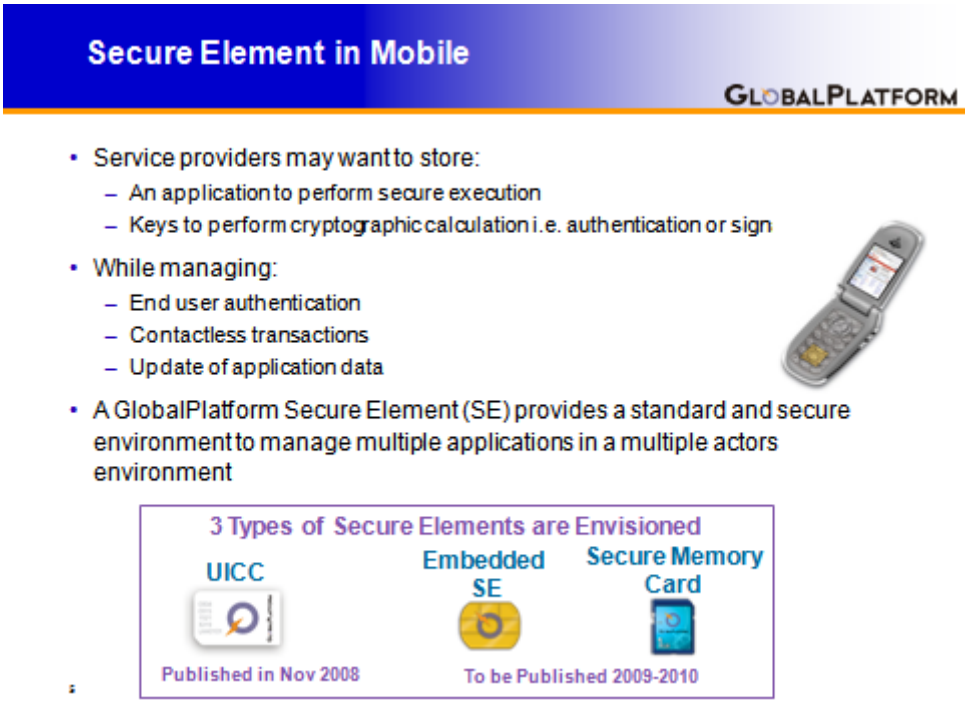
1. Introduction

In a near future, NFC contactless enabled mobile phones are expected to become ubiquitous. They will act as payment cards, transportation tickets, loyalty cards, access control badges and many other contactless services cards. Several pilots are already in progress worldwide but these are typically in closed environments, or limited in scope and number of players involved.

Many of the potential contactless services require one or more Secure Elements to store keys and applications. A Secure Element is a tamper resistant device with an embedded microprocessor chip.

The architecture of mobile handsets may support several Secure Elements of different types:

- UICC (a.k.a. SIM card)
- Embedded Secure Element
- Secure Memory card



In 2008, the GlobalPlatform Mobile Task Force decided to analyze potential implications of managing multiple Secure Elements in the same handset.

This document is the result of this investigation and describes requirements for managing multiple SE's .

2. Two different business approaches

2.1. Introduction

The discussion led to 2 different business models that are related to the role of actors in the value chain of delivering contactless services.

Secure Element issuers (SEI) offer a portfolio of services to their end customers by building portfolios of applications. Those applications and services are themselves provided by different service providers (SP).

One can anticipate that a Secure Element issuer will strike business agreements with multiple services providers and that a service provider will have some business relationships with multiple Secure Element issuers. GlobalPlatform's technology is a perfect foundation for any one of these actors: Secure Element issuers and service providers, to simplify the complexity and efects this new relationship matrix [n SEI's, m SP's]

One can assume that a(any) SEI that offers a portfolio of services to its end customers will ensure that appropriate customer relationship management (CRM) services, customer support and corresponding service level agreements (SLA's) will be put in place either by the SEI itself or by the various SP's the SEI has contracted with. The service availability may differ among the various SP's and applications depending of the capability of the Secure Element (security level, power off capacity,…) as well as the specific application requirements defined by the SP itself. Business arrangements between a SEI and SP's would typically include an online customer service desk (e.g. a hot line) to help end users during the usage of the SP's services.

One can easily extrapolate and envision that mobile handsets will often be capable of supporting multiple Secure Elements per handset. GlobalPlatform recognized this possibility and took the challenge of addressing the functional requirements implied by this technological possibility.

The research collected and reflection made by GlobalPlatform's Mobile Task-Force coalesced around 2 main functional architectures for 2 main business models: without aggregation vs with aggregation.

2.2. Architecture without aggregation

If multiple Secure Elements are located in the same Mobile handset, the service availability between comparable applications located on different Secure Elements may differ depending of the capability of the Secure Elements themselves (security level, power off capacity,…) as well as the customer support level of service offered by the various SEI's and SP's.

In order to avoid confusion at the end-user level (e.g. a customer support request to SEI A for an application supported by SEI B), a first architecture model is one in witch the end-user selects first a portfolio and the associated set of services, in other words the end-user selects first the Secure Element and the associated set of applications.

In this architecture, at one time, only one specific SE is able to perform a contactless transaction. The end user is responsible to select the right SE.

A simple example for such a business approach is a model where CRM or customer support services are directly managed by the SEI (on behalf of the SP's) for all the applications loaded onto the Secure Element the SEI is managing and/or responsible for.

2.3. Architecture with aggregation

Another example of business approach is a model where SP's are managing directly themselves their respective CRM and customer support services and are able to deploy their own applications across any type of Secure Element.
In such a business approach, SP's and SEI's wouldn't see a risk to have all Secure Elements managed all together to propose a global handset portfolio regrouping all services located in all SEs.

In this architecture, any application from any SE is able to perform a contactless transaction at any time, in other words all the various Secure Elements present on the same mobile handset may be active at any point in time.

In this architecture, the end-user sees a collection of all the services available in his/her mobile phone without knowing where they are hosted in his/her mobile phone.

2.4. Next steps

At this stage, the two business models are incompatible.

Managing multiple business models between actors is the core of the GlobalPlatform technology. In the smart card business, one actor making the investment of the smart card, called the issuer, has all management rights at the beginning of the card life and decides which actors will hosted in the card on specific agreement.

In the case of the mobile handset, the ownership responsibly and the investment can be very different depending of the market:

- Handset with operator subvention
- Handset offered by a service provider
- Handset bought by the end user.

Additionally the User may install in his/her handset a removable SE e.g. a memory card)

Even if the short term focus of the market is not in the management of multiple Secure Elements, GlobalPlatform Mobile Task Force would like to share the results of its investigation and these requirements with the overall industry.

GlobalPlatform is ready to participate to any effort when multiple Secure Elements management and the associated technology will be enough mature to be on the road map of other standardization organizations.

3. Requirements lists

In the following requirements, the term activation and desactivation of a SE is related to the possibility of the SE to access or not to a contactless router

3.1. Only one Secure Element active – no aggregation model

Nr	Description	Rationale	Remark
1	Among all SEs present on the mobile equipment, only one SE SHALL be activated by the user and visible to the reader at a time.	For customer care reasons, end users have to be aware of who is managing every SE. There is an end-user-licence-agreement (EULA) between the SE issuer and the end-user. This EULA describes the way the SE is managed by the SE issuer like application blocking/unblocking, application deletion, application update, application adding, SE replacement in case of loss, theft, broken… This EULA will very likely be different from a SE issuer to another. The end-user has to know under which EULA he is working.	Iimplies the specification of a lifecycle state for the SE
2	The active SE shall be chosen, explicitly through a native Menu of the phone, by the user and not changed without an active consent of the user.	Same as above. The ME is aware of the list of the connected SE and gives the possibility to the end-user to select an active SE among the connected ones list.	
3	In order to address consumer privacy only the minimum information necessary to select an application shall be transmitted to the reader.		
4	The ME native menu only displays the SE level. No information on the applications in the SE is displayed at this level.	The end-user first selects the active SE and then can manage (view, enable, disable, delete…) the applications through a SE issuer GUI.	Note: each SE shall only contain information on its own applications
5	Every SE SHALL provide a means that the application list of its SE can be displayed.	Different SEs owners mean different interface developers. Each SE owner will have its own graphic, ergonomic policies.	Supported in Amendment C
6	A firewalling feature shall be put in place between SEs, so no information from any SE can be retrieved by any other SE without authorization from the owner.	Each SE is the property of a different SE issuer	
7	If the user wants to use an application available in another SE, (s)he must first change the “active SE” before the transaction via the	The user shall be aware and give his active consent that he is leaving the world of one SE Issuer (and the associated EULA) and moves to the context of another SE issuer (and his EULA).	

Nr	Description	Rationale	Remark
	handset menu, and then select the application to be used for the transaction.		
8	It shall be possible to activate one or multiple payment application(s) on a single SE only.	The user shall be able to control which contactless applications are activated/deactivated	Supported in Amendment C
12	The host/user interface shall be able to dynamically retrieve all current contactless applications from an active SE and populate a (virtual) user list at any moment in time.	This means that in case a new application is loaded on a SE or an application is deleted, it will be automatically reflected in this User List	Supported in Amendment C
13	The status of every contactless application shall be registered in its SE itself (active over contactless interface or de-activated)		Supported in Amendment C
14	An active SE and its active contactless applications shall keep their state after power-off/power on	User friendliness	Supported in Amendment C
15	Application activation/de-activation is solely user controlled and only relates to the contactless reader interface		Supported in Amendment C
16	A single PPSE application listing the available payment applications in the active SE is required and shall be selectable by the POS	No change to the EMV contactless terminal infrastructure	Supported in Amendment C
17	A “registry” application shall exist on the SE capable of changing the priority and activation (selectable over the contactless interface) of the payment applications at the request of the user	Applying user choice	Supported in Amendment C
18	Contactless Applications shall have the capability to register themselves within the “registry”	Provide a mechanism to present the contactless applications to the user	Supported in Amendment C
20	The ability to modify an application’s state (activate or de-activate) indicating whether it is selectable by a POS over the contactless interface	Applying user choice	Supported in Amendment C
21	Application “registry” descriptions shall be clearly recognizable to the user allowing the user to view all possible payment applications It shall be possible to store user interface “information” (e.g. logo, label, etc…) associated with each payment application	Providing user with access to this information	Supported in Amendment C
22	The user shall be able to activate and prioritize one or more payment applications prior to presenting the	User ability to access the information and applying his/her choice	Supported in Amendment C

Nr	Description	Rationale	Remark
	mobile device to the POS Does not necessarily occur immediately preceding the presentation to the POS		
23	It shall be possible to register a group of contactless applications with relative priority visible to the user under a same display information provided during registration of the head of the group	Applying the existing ADF links of the card form factor to mobile	Supported in Amendment C
24	The registration information shall include an indicator that contactless application is blocked	To avoid unsuccessful user‘s attempts to activate a blocked application	Supported in Amendment C
25	The CRS shall reflect the change of contactless application states such as application locked / blocked etc…	User be aware of the changes or being unable to activate the application when it is not possible	Supported in Amendment C
26	Information about all applications relying on the PPSE shall be gathered by accessing the GlobalPlatform Contactless Registry Services (CRS) on a SE in the handset.	Providing user with a view of all contactless application on a SE in order to apply his/her choice on a SE	Supported in Amendment C
27	The registration information shall include an indicator on whether or not the application utilizes the PPSE for application selection	To be able to construct the FCI for response to PPSE select	Supported in Amendment C
28	The registration information shall include an indicator on whether this application can be active in combination with a PPSE (empty or not)	To provide deterministic selection between applications that use the PPSE and those that do not.	Supported in Amendment C
29	The registration information shall include an indicator of the type(s) of functionality supported by the application (access control, payment, transit, etc)	To be able to prioritize application selection per family of applications	Supported in Amendment C
30	The registration information shall include an identifier of the contactless protocol profile(s)/information supported by the application	To be able to apply conflict resolution for application activation on a SE	Supported in Amendment C
31	The registration information shall include the handset state requirements of the application. i.e., should this application be selectable when keypad or screen is not available? This may be better implemented as a resource requirement list taking into account e.g. keyboard access, GlobalPlatformRS	To facilitate the deployment of the application based on handset features/capabilities	

Nr	Description	Rationale	Remark
	connectivity , and/or display must be available for approval by the customer		
33	A SE shall be able to reorder selecting applications in order of priority provided by the user. Partial selection shall be performed in the order defined by the user.	Existing contactless reader have only partial selection capability	Supported in Amendment C
34	The CRS shall be able to store a 'discretionary data'; this PPSE specific data element is to be retrieved by the AAUI. Minimum size TBD	To allow proper construction of the FCI response in select PPSE	Supported in Amendment C
35	Transport applications have to be always accessible (also in battery off mode)	Gates' terminals will explicitly select the right application.	See 32
37	Specification for managing Multiple SE should not introduce new potential privacy breaches (i.e. new ways to get access to personal/private/sensitive data; new ways of tracking individuals…)	Privacy management It is not the role or mission of Global Platform to fix the potential privacy breaches in applications that will fall under the umbrella of multiple SEs. Today, there are legitimate applications (payment, ticketing…) that do not comply with the present and future privacy requirements. Fixing this is outside of the scope of Global Platform.	

3.2. All Secure Element active at the same time – aggregation model

Nr	Description	Rationale	Remark
1	When multiple SEs exist it shall be possible to collect and display to the user all contactless applications of all SEs.	User Interface applications should be able to display to the user contactless applications from any number of SEs and allow the user to control the activation/deactivation of these contactless application.	
2	It shall be possible that each SE contain one or more payment applications.	Each SE may contain application(s).	
3	It shall be possible to activate one or multiple payment application(s) on a single SE only.	The user shall be able to control which contactless applications are activated/deactivated	
4	It shall be possible to activate multiple payment applications across multiple SEs.	The user shall be able control which contactless applications are activated/deactivated	See nr 22
5	When multiple payment applications across multiple SEs are active, the POS reader shall receive only a single response to its PPSE request (reflecting all the active applications).	Legacy POS devices shall retrieve a single PPSE Select response reflecting all the active contactless applications as chosen by the user	See nr 23
6	Two lists are required: One towards the user, listing all contact-less applications (residing on all SEs), and another one towards the contacltess routing entity, listing all activated contactless applications (of all SEs). Conflicts of active contactless applications shall be avoided. Conflict resolution between applications from different SEs needs to be addressed appropriately	User shall be able to activate/de-activate its application	Potential concerns due to some domestic privacy policies
7	The Reader List shall be visible in battery low/off mode for the reader.	e.g., the reader shall be able to select a ticketing application in battery off mode	
9	A selection request from the reader to an active contactless application will be directly forwarded to the appropriate SE where the application is residing and all further communication will be between the reader and the SE.	No specific security requirements on the Reader List	
10	The host/user interface shall be able to dynamically retrieve all current contactless applications from all SEs and populate a (virtual) user list at any moment in time.	This means that in case a new application is loaded on a SE or an application is deleted, it will be automatically reflected in this User List	
11	An active SE and its active contactless applications shall keep their state after power-off/power on.	User friendliness	
12	Application activation/de-activation is solely user controlled and only relates to the reader interface.		
13	The presentation of the Reader List and application selection of the reader does		

Nr	Description	Rationale	Remark
	require timeliness		
14	It shall be possible to present to the user a list of all applications residing in all SEs.	The user should be able to find an application easily and quickly. The user does not need to be aware of multiple SEs.	
15	It shall be possible for a single entity to manage multiple secure domains in different SEs on the same device.	There should be no technical restrictions for OTA management of multiple SEs.	
16	It shall be possible to load and install applications with the same package ID and AID in different SEs.	No extra checks are needed across SEs.	
17	It shall be possible to activate applications in different SEs at the same time.	The user should be able to activate applications without being aware of multiple SEs.	
18	It shall not be possible for applications with the same AID in different SEs to be activated at the same time.	The restriction for the previous requirement is to prevent an unknown result to occur with the contactless reader.	
19	It shall not be a requirement for the contactless reader to be aware of multiple SEs to perform a transaction.	To allow legacy contactless readers to work with devices supporting multiple SEs.	
20	It shall be possible to select default application(s) for use in battery off mode.	To allow legacy contactless readers to work with devices supporting multiple SEs.	
22	For devices with multiple SEs there shall be a mechanism to collect the information from the different registries of the different SEs	Providing user with a global view of all contactless applications on all SEs in order to apply his/her choice cross all SEs	Potential concerns due to some domestic privacy policies
23	For devices with multiple SEs there shall be a single PPSE *selectable* by POS. The FCI returned in select PPSE shall include the user choice across all SEs –	No change to the EMV contactless terminal infrastructure and reflecting the user choice	
24	Information about all applications relying on the PPSE shall be gathered by accessing the GlobalPlatform Contactless Registry Services (CRS) on every SE in the handset.	Providing user with a global view of all contactless application on all SEs in order to apply his/her choice across all SEs	
25	The registration information shall include an identifier of the contactless protocol profile(s)/information supported by the application	To be able to apply conflict resolution for application activation across SEs	
26	The user shall be able to change the status of each application in the CRS of the SE. Status includes: Application activated/deactivated	Applying the user choice across all SEs	
27	Transport applications have to be always accessible (also in battery off mode)	Gates' terminals will explicitly select the right application.	
28	All SEs have to be active in the same time.		`
29	Specification for managing Multiple SE should not introduce new potential privacy breaches (i.e. new ways to get access to personal/private/sensitive data; new ways	Privacy management It is not the role or mission of Global Platform to fix the potential privacy breaches in applications that will fall under the umbrella of multiple SEs. Today,	

Nr	Description	Rationale	Remark
	of tracking individuals…)	there are legitimate applications (payment, ticketing…) that do not comply with the present and future privacy requirements. Fixing this is outside of the scope of Global Platform.	

4. Conclusion

NFC contactless enabled mobile phones as an everyday consumer device, for use in a wide array of business applications, is fast becoming a reality. For players within the mobile environment to be ready for the wave of opportunity NFC brings with it, it is vital for infrastructure modifications and expansion to be based on recognized industry standards. Without the appropriate standards to manage backend systems, exchange messages, download and personalize applications, and manage Secure Element contents, it will be impossible to achieve consistency, reliability and interoperability in the NFC contactless mobile ecosystem.

GlobalPlatform, as a cross-industry standards organization, has through its leadership and deep experience created several specifications that have laid a firm foundation for effective management of GlobalPlatform-based smart cards management. GlobalPlatform plans to continue its role by creating new and enhancing existing specifications to serve all entities in the mobile environment.

Publication of an updated version of the GlobalPlatform Messaging specification is planned for the beginning of 2010. This will be an important step in providing the specifications for standard messaging enabling exchanges between disparate systems in the GlobalPlatform smart card infrastructure.

GlobalPlatform will have a full set of specifications available for all roles in the contactless mobile ecosystem by the beginning of 2010. The specifications will include GlobalPlatform 2.2 [0], its amendments [1], [4] and the UICC Configuration [2] as the first configuration for Secure Elements. The specifications will facilitate the creation of a standard infrastructure allowing application/service providers, trusted service managers and mobile network operators to manage application download and personalization of NFC contactless enabled mobile phones, for issuance and post issuance of GlobalPlatform based Secure Elements compliant with the UICC Configuration specification [2].

APPENDIX A: References

Standard / Specification	Description	Ref
GlobalPlatform Card v 2.2	Card specification from GlobalPlatform	[0]
GlobalPlatform Confidential Card Content Management – Card Specification v2.2 – Amendment A v1.0	Defines a mechanism for an application provider to confidentially manage its own application when using a third party communications network.	[1]
UICC Configuration v1.0	An implementation guide for deploying GlobalPlatform Card Specification v2.2 within the mobile services sector and managing the secure over-the-air delivery of new services. It outlines the behaviour of each actor involved in a UICC implementation, how each one should be represented, and a summary of roles and responsibilities in a variety of business models	[2]
GlobalPlatform Messaging Specification v1.0	Describes the format and data requirements for various components of the systems infrastructure to communicate.	[3]
GlobalPlatform 2.2 Amendment C	Defines a mechanism for an end user to activate a contactless services when the card support multiples contacltess application	[4]

APPENDIX B: Abbreviations and Notations

Abbreviation	Meaning
AP	Application Provider (Actor)
CRS	Contactless registry Service
EULA	end-user-licence-agreement
GSM-A	Global System for Mobile Telecommunications Association
MNO	Mobile Network Operator
NFC	Near Field Communication
OTA	Over-The-Air
SE	Secure Element
SEI	Service Element Issuer
SP	Service Provider
UICC	Universal Integrated Circuit Card